

Sicherheit und Privatsphäre im Bereich der mobilen Endgeräte

vorgelegt von

M. Sc.

Sven Bock

ORCID: 0000-0002-9931-9569

an der Fakultät V - Verkehrs- und Maschinensysteme

der Technischen Universität Berlin

zur Erlangung des akademischen Grades

Doktor der Naturwissenschaften

- Dr. rer. nat. -

genehmigte Dissertation

Promotionsausschuss:

Vorsitzender	:	Prof. Dr.-Ing. Henning Jürgen Meyer, Technische Universität Berlin
Erstgutachter	:	Prof. Dr.-Ing. Matthias Rötting, Technische Universität Berlin
Zweitgutachter	:	Prof. Dr. Lothar Fritsch, Karlstads Universitet, Schweden

Tag der wissenschaftlichen Aussprache: 19.08.2021

Berlin 2021

Veröffentlichungen im Rahmen der vorliegenden Dissertation

Bock, S. (2017). My data is mine -rights and personal information on mobile device. 10.13140/RG.2.2.17526.83527.

Bock, S. (2018). My Data is Mine-Users' Handling of Personal Data in Everyday Life. SICHERHEIT 2018.

Momen, N & Bock, S. (2018). User Perception Analysis for Showing Personal Data Access as Privacy Implication Factor. 10.13140/RG.2.2.18227.66086.

Bock, S. (2019). How the availability of privacy information influences users' smartphone app selection behaviour. 10.13140/RG.2.2.26334.87364.

Bock, S. & Momen, N. (2020). Einfluss einer Datenschutzskala auf das Auswahlverhalten in einem App-Markt.

Momen, N. & Bock, S. & Fritsch, L. (2020). Accept - Maybe - Decline: Introducing Partial Consent for the Permission-based Access Control Model of Android. 71-80. 10.1145/3381991.3395603.

Momen, N. & Bock, S. (2020). Neither Do I Want to Accept, nor Decline; Is There an Alternative?. 10.1007/978-3-030-50732-9_74.

Bock, S. & Momen, N. (2020). A Study on User Preference: Influencing App Selection Decision with Privacy Indicator.

Bock, S., & Momen, N. (2020, October). Nudging the User with Privacy Indicator: A Study on the App Selection Behavior of the User. In Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (pp. 1-12).

Bock, S., Chowdhury, A. F., & Momen, N. Partial Consent: A Study on User Preference for Informed Consent.

Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich diese Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die von mir angegebenen Quellen und Hilfsmittel nicht benutzt und die den benutzten Werken wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Berlin, den 19.08.2021

Sven Bock

Danksagung

Die Fertigstellung dieser Dissertation habe ich der Unterstützung vieler Personen zu verdanken. Ich möchte mich besonders bei Prof. Dr. Matthias Rötting bedanken, der mich in den letzten 5 Jahren stets in meinem Vorhaben unterstützt und vor allem in herausfordernden Situationen Hinweise und Ideen für eine geeignete Problemlösung hervorbrachte. Darüber hinaus rechne ich ihm hoch an, dass er mir die Durchführung der Versuche als auch den Besuch diverser Konferenzen ermöglicht hat. Ich möchte mich auch bei Prof. Dr. Lothar Fritsch für die Übernahme der Rolle des externen Gutachters bedanken. Ein besonderer Dank geht an Dr. Nurul Momen, der mir sowohl bei der Themenfindung als auch bei der Durchführung des zweiten und dritten empirischen Versuchs geholfen hat. Die Zusammenarbeit mit Nurul war stets sehr effizient und lösungsorientiert und hat mir somit viel Spaß bereitet. Vor allem den Austausch unserer Ergebnisse und die Symbiose unserer Doktorarbeiten in unterschiedlichen Fachgebieten empfand ich stets als sehr spannend und führte zu einigen Veröffentlichungen von wissenschaftlichen Artikeln. Ferner möchte ich mich bei den zahlreichen Assistenten und Assistentinnen bedanken, ohne die die Fertigstellung dieser Dissertation nicht denkbar gewesen wäre. Zu guter Letzt möchte ich mich bei meiner Familie und meinen Freunden bedanken, die niemals an meinem Vorhaben gezweifelt haben und mir besonders in schwierigen Situationen zu Seite standen.

Abstract

This dissertation deals with the problem of the disclosure of personal data during the use of mobile devices. The thesis consists of three studies, whereby the participants were initially not informed about the research purposes in order to achieve higher validity of the results. The first study aimed to assess the importance of personal data for participants and how they handle it, while the second and third study present solutions that enable end users to adopt more privacy-friendly behaviour.

In the first empirical study, an experiment was designed to investigate the handling of 51 participants regarding the disclosure of their personal data. Furthermore, it was to be examined whether the presentation form of the participation agreement as a printed form or as a dialogue box influenced the participants' decision to accept or reject it. Both the reading time and the willingness to accept the participation agreement were recorded. The results showed a paradoxical behaviour, whereby on the one hand the participation agreement was hardly even read, and a liberal approach to the disclosure of data was observed in most cases. On the other hand, however, they attributed a high monetary and personal value to their data. This behaviour could be explained by the lack of understanding the long-term consequences of disclosure of personal data.

To create an awareness of these consequences, a privacy-scale was developed in the second study, on which the impact on the selection of applications was determined. For this purpose, a prototyped app market was developed, in which the privacy-scale illustrates the aggressiveness of the respective applications. After evaluating the behaviour with the help of eye-tracking, questionnaires and video confrontations, the results showed a significant influence of the privacy-scale on the selection behaviour of the 82 participants, though this influence decreased with increasing familiarity of the applications. However, the end users are often dependent on some applications and cannot use any alternative.

For this reason, a third empirical study was conducted to assess the use, acceptance, and desirability of temporary access authorisation. For this purpose, an application was developed which required access authorisation to different data types for different tasks. The participants then had the option of granting the authorisation temporarily, permanently or decline the access. This function was only used by one-fifth of the 32 participants, while half of the sample stated that they also wanted to use the temporary access authorisation on their private end device.

Zusammenfassung

Diese Dissertation behandelt die Problematik der Herausgabe von persönlichen Daten während der Nutzung mobiler Endgeräte. Dabei setzt sich die Arbeit aus drei Studien zusammen, wobei den Teilnehmenden für eine höhere Validität der Ergebnisse die Zwecke der Studien zunächst verschwiegen wurden. Die erste Studie diente der Erkenntnisgewinnung über den Stellenwert der persönlichen Daten seitens der Teilnehmenden und dem Umgang mit diesen, während die zweite und dritte Studie Lösungen vorstellen, welche den Endnutzenden die Möglichkeit geben, ein datenschutzfreundlicheres Verhalten aufzuzeigen.

In der ersten empirischen Studie wurde ein Experiment entworfen, welches die Freizügigkeit der 51 Teilnehmenden bezüglich ihrer persönlichen Daten untersuchen sollte. Ferner wurde geprüft, ob die Präsentationsform der Teilnahmevereinbarung als gedruckte Form oder als Dialogfenster Einfluss auf die Entscheidung der Teilnehmenden bezüglich der Annahme oder Ablehnung dieser hatte. Hierbei wurde sowohl die Lesezeit als auch die Bereitschaft, die Teilnahmevereinbarung zu akzeptieren, festgehalten. Die Ergebnisse zeigen ein paradoxes Verhalten auf, wobei einerseits die Teilnahmevereinbarung kaum gelesen und meist ein freizügiger Umgang mit der Weitergabe der Daten beobachtet wurde. Andererseits haben sie ihren Daten jedoch einen hohen monetären und persönlichen Wert zugeschrieben. Diese Handlungsweise konnte mit der Uneinsichtigkeit der langfristigen Konsequenzen bei der Weitergabe von persönlichen Daten begründet werden.

Für das Schaffen eines Bewusstseins gegenüber diesen Konsequenzen wurde in der zweiten Studie eine Datenschutzskala entworfen, deren Einfluss auf die Applikationsauswahl eruiert wurde. Hierfür wurde ein prototypisierter App-Markt entwickelt, in dem die Datenschutzskala die Aggressivität der jeweiligen Applikationen illustriert. Nach dem Auswerten des Verhaltens mit Hilfe von Eye-Tracking, Fragebögen und Videokonfrontationen zeigen die Ergebnisse einen signifikanten Einfluss der Datenschutzskala auf das Auswahlverhalten der 82 Teilnehmenden, wobei dieser Einfluss mit steigender Bekanntheit der Applikationen abnahm. Im Alltag sind die Endnutzenden allerdings oft auf einige Applikationen angewiesen und können keine Alternative verwenden.

Aus diesem Grund wurde eine dritte empirische Studie durchgeführt, welche die Verwendung, Akzeptanz und Erwünschtheit einer temporären Zugriffsberechtigung ermitteln sollte. Hierfür wurde eine Applikation entwickelt, welche bei unterschiedlichen Aufgaben Zugriffsberechtigungen auf verschiedene Daten einforderte. Die 32 Teilnehmenden hatten anschließend die Möglichkeit, die Berechtigung nicht, temporär oder endgültig zu erteilen. Dabei wurde die Funktion lediglich von einem Fünftel der Teilnehmenden angewandt, wobei die Hälfte der Stichprobe angab, die temporäre Zugriffsberechtigung auch auf ihrem privaten Endgerät nutzen zu wollen.

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
bzw.	Beziehungsweise
CFIP	Concern for information privacy
CTA	Click-Through-Agreement
CPM	Communication Privacy Management Theorie
ect.	et cetera
EULA	Endbenutzer-Lizenz-Vertrag
IUIPC	Internet Users Information Privacy Concerns
MUIPC	Mobile Users Information Privacy Concerns
z. B.	Zum Beispiel

Inhalt

1 Einleitung 1
1.1 Aufgabenstellung 3
1.2 Gliederung 4
2 Grundlagen und Definitionen 7
2.1 Definitionen 7
2.1.1 Datenschutz 7
2.1.2 Privatsphäre der Daten 8
2.1.3 Mobile Endgeräte 8
2.1.4 Betriebssystem 9
2.1.5 Software Rechte 10
2.1.6 Applikationen 11
2.1.7 Behaviorismus 12
2.1.8 EU-Datenschutzgrundverordnung 13
2.2 Grundlagen 14
2.2.1 Sammeln und Verwenden von Daten 14
2.2.2 Ertragseinbringung durch Applikationen 16
2.2.3 In-App Werbung 18
2.2.4 Rechte und deren Abtretung 19
2.2.5 Sicherheitsverhalten und Konditionierung 19
2.2.6 Verhalten der Endnutzenden gegenüber den AGBs und EULAs 22
2.2.7 Einschätzung der Wichtigkeit der Daten seitens der Endnutzenden 23
2.2.8 Privacy Paradox 26
2.2.9 Konsequenzen für die Endnutzenden 26
2.2.10 Umgang mit der Datensicherheit in Unternehmen 27
2.2.11 Auswirkungen von verfügbaren Informationen über den Schutz der Privatsphäre auf das Kaufverhalten 29
2.2.12 Strategien zur Schaffung von Privatsphäre 33
2.2.13 Einflüsse auf datenschutzrechtliche Bedenken beim Herunterladen von Applikationen 33
3 Stand der Forschung 35
4 Versuchsübergreifende Fragestellungen 37
5 Empirischer Versuch 1 – Umgang mit persönlichen Daten und deren Weitergabe 39
5.1 Forschungsfragen 39
5.2 Hypothesen 40
5.3 Versuchsdesign 41
5.4 Untersuchungsvariablen 42

5.5 Versuchsvorbereitung und Aufbau 44
5.5.1 Fragebogen zur Erfassung der Einstellung gegenüber der Weitergabe der Daten und Rechte 44
5.5.2 Programm zur Entscheidungsfindung 46
5.5.3 Täuschungsexperiment 47
5.5.4 Auswahl der Teilnehmenden 51
5.6 Datenaufbereitung 51
5.6.1 Demographische Daten 51
5.6.2 Teilnahmevereinbarungen 51
5.6.3 Fragebogen 52
5.6.4 Ankreuzbogen zur Weitergabe der Daten 53
5.6.5 Demographische Daten der Stichprobe 53
5.6.6 Interview 53
5.7 Ergebnisse 54
5.7.1 Vergleich mit dem Umgang der Teilnahmevereinbarungen 54
5.7.2 Zusammenhang zwischen dem Alter und den Begründungen für den Umgang mit den Teilnahmevereinbarungen sowie der Nutzung von bestimmten Applikationskategorien 60
5.7.3 Zusammenhang zwischen Geschlecht und Begründung 60
5.7.4 Zeitpunkt der geleisteten Unterschrift und Begründungen für den Umgang mit den Teilnahmevereinbarungen 61
5.7.5 Gewählte Vergütung 62
5.7.6 Interview 64
5.7.7 Fragebogen 67
5.8 Diskussion 77
5.8.1 Zur Hypothese 1: Aufgewendete Zeit zum Lesen der Teilnahmevereinbarung 78
5.8.2 Zur Hypothese 2: Stellenwert des Schutzes der Persönlichen Daten 80
5.8.3 Zur Hypothese 3: Akzeptanz geringer Einbußen zur Wahrung der Rechte und Daten 82
5.8.4 Zur Hypothese 4: Unterschied des Datenschutzes im gewerblichen und privaten Bereich 83
5.8.5 Zur Hypothese 5: Gleichgültigkeit gegenüber der Abgabe von Informationen durch uneinsichtige Konsequenzen 84
5.8.6 Zur Hypothese 6: Aushändigen von persönlichen Daten für eine geringe Gegenleistung 86
5.8.7 Zur Hypothese 7: Unterschiede der Lesedauer zwischen den unterschiedlichen Präsentationsformen 88
5.8.8 Diskussion der explorativen Ergebnisse 89
5.9 Probleme und Ausblick 91
5.10 Fazit 92

6 Empirischer Versuch 2 – Einfluss einer Datenschutzskala auf das Auswahlverhalten im App-Markt 94
6.1 Forschungsfragen 94
6.2 Hypothesen 95
6.3 Versuchsdesign 99
6.4 Untersuchungsvariablen 101
6.5 Versuchsvorbereitung 104
6.5.1 Sammeln der Zugriffsdaten 105
6.5.2 Berechnung des Privacy-Werts 115
6.5.3 Entwurf der Skalen 116
6.5.4 Vorstudie zur Bestimmung einer adäquaten Illustrierung 117
6.5.5 Erstellung des App-Marktes 120
6.5.6 Stichprobenumfangsberechnung 122
6.5.7 Auswahl der Teilnehmenden 122
6.6 Aufbau 123
6.6.1 Einleitung und Einverständniserklärung 123
6.6.2 Bereits installierte Applikationen 124
6.6.3 Experiment zur Auswahl geeigneter Applikationen mit Eye-Tracking 125
6.6.4 Aufklärung über das Ziel der Studie 126
6.6.5 Videokonfrontation mit Fragebogenteil zur Applikationsauswahl 126
6.6.6 Bewertung der Datenschutzskala 127
6.6.7 Bedenken der Nutzenden im Bereich der mobilen Endgeräte (MUIPC) 127
6.6.8 Demographische Daten 129
6.7 Datenaufbereitung 129
6.7.1 Demographische Daten der Stichprobe 129
6.7.2 Fragebogen 130
6.7.3 Eye-Tracking-Video 131
6.7.4 Interview 144
6.8 Ergebnisse 146
6.8.1 Demographie der Teilnehmenden 146
6.8.2 Eye-Tracking-Video 148
6.8.3 Ergebnisse ausgewählter Applikationen 156
6.8.4 Angemessenheit der Applikationsauswahl (Score- Vergleich) 157
6.8.5 Interview 160
6.8.6 Fragebogen 164
6.8.7 Zusammenhang zwischen der Auswahl der Applikation (Score) und den Bedenken über den Datenschutz (MUIPC) 189

6.9 Diskussion 191
6.9.1 Zur Hypothese 1: Diskussion der Einfachheit der Applikationsauswahl und Vertrauenswürdigkeit der Applikation 191
6.9.2 Zur Hypothese 2: Diskussion über die Angemessenheit ausgewählter Applikationen 196
6.9.3 Zur Hypothese 3: Diskussion zum Vergleich der Differenzen der Entscheidungszeiten der Applikation in chronologischer Reihenfolge 200
6.9.4 Zur Hypothese 4: Diskussion zum Vergleich der Fixationszeiten 203
6.9.5 Diskussion zum Vergleich der Entscheidungszeiten zwischen den Szenarien 204
6.9.6 Diskussion zu Entscheidungszeiten zwischen den Gruppen 205
6.9.7 Diskussion zur Bekanntheit der ausgewählten Applikation 205
6.9.8 Diskussion zur Bewertung der Datenschutzskala 209
6.9.9 Diskussion zum Measuring Mobile Users Concerns for Information Privacy (MUIPC) 210
6.9.10 Diskussion zum Zusammenhang zwischen der Auswahl der Applikation (Score) und den Bedenken über den Datenschutz (MUIPC) 211
6.9.11 Diskussion zur Relevanz der Methoden zur Applikationsbewertung 212
6.9.12 Diskussion der Videokonfrontation anhand des Interviews 214
6.10 Probleme und Ausblick 215
6.11 Fazit 218
7 Empirischer Versuch 3 – Akzeptanz und Verwendung einer temporären Zugriffsberechtigung 220
7.1 Forschungsfragen 220
7.2 Hypothesen 222
7.3 Versuchsdesign 224
7.3.1 Untersuchungsvariablen 226
7.3.2 Versuchsvorbereitung 227
7.3.3 Implementierung der temporären Zugriffsberechtigung in eine Nachrichtenapplikation 227
7.3.4 Auswahl der Teilnehmenden 229
7.4 Aufbau 230
7.4.1 Einleitung und Einverständniserklärung 230
7.4.2 Device-ID 231
7.4.3 Aufgaben 231
7.4.4 Fragebogen zu Akzeptanz und Erwünschtheit der temporären Zugriffsberechtigungen 232
7.4.5 Aufklärung 234
7.5 Datenaufbereitung 234
7.5.1 Demographische Daten der Stichprobe 235
7.5.2 Fragebogen über die Akzeptanz der temporären Zugriffsberechtigung 235
7.5.3 Device ID 237

7.5.4 Applikationsdaten 237
7.6 Ergebnisse 238
7.6.1 Demographische Daten der Stichprobe 238
7.6.2 Fragebogen über die Akzeptanz der vorübergehenden Datenfreigabe 240
7.6.3 Applikationsdaten 246
7.7 Diskussion 249
7.7.1 Zur Hypothese 1: Diskussion über die Anwendung der temporären Zugriffsberechtigung 249
7.7.2 Zur Hypothese 2: Diskussion über die Bewertung der temporären Zugriffsberechtigung 251
7.7.3 Zur Hypothese 3: Diskussion über die Erwünschtheit der temporären Zugriffsberechtigung 252
7.7.4 Zur Hypothese 4: Diskussion über das Ärgernis durch die wiederkehrende Anfrage einer Berechtigung 254
7.7.5 Zur Hypothese 5: Diskussion über die Abwägung zwischen der Kontrolle der Daten und dem wiederkehrenden Anfragen für die Berechtigung 255
7.7.6 Diskussion der explorativen Ergebnisse 255
7.8 Probleme und Ausblick 258
7.9 Fazit 259
8 Versuchsübergreifendes Fazit 262
9 Literaturverzeichnis 267
Anhang I
Anhang A. Measuring mobile users' concerns for information privacy (MUIPC) I
Anhang B. Fragebogen zur Erfassung der Einstellung gegenüber der Weitergabe der Daten und Rechte II
Anhang C. Quellcode zum Programm zur Entscheidungsfindung VI
Anhang D. Standardisierte Einführung zum ersten Versuch XVII
Anhang E. Teinahmebedingungen zum ersten Versuch XVIII
Anhang F. Liste der Begriffspaare XXI
Anhang G. Dokument zur Weitergabe der Daten XXV
Anhang H. Interviewfragen XXVII
Anhang I. Aufklärung XXVIII
Anhang J. Tabellen zum ersten Versuch XXIX
Anhang K. Variablen zum ersten Versuch L
Anhang L. Daten der Personas LIII
Anhang M. Liste der Antworten zu der Frage der am meisten genutzten Applikationen LIII
Anhang N. Liste zur Frage der am wenigsten vertrauten Applikationen LIV
Anhang O. Abbildungen der Skalen zum Vortest LV

Anhang P. Fragebogen zur Vorstudie LX

Anhang Q. Beschreibung der Datenschutzskala mit Diagrammen zu Abfrage der Rechte und Risiko zur Freigabe persönlicher Informationen LXI

Anhang R. Einverständniserklärung zur zweiten Studie LXII

Anhang S. Anleitung zur Generierung des persönlichen Codes LXIII

Anhang T. Einverständniserklärung für Video- und Tonaufnahme LXIV

Anhang U. Fragebogen des 2. empirischen Versuchs LXV

Anhang V. Szenarien LXXIV

Anhang W. Aufklärung über den Zweck der zweiten Studie LXXV

Anhang X. Bildschirmabzug der A-Ware Applikation LXXVI

Anhang Y. Tabellen zum zweiten Versuch LXXVII

Anhang Z. Entscheidungsmotive für die Auswahl der Applikationen CCCXIX

Anhang AA. Variablen zum zweiten Versuch CCCXX

Anhang BB. Einverständniserklärung zum dritten empirischen Versuch CCCXXXIII

Anhang CC. Aufgabenstellung zum dritten empirischen Versuch CCCXXXIV

Anhang DD. Einstellungsmenü mit Device-ID CCCXXXVI

Anhang EE. Aufklärung zum dritten empirischen Versuch CCCXXXVII

Anhang FF. Variablen zum dritten Versuch CCCXXXVIII

Anhang GG. Tabellen zum dritten Versuch CCCXL

Anhang HH. Fragebogen zum dritten Versuch CCCLIII

Anhang II. Übersicht von den Forschungsfragen und den entsprechenden Hypothesen CCCLIX

Tabellenverzeichnis

Tabelle 1 Median des App-Score getrennt nach Gruppen verschiedener Entscheidungsmotive 163
Tabelle 2 Mann-Whitney-U-Test gemessene Lesedauer und Präsentationsform XXIX
Tabelle 3 T-Test der gemessenen Lesedauer und Präsentationsform XXX
Tabelle 4 Mann-Whitney-U-Test gemessene Lesedauer und Geschlecht XXXI
Tabelle 5 T-Test gemessene Lesedauer und Geschlecht XXXII
Tabelle 6 Mann-Whitney-U-Test der Gruppe, die soziale Medien häufig nutzt, und der Lesedauer XXXIII
Tabelle 7 Mann-Whitney-U-Test der Gruppe, die Messenger-Applikationen häufig nutzt und Lesedauer XXXIII
Tabelle 8 Korrelationen zwischen Alter und Lesedauer XXXIV
Tabelle 9 Korrelationen zwischen gewählter Vergütung und gemessener Lesedauer XXXIV
Tabelle 10 *Korrelation zwischen gemessener Lesedauer und Häufigkeit des Lesens der AGB vor der Installation einer Software* XXXIV
Tabelle 11 Korrelationen zwischen den Begründungen für das Unterlassen des Lesens der AGBs und der gemessenen Lesedauer XXXV
Tabelle 12 Korrelationen zwischen den Begründungen für das Lesen der AGBs und der gemessenen Lesedauer XXXV
Tabelle 13 Wilcoxon-Test für gemessene Lesedauer der Teilnahmevereinbarungen, die im Fragebogen angegebene Lesedauer und die im Interview geschätzte Lesedauer XXXVI
Tabelle 14 Korrelationen Alter und Nutzung von verschiedenen Applikationen XXXVII
Tabelle 15 T-Test Alter und Zeitpunkt der Unterschrift..... XXXVIII
Tabelle 16 Korrelationen zwischen Geschlecht und Zeitpunkt der Unterschrift XXXIX
Tabelle 17 Mann-Whitney-U-Test Zeitpunkt der Unterschrift und Lesedauer XXXIX
Tabelle 18 Mann-Whitney-U-Test Vergütung in Euro und Geschlecht XL
Tabelle 19 Korrelationen zwischen Vergütung in Euro und Alter XLI
Tabelle 20 Mann-Whitney-U-Test Vergütung und Präsentationsform XLI
Tabelle 21 Mann-Whitney-U-Test Vergütung in Euro und Zeitpunkt der Unterschrift.....XLII
Tabelle 22 Mann-Whitney-U-Test für Vergütung in Euro und Nutzung verschiedener Applikationsgruppen XLIII
Tabelle 23 Korrelationen Vergütung und Begründung für Häufigkeiten des Lesens der AGBs.....XLIV
Tabelle 24 Mann-Whitney-U-Tests von verschiedenen Applikationsgruppen und der gemessenen Vergütung in Euro XLV
Tabelle 25 Korrelationen zwischen Geschlecht und den Begründungen warum AGBs nicht gelesen wurden XLVI
Tabelle 26 Korrelationen zwischen Geschlecht und den Begründungen warum AGBs gelesen wurden XLVI
Tabelle 27 Korrelationen des Geschlechtes mit den verschiedenen Kategorien der Applikationen XLVII
Tabelle 28 Mann-Whitney-U-Tests Vergleich zwischen dem Stellenwert des Datenschutzes und der Anzahl an angegebenen Konsequenzen XLVIII
Tabelle 29 Mann-Whitney-U-Tests Vergleich zwischen dem Stellenwert des Datenschutzes und dem Geschlecht.....XLIX
Tabelle 30 Korrelationen zwischen finanziellem Aufwand für neue Applikationen und finanziellem Aufwand für Schutz der Privatsphäre XLIX
Tabelle 31 Auflistung der Applikationen zur Messung der Aggressivität nach Kategorien LXXVII
Tabelle 32 Friedman-Test der Bewertung der fünf Skalen LXXVIII
Tabelle 33 *Friedman-Test der Bewertung der sieben Skalen* LXXVIII
Tabelle 34 *Häufigkeiten der Auswahl nach Dartstellungsposition in der Benutzeroberfläche* LXXVIII
Tabelle 35 Demographische Daten Alter und Geschlecht LXXIX

Tabelle 36 Demographische Daten Bildung LXXIX
Tabelle 37 Tägliche Handynutzung in Stunden LXXIX
Tabelle 38 Technikaffinität LXXIX
Tabelle 39 Häufigkeiten der Auswahl zum allgemeinen Fragen bezüglich der Privatsphäre LXXX
Tabelle 40 Demographische Daten Alter und Geschlecht für das Eye-tracking-Video LXXXI
Tabelle 41 Entscheidungszeiten in Sekunden der jeweiligen Szenarien LXXXII
Tabelle 42 Friedman-Test der Entscheidungszeiten zwischen den Szenarien LXXXII
Tabelle 43 Wilcoxon-Test für den Vergleich der Entscheidungszeiten zwischen den Szenarien ... LXXXIII
Tabelle 44 Entscheidungszeiten getrennt nach Szenarien und Gruppen LXXXVI
Tabelle 45 Kruskal-Wallis-Test Vergleich der Entscheidungszeiten in Sekunden zwischen den Gruppen LXXXVII
Tabelle 46 *Mann-Whitney-U-Test Vergleich der Entscheidungszeiten zwischen den Gruppen* LXXXVIII
Tabelle 47 *Mann-Whitney-U-Test Vergleich der Entscheidungszeiten zwischen den Gruppen A und B* LXXXIX
Tabelle 48 *Mann-Whitney-U-Test Vergleich der Entscheidungszeiten zwischen den Gruppen A und C* XCI
Tabelle 49 *Mann-Whitney-U-Test Vergleich der Entscheidungszeiten zwischen den Gruppen A und D* XCII
Tabelle 50 *Mann-Whitney-U-Test Vergleich der Entscheidungszeiten zwischen den Gruppen B und C* XCIV
Tabelle 51 Mann-Whitney-U-Test Vergleich der Entscheidungszeiten zwischen den Gruppen B und D XCV
Tabelle 52 *Mann-Whitney-U-Test Vergleich der Entscheidungszeiten zwischen den Gruppen C und D* XCVII
Tabelle 53 *Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen* XCVIII
Tabelle 54 *Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen nach Gruppen* XCIX
Tabelle 55 *Kruskal-Wallis-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppen* XCIX
Tabelle 56 *Mann-Whitney-U-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppe A und B* CI
Tabelle 57 *Mann-Whitney-U-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppe A und C* CIII
Tabelle 58 *Mann-Whitney-U-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppe A und D* CIV
Tabelle 59 *Mann-Whitney-U-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppe B und C* CVI
Tabelle 60 *Mann-Whitney-U-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppe B und D* CVIII
Tabelle 61 *Mann-Whitney-U-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppe C und D* CIX
Tabelle 62 *T-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppen A und B* CXI
Tabelle 63 *T-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppen A und C* CXII
Tabelle 64 *T-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppen A und D* CXIII
Tabelle 65 *T-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppen B und C* CXIV

Tabelle 66 *T-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppen B und D* CXV
Tabelle 67 *T-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppen C und D* CXVI
Tabelle 68 *Fixationszeiten auf Symbol, Text und Skala nach Gruppen* CXVII
Tabelle 69 *Kruskal-Wallis-Test Vergleich der Fixationszeiten auf Symbol, Text und Skala zwischen den Gruppen* CXVII
Tabelle 70 *Mann-Whitney-U-Test Vergleich der Fixationszeiten zwischen Gruppe A und B* CXVIII
Tabelle 71 *Mann-Whitney-U-Test Vergleich der Fixationszeiten zwischen Gruppe A und C* CXIX
Tabelle 72 *Mann-Whitney-U-Test Vergleich der Fixationszeiten zwischen Gruppe A und D*.....CXX
Tabelle 73 *Mann-Whitney-U-Test Vergleich der Fixationszeiten zwischen Gruppe B und C* CXXI
Tabelle 74 *Mann-Whitney-U-Test Vergleich der Fixationszeiten zwischen Gruppe B und D*.....CXXII
Tabelle 75 *Mann-Whitney-U-Test Vergleich der Fixationszeiten zwischen Gruppe C und D*.....CXXIII
Tabelle 76 *Fixationszeiten auf die jeweiligen Gebiete nach Gruppen* CXXIV
Tabelle 77 *Kruskal-Wallis-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen* CXXIV
Tabelle 78 *Anzahl der Fixationswechsel auf die jeweiligen Gebiete nach Gruppen* CXXIX
Tabelle 79 *Kruskal-Wallis-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen* CXXIX
Tabelle 80 *Mann-Whitney-U-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen A und B*..... CXXXIV
Tabelle 81 *Mann-Whitney-U-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen A und C*.....138
Tabelle 82 *Mann-Whitney-U-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen A und D* CXLI
Tabelle 83 *Mann-Whitney-U-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen B und C*.....CXLIV
Tabelle 84 *Mann-Whitney-U-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen B und D* CXLVII
Tabelle 85 *Mann-Whitney-U-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen C und D* CL
Tabelle 86 *T-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen* ...CLIII
Tabelle 87 *Auflistung der ausgewählten Applikationen mit den entsprechenden Häufigkeiten*.....CLIX
Tabelle 88 *Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Gruppen* CLXII
Tabelle 89 *Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala*.CLXII
Tabelle 90 *Kruskal-Wallis-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen*.....CLXIII
Tabelle 91 *Mann-Whitney-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen A, B, C (mit Datenschutzskala) und D (ohne Datenschutzskala)*.....CLXV
Tabelle 92 Mann-Whitney-U-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen A und B.....CLXVI
Tabelle 93 *Mann-Whitney-U-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen A und C*.....CLXVIII
Tabelle 94 *Mann-Whitney-U-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen A und D* CLXIX
Tabelle 95 *Mann-Whitney-U-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen B und C*.....CLXXI
Tabelle 96 *Mann-Whitney-U-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen B und D* CLXXII

Tabelle 97 *Mann-Whitney-U-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen C und D* CLXXIV
Tabelle 98 *Spearmann-Rho-Test zwischen den Datenschutzscore der Scenarios und des MUIPCs* CLXXV
Tabelle 99 *Auswertung der Entscheidungsmotive über die gesamte Stichprobe* CLXXVI
Tabelle 100 *Auswertung der Entscheidungsmotive sortiert nach Gruppe A* CLXXVII
Tabelle 101 *Auswertung der Entscheidungsmotive sortiert nach Gruppe B* CLXXVIII
Tabelle 102 *Auswertung der Entscheidungsmotive sortiert nach Gruppe C* CLXXIX
Tabelle 103 *Auswertung der Entscheidungsmotive sortiert nach Gruppe D* CLXXX
Tabelle 104 *Kruskal-Wallis-Test Vergleich des App-Scores nach der Entscheidungsmotive zwischen den Gruppen* CLXXXI
Tabelle 105 *Mann-Whitney-U-Test Vergleich Gruppe 1 und 2* CLXXXIII
Tabelle 106 *Mann-Whitney-U-Test Vergleich Gruppe 1 und 3* CLXXXIV
Tabelle 107 *Mann-Whitney-U-Test Vergleich Gruppe 2 und 3* CLXXXV
Tabelle 108 *Bekanntheit der ausgewählten Applikation* CLXXXVII
Tabelle 109 *Bekanntheit der ausgewählten Applikation nach Gruppen getrennt* CLXXXVII
Tabelle 110 *Bewertung der Datenschutzskala* CXC
Tabelle 111 *Kruskal-Wallis-Test Vergleich der Bewertung der Datenschutzskala zwischen den Gruppen* CXCI
Tabelle 112 *Mann-Whitney-U-Test Vergleich der Bewertung der Datenschutzskala zwischen den Gruppen A und B* CXCV
Tabelle 113 *Mann-Whitney-U-Test Vergleich der Bewertung der Datenschutzskala zwischen den Gruppen A und C* CXCIX
Tabelle 114 *Mann-Whitney-U-Test Vergleich der Bewertung der Datenschutzskala zwischen den Gruppen B und C* CCII
Tabelle 115 *Einfachheit der Auswahl und Vertrauenswürdigkeit der Applikation geteilt nach Gruppen* CCV
Tabelle 116 *Kruskal-Wallis-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikation zwischen den Gruppen* CCVI
Tabelle 117 *Mann-Whitney-U-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikation zwischen den Gruppen A und B* CCXI
Tabelle 118 *Mann-Whitney-U-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikation zwischen den Gruppen A und C* CCXV
Tabelle 119 *Mann-Whitney-U-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikation zwischen den Gruppen A und D* CCXVIII
Tabelle 120 *Mann-Whitney-U-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikation zwischen den Gruppen B und C* CCXXI
Tabelle 121 *Mann-Whitney-U-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikation zwischen den Gruppen B und D* CCXXIV
Tabelle 122 *Mann-Whitney-U-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikation zwischen den Gruppen C und D* CCXXVII
Tabelle 123 *T-Test Vergleich der Vertrauenswürdigkeit der Applikation Messenger zwischen den Gruppen* CCXXX
Tabelle 124 *T-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikation E-Mail, Fitness und Spiele, zwischen den Gruppen B und D* CCXXXII
Tabelle 125 *Häufigkeiten der Einschätzung der Vertrauenswürdigkeit durch die erste Methode (gestauchte Reskalierung)* CCXXXIII
Tabelle 126 *Häufigkeiten der Einschätzung der Vertrauenswürdigkeit durch die zweite Methode (prozentuale Reskalierung)* CCXXXIII
Tabelle 127 *Häufigkeiten der Einschätzung der Vertrauenswürdigkeit durch die dritte Methode (dividierte Reskalierung)* CCXXXIII

Tabelle 128 *Häufigkeit der Differenzen unter Verwendung der ersten Methode (gestauchte Reskalierung)* CCXXXIV
Tabelle 129 *Häufigkeit der Differenzen unter Verwendung der zweiten Methode (prozentuale Reskalierung)* CCXXXVI
Tabelle 130 *Häufigkeit der Differenzen unter Verwendung der dritten Methode (dividierte Reskalierung)* CCXL
Tabelle 131 *Mittelwerte der Beträge der Differenzen zwischen der angegebenen Vertrauenswürdigkeit und der angegebenen Aggressivität durch die Datenschutzskala unter Verwendung der ersten Methode (gestauchte Reskalierung)* CCXLVII
Tabelle 132 *Mittelwerte der Beträge der Differenzen zwischen der angegebenen Vertrauenswürdigkeit und der angegebenen Aggressivität durch die Datenschutzskala unter Verwendung der zweiten Methode (prozentuale Reskalierung)* CCXLVIII
Tabelle 133 *Mittelwerte der Beträge der Differenzen zwischen der angegebenen Vertrauenswürdigkeit und der angegebenen Aggressivität durch die Datenschutzskala unter Verwendung der dritten Methode (dividierte Reskalierung)* CCXLIX
Tabelle 134 *Kruskal-Wallis-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppen (gestauchte Reskalierung)* CCL
Tabelle *135 Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und B (gestauchte Reskalierung)* CCLII
Tabelle 136 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und C (gestauchte Reskalierung)* CCLIV
Tabelle *137 Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und D gestauchte (Reskalierung)* CCLVI
Tabelle 138 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe B und C (gestauchte Reskalierung)* CCLVII
Tabelle 139 Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe B und D (gestauchte Reskalierung) CCLIX
Tabelle 140 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe C und D (gestauchte Reskalierung)* CCLXI
Tabelle 141 *Kruskal-Wallis-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppen (prozentuale Reskalierung)* CCLXIII
Tabelle 142 Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und B (prozentuale Reskalierung) CCLXV
Tabelle 143 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und C (prozentuale Reskalierung)* CCLXVII
Tabelle 144 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und D (prozentuale Reskalierung)* CCLXVIII
Tabelle 145 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe B und C (prozentuale Reskalierung)* CCLXX
Tabelle 146 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe C und D (prozentuale Reskalierung)* CCLXXI
Tabelle 147 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe B und D (prozentuale Reskalierung)* CCLXXIII
Tabelle 148 *T-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und B, den Gruppen A und C, den Gruppen A und D (prozentuale Reskalierung)* CCLXXIV
Tabelle 149 *Kruskal-Wallis-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppen (dividierte Reskalierung)* CCLXXVI
Tabelle 150 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und B (dividierte Reskalierung)* CCLXXVIII

Tabelle 151 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und C (dividierte Reskalierung)* CCLXXIX
Tabelle 152 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und D (dividierte Reskalierung)* CCLXXXI
Tabelle 153 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe B und C (dividierte Reskalierung)*.....CCLXXXII
Tabelle 154 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe C und D (dividierte Reskalierung)* CCLXXXIII
Tabelle 155 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe B und D (dividierte Reskalierung)* CCLXXXV
Tabelle 156 *T-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppen (dividierte Reskalierung)*.....CCLXXXVII
Tabelle 157 *Korrelation zwischen der Technikaffinität und der Adäquatheit der angegebenen Vertrauenswürdigkeit*..... CCXCII
Tabelle 158 *Korrelation zwischen dem Alter und der Adäquatheit der angegebenen Vertrauenswürdigkeit*..... CCXCII
Tabelle 159 *Korrelation zwischen dem Geschlecht und der Adäquatheit der angegebenen Vertrauenswürdigkeit*..... CCXCIII
Tabelle 160 *Korrelation zwischen dem höchsten Bildungsabschluss und der Adäquatheit der angegebenen Vertrauenswürdigkeit* CCXCIII
Tabelle 161 *Korrelation zwischen dem Stunden der Handynutzung und der Adäquatheit der angegebenen Vertrauenswürdigkeit* CCXCIV
Tabelle 162 *Korrelation zwischen der Privatsphäre und der Adäquatheit der angegebenen Vertrauenswürdigkeit*..... CCXCIV
Tabelle 163 *Ergebnisse zur Messung der Bedenken von Mobilfunknutzern hinsichtlich des Datenschutzes (MUIPC)*..... CCXCV
Tabelle 164 Ergebnisse zur Messung der Bedenken von Mobilfunknutzern hinsichtlich des Datenschutzes (MUIPC)..... CCXCVI
Tabelle 165 *Mittelwerte der Relevanz der Bewertungsmethoden einer Applikation für die Applikationsauswahl* CCXCVII
Tabelle 166 *Friedman-Test Vergleich der verschiedenen Applikationsbewertungsmethoden untereinander*..... CCXCVIII
Tabelle 167 *Wilcoxon-Test paarweise Vergleich der verschiedenen Applikationsbewertungsmethoden untereinander*..... CCXCVIII
Tabelle 168 *Kruskal-Wallis-Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen*..... CCCII
Tabelle 169 *Mann-Whitney-U-Test Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen A und B* CCCIII
Tabelle 170 *Mann-Whitney-U-Test Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen A und C* CCCV
Tabelle 171 *Mann-Whitney-U-Test Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen A und D* CCCVI
Tabelle 172 *Mann-Whitney-U-Test Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen B und C*..... CCCVIII
Tabelle 173 *Mann-Whitney-U-Test Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen C und D* CCCIX
Tabelle 174 *Mann-Whitney-U-Test Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen B und D* CCCX
Tabelle 175 *T-Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen* CCCXII

Tabelle 176 *Angemessenheit der Applikationsauswahl (Datenschutzscore)* CCCXVI
Tabelle 177 *Spearman-Rho-Test zwischen den Datenschutzscore der Scenarios und des MUIPCs* CCCXVII
Tabelle 178 *Demographische Daten Alter und Geschlecht* CCCXL
Tabelle 179 *Demographische Daten Bildung* CCCXL
Tabelle 180 *Tägliche Handynutzung in Stunden* CCCXL
Tabelle 181 *Technikaffinität* CCCXL
Tabelle 182 *Wichtigkeit der Privatsphäre* CCCXL
Tabelle 183 *Häufigkeiten des Schutzes der persönlichen Daten* CCCXLI
Tabelle 184 *Mittelwerte zu Bewertung der „Maybe"-Option* CCCXLI
Tabelle 185 *Häufigkeiten der Dauer der Zugriffsberechtigung* CCCXLII
Tabelle 186 *Häufigkeiten zu Bewertung der „Maybe"-Option* CCCXLII
Tabelle 187 *Häufigkeiten der Berechtigungen bei denen die temporäre Zugriffsberechtigung genutzt werden würden* CCCXLIII
Tabelle 188 *Häufigkeiten der Verbesserungsvorschläge für die temporäre Zugriffsberechtigung* CCCXLIII
Tabelle 189 *Häufigkeiten der alltäglichen Situationen in denen der temporäre Zugriffsberechtigung genutzt wird* CCCXLIV
Tabelle 190 *Häufigkeiten der ersten Eindrucke über die temporäre Zugriffsberechtigung* CCCXLIV
Tabelle 191 *Häufigkeiten der Nutzung der temporären Zugriffsberechtigung* CCCXLIV
Tabelle 192 *Häufigkeiten des Verständnisses über die temporäre Zugriffsberechtigung* CCCXLV
Tabelle 193 *Häufigkeiten der Gründe für die Verwendung der temporären Zugriffsberechtigung* CCCXLV
Tabelle 194 *Häufigkeiten der Angemessenheit der Dauer der temporären Zugriffberechtigung* CCCXLV
Tabelle 195 *Zusammenhang zwischen Auffallen der „Maybe"-Option und den gefallen der „Maybe"-Option sowie der Wichtigkeit der Kontrolle der persönlichen Daten* CCCXLVI
Tabelle 196 *Zusammenhang zwischen der Wichtigkeit der Privatsphäre und den Aussagen der ersten Frage bezüglich der „Maybe"-Option* CCCXLVI
Tabelle 197 *Zusammenhang zwischen der Dauer der erteilten Zugriffsberechtigung und den zweiten bis vierten Aussagen der ersten Frage bezüglich der „Maybe"-Option* CCCXLVII
Tabelle 198 *Zusammenhang zwischen der technischen Affinität und den Aussagen der ersten Frage bezüglich der „Maybe"-Option* CCCXLVII
Tabelle 199 *Zusammenhang zwischen der Handynutzung und den zweiten bis vierten Aussagen der ersten Frage bezüglich der „Maybe"-Option* CCCXLVIII
Tabelle 200 *Zusammenhang zwischen dem Alter und den Aussagen der ersten Frage bezüglich der „Maybe"-Option* CCCXLVIII
Tabelle 201 *Zusammenhang zwischen der technischen Affinität und dem Handynutzung* CCCXLIX
Tabelle 202 *Häufigkeiten der gewählten Optionen getrennt nach der Berechtigungsart* CCCXLIX
Tabelle 203 *Häufigkeiten der gewählten Optionen insgesamt* CCCL
Tabelle 204 *Häufigkeiten der ausgewählten Dauer der temporären Zugriffsberechtigung* CCCLI
Tabelle 205 *Durchschnittliche Dauer der temporären Zugriffsberechtigung getrennt nach der Berechtigungsart* CCCLI
Tabelle 206 *Zusammenhang zwischen der Wichtigkeit der Privatsphäre und der gewählten Optionen* CCCLI
Tabelle 207 *Durchschnittliche Auswahl der Optionen auf die angefragte Zugriffsberechtigung* CCCLI
Tabelle 208 *Durchschnittliche Auswahl der Optionen auf die angefragte Zugriffsberechtigung getrennt nach Nutzen der „Maybe"-Option* CCCLII
Tabelle 209 *Mann-Whitney-U-Test Vergleich der durchschnittlichen Auswahl der Optionen auf die angefragte Zugriffsberechtigung getrennt nach Nutzen der „Maybe"-Option* CCCLII

Abbildungsverzeichnis

Abbildung 1. Flussdiagramm des ersten empirischen Versuchs bezüglich des Umgangs mit persönlichen Daten. 42
Abbildung 2. Verteilung des Geschlechtes der Stichprobe. 53
Abbildung 3. Vergleich der Lesedauer zwischen den unterschiedlichen Präsentationsformen. 55
Abbildung 4. Vergleich der gemessenen, angegebenen und abgefragten Zeiten zum Lesen der Teilnahmevereinbarungen. 58
Abbildung 5. Verteilung der Antworten zu den sozialen Repräsentationen. 59
Abbildung 6. Absolute Häufigkeiten der von den Teilnehmenden angegebenen Vergütung. 62
Abbildung 7. Absolute Häufigkeiten der Teilnehmenden, welche angaben, die Teilnahmevereinbarung gelesen, nicht gelesen oder überflogen zu haben. 65
Abbildung 8. Absolute Häufigkeiten der von den Teilnehmenden angegebenen Auffälligkeiten in den Teilnahmevereinbarungen. 66
Abbildung 9. Kategorien, der auf dem eigenen mobilen Endgerät am häufigsten verwendeten Applikationen. 68
Abbildung 10. Kategorien der Applikationen, denen auf dem eigenen mobilen Endgerät am meisten misstraut wird. 69
Abbildung 11. Prozentuale Häufigkeiten der angegebenen Konsequenzen der Weitergabe von persönlichen Daten. 74
Abbildung 12. Durchschnittlicher Stellenwert des Schutzes persönlicher Daten. 76
Abbildung 13. Flussdiagramm des zweiten empirischen Versuchs bezüglich der Datenschutzskala. ..101
Abbildung 14. Änderung der Berechtigungsanfragen und der Berechtigungsnutzung vor und nach Inkrafttreten der DSGVO (N. Momen et al., 2019). 110
Abbildung 15. Vergleich zwischen den deklarierten und genutzten Berechtigungen vor und nach Inkrafttreten der DSGVO. (N. Momen et al., 2019). 111
Abbildung 16. a) Startbildschirm des prototypisierten App-Marktes mit Datenschutzskala und b) Auflistung der Applikationen nach der Suche. 121
Abbildung 17. Applikation nach Auswahl vor der Installation. 137
Abbildung 18. Verteilung des Geschlechtes, des Alter, der Bildung und der Handynutzung der Stichprobe. 147
Abbildung 19. Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Gruppen sowie nach der Präsenz einer Datenschutzskala. 158
Abbildung 20. Entscheidungsmotive für die Auswahl der Applikationen über die Stichprobe N = 82. 162
Abbildung 21. Bewertung der Datenschutzskala. 169
Abbildung 22. a) Bildschirmabzug des Dialogfensters zur Abfrage der Zugriffsberechtigung mit Implementierung der temporären Option, b) der Oberfläche der Nachrichtenapplikation und c) den Einstellungen zur Bestimmung der Zeitspanne für die die Zugriffsberechtigung erteilt wird. 225
Abbildung 23. Flussdiagramm des dritten empirischen Versuchs bezüglich der Datenschutzskala. ..226
Abbildung 24. Flussdiagramm des Zugriffkontrollmodells mit Implementierung der temporären Zugriffsberechtigung, dargestellt nach N. Momen et al. (2020). 228
Abbildung 25. Flussdiagramm der Funktionsweise der temporären Zugriffsberechtigung, dargestellt nach N. Momen et al. (2020). 229
Abbildung 26. Verteilung des Geschlechtes, des Alter, der Bildung und der Handynutzung der Stichprobe. 239
Abbildung 27. Verteilung der gewünschten Dauer der temporären Zugriffsberechtigung. 242
Abbildung 28. Bubble-Scale. LV

Abbildung 29. Smiley-Scale. LV
Abbildung 30. Label-Scale. LVI
Abbildung 31. Arrow-Bar-Scale. LVI
Abbildung 32. Arrow-Speedometer-Scale. LVII
Abbildung 33. Lock Scale. LVII
Abbildung 34. Mask Scale. LVIII
Abbildung 35. Beispielhafte Darstellung des Online-Fragebogens. LIX
Abbildung 36. Beschreibung der Datenschutzskala mit Diagramm zur Abfrage der Rechte und Freigabe persönlicher Daten. LXI
Abbildung 37. Bildschirmabzug der A-Ware Applikation. LXXVI
Abbildung 38 Entscheidungsmotive in den ursprünglichen Gruppe A-D des Laborexperimentes CCCXIX
Abbildung 39 Hypothesenübersicht zum ersten Versuch CCCLIX
Abbildung 40 Hypothesenübersicht zum zweiten Versuch CCCLX
Abbildung 41 Hypothesenübersicht zum dritten Versuch CCCLXI

1 Einleitung

„Ich akzeptiere“. Das sind jene Worte, mit denen man am Ende einer Onlinetransaktion konfrontiert wird. Dabei spielt es keine Rolle, ob es sich um den Erwerb eines physischen Gegenstandes oder einer Applikation handelt. In jedem Fall ist die Zustimmung der Einverständniserklärung erforderlich. Oft ist diese in umschweifender und komplizierter juristischer Sprache verfasst, sodass nur die wenigsten Endverbrauchenden im Stande sind, diese zu verstehen. Infolgedessen sind sich die Endverbrauchenden über das Ausmaß, in dem ihre Daten und Rechte genutzt werden, nicht bewusst und auch über die damit verbundenen Konsequenzen im Unklaren. Vor allem im gegenwärtigen Zeitalter der Digitalisierung, in dem 91,9 % der privaten Haushalte über einen eigenen Computer verfügen (Statistisches Bundesamt, 2020), 81,7 % der Bevölkerung (Bitkom, 2019) in Deutschland ein Smartphone und 58 % ein Tablet besitzen (Bitkom, 2020), sollte der Thematik der Datensicherheit ein hoher Stellenwert zugeschrieben werden. Dies spiegelt sich auch in der Anzahl der heruntergeladenen Applikationen wider. Allein im Vereinigten Königreich, in Frankreich und in Deutschland wurden im Jahre 2016 sechs Milliarden Applikationen aus dem App und Play Store heruntergeladen (Priori Data, 2017).

Viele Unternehmen betreiben einen hohen finanziellen Aufwand, um die Daten von Nutzenden zu sammeln und zu analysieren. Der Wert dieser Daten nimmt aufgrund der hohen Nachfrage stetig zu, da Unternehmen immer stärker ein One-to-One-Marketing anstreben, welches die individuelle Kundenadressierung beinhaltet und zusätzliche Informationen über das Nutzerverhalten akquiriert werden (Baeriswyl, 2000). Verschiedene Konzepte und Techniken steigern die Effizienz und ermöglichen zielgerichtete Marketingstrategien und Vertriebsprogramme.

Das Sammeln von Nutzer- und Kundendaten begann mit der Einführung von Kundenkarten, mit denen das Kaufverhalten jeder einzelnen Person verfolgt wird. Ziel ist es, das Verbraucherverhalten einer Person so zu beeinflussen, dass sie die Produkte, welche von dem Unternehmen angeboten werden, erwirbt. Zusätzlich zu dem Verbraucherverhalten werden Persönlichkeitsprofile angelegt, welche es unter anderem ermöglichen, die Kreditwürdigkeit bestimmter Personen in Kenntnis zu bringen. Mit dem zunehmenden Sammeln und Evaluieren spezifischer und personenbezogener Daten wurde es immer wichtiger, Maßnahmen zu ergreifen, um die Daten zu schützen (Baeriswyl, 2000). Nach einer Umfrage in den Vereinigten Staaten von Amerika aus dem Jahr 2000 glauben 75 % der Bevölkerung, dass sie keine vollständige Kontrolle mehr über ihre persönlichen Daten haben und sehen sich selbst als gläserne Konsumenten, welche der Manipulation durch Unternehmen ausgeliefert sind. Darüber hinaus war die Mehrheit der Befragten der Meinung, dass Unternehmen zu viele persönliche Informationen verwalten würden (Reidenberg, 1997). Mit der Zunahme von gesammelten Daten und

verbesserten analytischen Möglichkeiten ist ein zunehmend detaillierterer Kontrollprozess des Individuums seitens der Unternehmen möglich. Hierzu trägt auch das Warehousing-Konzept aktiv bei, welches eine funktions- und zeitgerechte Verfügung der Kundendaten zum Ziel hat (Baeriswyl, 2000).

Ein auffallendes Verhalten der Endnutzenden ist die starke Abneigung gegen die staatliche Vorratsdatenspeicherung, während jedoch unzählige persönliche Daten und Ablichtungen freiwillig auf private Datenzentren hochgeladen werden, ohne dass hierfür eine Notwendigkeit besteht (M. Schmidt, 2015). Ein gutes Beispiel hierfür ist die Nutzung von Social Media Plattformen wie Facebook und anderen. Die Weitergabe des Kaufverhaltens, welches durch die Kreditkarte aufgezeichnet wird oder das Bewegungsprofil, das durch Fluggesellschaften oftmals an dritte Unternehmen weitergegeben wird, sollte im Datenschutzgesetz kritisch betrachtet werden.

In früheren Zeiten stand man der Fusionierung von Banken und Versicherungen sehr skeptisch gegenüber (Baeriswyl, 2000), da persönliche Patienteninformationen in den Bankensektor flossen. Gleichzeitig konnte hierbei jedoch die Kundenfreundlichkeit gesteigert werden. Eine ähnliche Entwicklung, die Diversifizierung der Angebote innerhalb einer Firma, kann heutzutage bei den führenden Anbietern für Internetdienstleistungen beobachtet werden. Als Beispiel kann hierfür die Google LLC herangezogen werden, welche nicht mehr nur als reine Suchmaschine angesehen werden darf. Nach dem Aufkauf und den Gründungen vieler Tochterunternehmen tangiert Google mittlerweile das Leben der Nutzenden in vielen Bereichen. Dies hat zum Vorteil, dass die verschiedenen Dienste auf die Person individuell abgestimmt werden können, indem sie untereinander Informationen austauschen und ergänzen. Dabei wird das Nutzerprofil immer vollständiger, da Daten aus den verschiedensten Lebensbereichen gesammelt und gemeinsam analysiert werden können. Dies ermöglicht dem Unternehmen ein sehr detailliertes Bild über die Nutzenden zu bekommen, welches das Unternehmen einerseits für sich selbst nutzen, andererseits gegen einen finanziellen Wert an dritte Unternehmen aushändigen kann. Heutzutage bietet Google unter anderem ein E-Mail-Postfach (GoogleMail), eine Video Sharing Plattform (YouTube), einen Datenspeicher (GoogleDrive) sowie Satellitenbilder (GoogleEarth/ GoogleMaps) an. Zusätzlich zu diesen Dienstleistungen vertreibt das Unternehmen auch eigene Computer (Chromebook) und Smartphones (Nexus Serien). Das Betriebssystem Android, welches ebenfalls von Google entwickelt wurde, erschließt einen Marktanteil von über 70 % in Deutschland (Kantar, 2020). Heutzutage erweist es sich als Herausforderung, die Dienstleistungen jener Unternehmen nicht zu nutzen, weil die populärsten Dienste von wenigen großen Unternehmen stammen. Somit ist der Besitz eines Smartphones meist mit der Offenlegung von persönlichen Informationen an große Unternehmen verbunden.

1.1 Aufgabenstellung

Im Fokus der ersten Studie dieser Dissertation steht die Erhebung des Bewusstseins der Endnutzenden mobiler Endgeräte über die Weitergabe persönlicher Daten an Dritte. Dabei soll unter anderem untersucht werden, ob die Teilnehmenden Kenntnis über den Datentransfer und deren Konsequenzen beim Nutzen dieser Geräte verfügen. Zusätzlich soll ein Fragebogen über die subjektive Relevanz des Problems durchgeführt werden. Hiermit soll ermittelt werden, ob Nutzende das Gefühl haben, in ihren Rechten verletzt worden zu sein und falls dies der Fall ist, soll in einem folgenden Schritt eruiert werden, wie schwerwiegend die Verwendung und die Weitergabe ihrer Daten eingestuft wird. Ziel ist es zu verstehen, wie wichtig den Nutzenden der Schutz ihrer Rechte ist. Um dies zu ermöglichen, wird in einer ersten Studie ein Experiment gestaltet, welches dazu dient, die Freizügigkeit von Versuchspersonen im Hinblick auf die Weitergabe ihrer Daten zu untersuchen. Dabei müssen die Teilnehmenden abwägen, ob sie ihre Daten für eine finanzielle Gegenleistung aushändigen. Ergänzend soll ermittelt werden, welchen finanziellen Aufwand die Versuchspersonen gewillt sind aufzuwenden, um einen gewissen Grad an Sicherheit und Schutz ihrer Daten zu erlangen.

In einer zweiten Studie soll anschließend eine Lösung gefunden werden, den Nutzenden mobiler Endgeräte zu ermöglichen, einzusehen, wie häufig Applikationen auf einzelne Daten bzw. Zugriffsberechtigungen zugreifen. Hierfür sollen zunächst 80 Applikationen in den Kategorien Messenger, Videokonferenzen, Wetter, E-Mail, Musik, Fitness, Spiele und Nachrichten über einen Zeitraum von sechs Monaten auf ihre Aktivitäten besonders im Standby-Modus überwacht werden. Anschließend gilt es, im Rahmen einer Fokus-Gruppe möglichst leicht verständliche und intuitive Illustrationen für eine Datenschutzskala zu entwerfen und diese anschließend von Teilnehmenden auf verschiedene Attribute beurteilen zu lassen. Ferner soll mit den gesammelten Daten anschließend eine Datenschutzskala erstellt werden, welche die Applikationen in verschiedene Kategorien einsortiert und den Endnutzenden somit ermöglicht, eine datenschutzfreundliche Auswahl zu treffen. Der Einfluss dieser Datenschutzskala soll in einem breiteren umfangreichen empirischen Experiment untersucht werden, indem unterschiedliche Stichproben mit verschiedenem Informationsgehalt über die Aggressivität der Applikation (Anzahl und Häufigkeit der Nutzung der Zugriffsberechtigung) eine Reihe von Aufgaben erfüllen soll. Um diese Aufgaben zu bewältigen, wird es von Nöten sein, stets eine neue Applikation aus dem App-Markt herunterzuladen. Dabei soll untersucht werden, ob die Implementierung einer Datenschutzskala Auswirkungen auf die Applikationsauswahl hat. Ferner soll eruiert werden, ob die Datenschutzskala einer Erläuterung bedarf oder ohne diese richtig interpretiert wird. Auch die Akzeptanz und der Bedarf der Datenschutzskala soll im Rahmen dieses Versuches erhoben werden.

In der dritten Studie wird nach einer Lösung gesucht, den Endnutzenden die Möglichkeit zu geben, die Zugriffsberechtigung von Applikationen zeitlich zu beschränken. Derzeit ist es den Endnutzenden lediglich möglich, den Zugriffsberechtigungen auf unbestimmte Zeit zuzustimmen oder diese abzulehnen und die Applikation nicht zu nutzen. Im Rahmen der dritten Studie soll neben dem Akzeptieren und dem Ablehnen der Zugriffsberechtigung eine dritte Option implementiert werden, welche eine temporäre Zustimmung beinhaltet. So sollen die Applikationen die Zugriffsberechtigung lediglich für den Zeitraum erhalten, für den sie benötigt werden, um ihre primären Funktionen auszuführen. Nach einem bestimmten Zeitraum, der von den Nutzenden festgelegt wird, sollen die vergebenen Zugriffsberechtigungen widerrufen werden. Versucht die Applikation anschließend erneut auf die Daten zuzugreifen, so folgt eine wiederholte Anfrage zur Vergabe der Zugriffsberechtigung. Ziel der dritten Studie ist es, zu eruieren, ob die Funktion einer temporären Zugriffsberechtigung von den Endnutzenden gewollt ist und benutzt werden würde. Hierfür soll eine Applikation entworfen werden, in der diese temporäre Zugriffsberechtigung als Mock-Up implementiert werden soll. Anschließend soll diese Applikation von den Teilnehmenden dieser Studie heruntergeladen und installiert werden. Während einer Zeitspanne von zehn Tagen werden den Teilnehmenden verschiedene Aufgaben zugesandt, die der Zustimmung einer Zugriffsberechtigung bedürfen. Hierbei soll darauf geachtet werden, ob die Funktion der temporären Zugriffsberechtigungen genutzt wird, welche Schwächen diese Funktion aufweist und was nötig wäre, um die Funktion im alltäglichen Gebrauch zu implementieren.

Der Aufbau und die Durchführung der drei empirischen Versuche wurden jeweils von der Ethik-Komission des Instituts für Psychologie und Arbeitswissenschaften (IPA) geprüft und genehmigt.

1.2 Gliederung

Das **erste Kapitel** dieser Dissertation schildert kurz das vorliegende Problem des Aushändigens und der Weitergabe von persönlichen Daten in alltäglichen Situationen und deren Monetarisierung durch große Unternehmen vor allem im digitalen Dienstleistungsbereich. Anschließend werden die Aufgabenstellungen vorgestellt, welche im Rahmen von drei umfangreichen Studien durchgeführt wurden. Dabei werden mit der ersten Studie die Ursachen für das freizügige Verhalten gegenüber der Weitergabe von persönlichen Daten an Dritte seitens der Endnutzenden untersucht, während in der zweiten und dritten Studie Lösungen für das Aufzeigen eines datenschutzfreundlicheren Verhaltens entwickelt und evaluiert werden.

Im **zweiten Kapitel** werden die wichtigsten Begriffe innerhalb der Dissertation definiert und erläutert. Dazu gehören beispielsweise der Datenschutz, die Privatsphäre der Daten, die invasiven Applikationen sowie die EU-Datenschutzverordnung. In der zweiten Hälfte dieses Kapitels werden die grundlegenden Zusammenhänge der eben erwähnten Begrifflichkeiten erläutert und im Kontext des Datenschutzes eingeordnet. So wird hier aufgezeigt, wo das Sammeln von Nutzerdaten seinen Anfang hatte, wie es heute durchgeführt wird, wie die Nutzenden damit umgehen und welche Meinung sie über den Umgang mit ihren persönlichen Daten haben. Ferner wird genauer betrachtet, welche Konsequenzen die Weitergabe von persönlichen Daten, wie z.B. das Kaufverhalten, für die Endnutzenden hat. Darüber hinaus werden verschiedene Strategien zur Schaffung von Privatsphäre und datenschutzrechtliche Bedenken beim Herunterladen von Applikationen vorgestellt.

Im **dritten Kapitel** werden bereits entwickelte und evaluierte Lösungen zum Schutz der Daten und der Privatsphäre der Endnutzenden präsentiert. Allgemein bilden das zweite und dritte Kapitel die theoretischen Grundlagen für die Forschungsfragen der drei folgenden Versuche.

Das **vierte Kapitel** dieser Dissertation umfasst den ersten empirischen Versuch zum Umgang mit persönlichen Daten und der Weitergabe seitens der Endnutzenden. Diesbezüglich wurde ein Täuschungsexperiment entwickelt, durchgeführt und ausgewertet, in dem untersucht werden sollte, wie die Nutzenden mit ihren persönlichen Daten umgehen und was die Gründe dafür sein könnten.

Das **fünfte Kapitel** beinhaltet den zweiten empirischen Versuch zum Einfluss einer Datenschutzskala auf das Auswahlverhalten in einem App-Markt. Hierfür wurden Zugriffsanfragen diverser Applikationen gesammelt und eine speziell für das Experiment entworfene Datenschutzskala in einem prototypisierten App-Markt implementiert.

Das **sechste Kapitel** behandelt die Akzeptanz und Verwendung einer temporären Zugriffsberechtigung. Dabei wurde eine Applikation entwickelt, welche neben den Optionen „Akzeptieren“ und „Ablehnen“ über eine weitere Funktion der temporären Zugriffsberechtigung verfügt. Diese Applikation fand anschließend Verwendung in dem dritten empirischen Versuch, welcher den Umgang mit dieser weiteren Option näher betrachtet.

Die drei empirischen Experimente sind ähnlich aufgebaut:

Zunächst werden die Forschungsfragen aus der Theorie in Kapitel 2 und 3 formuliert, um anschließend Hypothesen zu bilden. Danach wird das Versuchsdesign vorgestellt und die Untersuchungsvariablen definiert. Nachfolgend werden die nötigen Schritte zur Versuchsvorbereitung, wie z.B. das Entwerfen von Programmen oder die Erstellung von Fragebögen beschrieben, um daraufhin den Aufbau bzw. die

Durchführung des Versuchs vorzustellen. Weiterhin wird die Datenaufbereitung, also die Methodik zur Formatierung und Zusammenfassung der Rohdaten näher beschrieben, um diese anschließend statistisch auswerten zu können. Schließlich werden die Ergebnisse vorgestellt, um diese anschließend zu diskutieren. Daraufhin folgt ein Überblick von den Problemen, die während des Versuches oder dessen Auswertung entstanden sind und wie diese gelöst wurden bzw. zukünftig gelöst werden könnten. Abschließend erfolgt ein Fazit, welches die Problematik beschreibt, den Lösungsweg schildert und die Ergebnisse aufzeigt.

Das **siebte Kapitel** beinhaltet ein versuchsübergreifendes Fazit, welches die drei Studien miteinander verbindet, sodass verdeutlicht wird, wie die Erkenntnisse der vorrangegangenen Studien in die darauffolgenden eingeflossen sind.

2 Grundlagen und Definitionen

Im folgenden Abschnitt wird die Theorie und somit die Grundlagen und die Definitionen, auf denen die später postulierten Hypothesen basieren, vorgestellt. Im Abschnitt der Definitionen werden Begriffe erläutert, welche in dieser Dissertation von hoher Relevanz sind. Im Kapitel der Grundlagen werden Verknüpfungen zwischen bestimmten Themenbereichen aufgezeigt, wobei ein besonderer Fokus auf dem Sammeln, der Weitergabe und dem Schutz persönlicher Daten liegt.

2.1 Definitionen

Dieser Abschnitt dient zur Eingrenzung der Begriffe „Datenschutz“ und „Privatsphäre der Daten“. Weiterhin werden unter anderem die Begriffe „mobile Endgeräte“, „Applikation“ und „Betriebssystem“ definiert sowie „EU-Datenschutzgrundverordnung“ erläutert.

2.1.1 Datenschutz

Um eine möglichst valide und standardisierte Definition des Begriffs Datenschutz zu verwenden, wird diese aus dem Bundesdatenschutzgesetz entnommen. Somit wird der Datenschutz folgendermaßen definiert: „Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“ (BDSG, 2015, S. 3). Der Begriff des Datenschutzes beinhaltet somit zwei Bedeutungen. Die erste umfasst den „Schutz der (gespeicherten) Daten und ihrer Verarbeitung vor unerwünschtem Zugriff (vor allem im Sinne von zweckwidrigem Missbrauch) oder Verlust“ (Witt, 2008). Die zweite Bedeutung betrifft den „Schutz des Bürgers vor unerwünschten Folgen (insbesondere durch zweckwidrigen Missbrauch) aufgrund des Zugriffs auf (gespeicherte) Daten bzw. des ungewollten Datenverlusts“ (Witt, 2008). Hieraus ist zu schlussfolgern, dass die erste Bedeutung Voraussetzung für die zweite ist. Darüber hinaus kann von der ersten Sichtweise die Definition der Datensicherheit abgeleitet werden. Die Definition der Datensicherheit umfasst nach Witt den „Schutz der gespeicherten Daten vor Beeinträchtigung durch höhere Gewalt, menschliche oder technische Fehler und Missbrauch“ (Witt, 2008).

Darüber hinaus ist nach Pommerening (1991) bei der Definition des Datenschutzes die Vermeidung von ungewollter Änderung oder Verfälschung von Daten hinzuzufügen. Auch der Schutz der Integrität des Systems, dessen Priorität über der Vertraulichkeit der Daten eingestuft wird, ist Teil der Aufgabe

des Datenschutzes. Ferner ist Pommerening der Meinung, dass ein Bereich des Aufgabenfeldes des Datenschutzes auch den Schutz vor fehlerhaften Daten einschließt (Pommerening, 1991).

2.1.2 Privatsphäre der Daten

Die Privatsphäre im deutschen Raum wird rechtlich gesehen vom Artikel 1 Absatz 1 GG, welcher die Menschenwürde garantiert, sowie von Artikel 2 Absatz 2 GG, welcher die freie Entfaltung der Persönlichkeit gewährleistet, abgeleitet. Im so genannten Volkszählungsurteil des Bundesverfassungsgerichtes von 1983 (15.12.1983) wird festgehalten dass, „[u]nter den Bedingungen der modernen Datenverarbeitung […] der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 GG umfasst [wird]. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

Darüber hinaus unterscheidet Hubmann (1953) zwischen drei Persönlichkeitssphären. Die Geheim- bzw. Intimsphäre bildet die engste Sphäre und umfasst den Schutz der inneren Gedanken- und Gefühlswelt sowie den Schutz des Sexualbereichs. Sie beinhaltet somit einen unantastbaren Bereich privater Lebensgestaltung, der dem Zugriff des Staates entzogen ist. Die Daten bzw. die Informationen der Privatsphäre sind dabei für einen unbestimmten, aber beschränkten Personenkreis zugänglich. Darüberhinausgehende Kreise, sowie die Öffentlichkeit, haben jedoch keinen Zugang. Die Individualsphäre ist rechtlich ungeschützt und beinhaltet unter anderem den Namen, die Ehre und die Rechte am eigenen Bild eines Menschen (Hubmann, 1953).

Hierbei ist zu erwähnen, dass verschiedene Autoren der Meinung sind, es würden mehr unterschiedliche Sphären existieren. Ferner liegen generell einige Kritiken am Ansatz der Sphärentheorie vor (Hugl, 2012).

2.1.3 Mobile Endgeräte

Der Begriff der mobilen Endgeräte beinhaltet alle elektronischen Geräte für die mobile, netzunabhängige Daten-, Sprach- und Bildkommunikation, Navigation, Datenspeicherung und das Mobile Computing. Mobile Endgeräte ermöglichen die mobile Kommunikation und bieten eine Plattform zur Installation und zum Gebrauch mobiler Applikationen (Maske, 2012). Meist kombinieren

mobile Endgeräte mehrere Funktionalitäten in einem Gerät. Beispielsweise sind einige Smartphones im Stande sowohl für Navigationszwecke und Videotelefonie als auch für das mobile Fernsehen genutzt zu werden. Die wohl bekanntesten und weitverbreitetsten mobilen Endgeräte sind Smartphones und Tablets für die Sprach- und Bildkommunikation (Office for National Statistics (UK)., 2019). Vor allem durch die ständige Entwicklung neuer Dienste und Applikationen ist die Funktionalität dieser Geräte um Daten-, Text- und Streaming-Dienste bereichert worden.

Für die Bild- und Videoerfassung sind neben Smartphones auch Digitalkameras sowie Camcorder geeignet. Die Wiedergabe von Video-, Audio, oder Foto-Dateien kann beispielsweise ebenfalls mit einem MP3-, MP4- bzw. einem Multimedia-Player erfolgen.

Die Verarbeitung von Daten kann mit allen Geräten, wie zum Beispiel Handhelds, Palmtops, PDAs, Notebooks, Subnotebooks, Netbooks, Tablets und Hybrid-Computer erfolgen.

Besonders Smartphones enthalten viele verschiedene Funktionen. Durch die heutigen Technologien 3G, LTE und das landesweite WLAN (Stanley, 2010) und die damit zusammenhängende schnelle Datenverbindung werden Smartphones bevorzugt für das Surfen mit Webbrowsern, das Empfangen und Senden von E-Mails, die Nutzung von sozialen Netzwerken, Finanz-, Gesundheits-, und anderen Dienstleistungen genutzt. Darüber hinaus umfasst der Umgang mit Smartphones meist auch die Nutzung von Fotoalben, Spielen, Kalendern und Kontaktlisten. Somit können persönlichere Daten erfasst werden, als es bei der Verwendung von herkömmlichen Computern möglich ist. Darunter fallen zum Beispiel Identitäten, bevorstehende Termine, Zeit, die für verschiedene Apps aufgewendet wurde, persönliche Kontakte, Echtzeitstandorte und weitere. Derzeit nutzen Anbieter leistungsstarke Überwachungstechnologien, um mobile Nutzende zu verfolgen und zu profilieren (Xu et al., 2012).

2.1.4 Betriebssystem

Ein Betriebssystem besteht aus einer Ansammlung von Steuerprogrammen, welche das Benutzen des Computers und daran angeschlossener Geräte für die Nutzenden vereinfachen. Das Betriebssystem ist somit als Verbindung zwischen den Nutzenden und der Hardware zu betrachten, welches die Funktion hat, die spezifischen Aufgaben tatsächlich zu erfüllen. Die Software des Betriebssystems ist in der Lage wesentlich komplexere Operationen durchzuführen, die nur mit der Hardware nicht zu vollbringen wären. Dies vereinfacht es den Nutzenden ein bestimmtes Programm auszuführen oder eines selbst zu schreiben. Über die vereinfachte Ausführung der Benutzerprogramme hinaus ist die Software in der Lage den Gebrauch der verfügbaren Betriebsmittel, wie zum Beispiel den Hauptspeicher, Schnelldrucker etc. zu koordinieren, Fehler in Benutzerprogrammen zu entdecken,

Rechenzeitabrechnungen durchzuführen, Information zu schützen, angemessene Maßnahmen bei Hardwarefehlern einzuleiten und zahlreiche weitere Funktionen zu erfüllen.

Bei den aktuellen Betriebssystemen sind Unterschiede in Bezug auf die von ihnen unterstützte Hardware, die Komplexität und die Art der von ihnen zu erledigenden Aufgaben sehr umfassend. Beispielsweise berechnen einige Betriebssysteme Nutzerprogramme sequenziell nacheinander, während andere Systeme wiederum in der Lage sind mehrere Prozesse und Aufgaben gleichzeitig durchzuführen und somit beispielsweise mehreren Benutzenden die Möglichkeit zu geben einen Rechner über mehrere Terminals gleichzeitig zu nutzen. Weitere Systeme erfüllen die Realzeitanforderungen, welche als Bedingung eine bestimmte Reaktion des Rechners auf ein äußeres Signal in einer vorgegebenen Zeitspanne erfordert oder führen bestimmte vorgegebene Aufgaben an einer sehr hohen Anzahl von Terminals gleichzeitig durch (Coy, 1988).

In dieser Arbeit werden die Betriebssysteme mobiler Endgeräte wie Android und iOS fokussiert, weil diese Betriebssysteme mit einem Marktanteil von 73 % (Android) und 26 % (iOS), den größten Teil des deutschen Marktes abdecken. Diese Angaben beziehen sich auf den Zeitraum Juni 2020 (Kantar, 2020).

2.1.5 Software Rechte

Im folgenden Abschnitt wird das Rechtesystem des Betriebssystems Android näher erklärt. Sämtliche Funktionen und Schnittstellen werden laut Android zunächst für Applikationen von Drittanbietern gesperrt. Erst nachdem die Freigabe von den Nutzenden in Form eines Dialogfensters, welches die angeforderten Zugriffe auflistet, erteilt wurde, ist die Applikation im Stande diese zu nutzen. Dabei ist das Erteilen einzelner Rechte durch die Nutzenden erst seit der Android Version 6.0 (Marshmallow) möglich (Zhauniarovich & Gadyatskaya, 2016). Bei älteren Versionen hingegen erfolgt entweder das Einverständnis mit der Abgabe aller angeforderten Rechte oder die Installation der Applikation wird abgebrochen. Dabei ist es schwierig zu differenzieren welche Rechte für den tatsächlichen Gebrauch der Applikation von Nöten sind und welche nur dazu dienen Informationen über die Endnutzenden zu sammeln. Die Rechte beziehen sich dabei sowohl auf den Zugriff auf Hardwarefunktionen wie die Nutzung der Kamera, die Erfassung der Position über das GPS, sowie die Bluetooth-, Telefon- und Netzwerkfunktion, als auch auf den Zugriff auf Daten, wie die gesammelten Kontakte oder Kalendereinträge (Android Open Source Project o.J.).

2.1.6 Applikationen

Applikationen bzw. Anwendungsprogramme oder auch kurz Apps sind Computerprogramme, die genutzt werden, um eine nützliche oder gewünschte, nicht systemtechnische Funktionalität zu bearbeiten oder zu unterstützen. Die Applikationen dienen somit der Lösung von Benutzerproblemen (Hermann et al., 1993). Im Rahmen dieser Arbeit werden vor allem Applikationen betrachtet, die unter den Betriebssystemen Android oder iOS in den entsprechenden App-Märkten zur Verfügung gestellt werden. Bei den App-Märkten handelt es sich um internetbasierte, digitale Vertriebsplattformen für Softwares, welche entweder vom Betreiber selbst, jedoch überwiegend von Drittanbietern zur Verfügung gestellt werden. Dabei stellen die App-Märkte mittlerweile ein außerordentlich umfangreiches Sortiment an Applikationen zur Verfügung. Derzeit bietet der Google Play Store mehr als 3 Millionen Applikationen zum Herunterladen an (AppBrain, 2020b), wovon etwa 2,6 Millionen kostenfrei waren (AppBrain, 2020a). Die Anzahl der angebotenen Applikationen im Apple App Store lag im Jahr 2019 bei ca. 2 Millionen (Appfigures, 2019), wobei eine Statistik aus dem Jahr 2014 zeigte, dass der Anteil von kostenfreien Applikationen im Apple App Store bei etwa 80 % liegt (Distimo, 2014). Eine manuelle Überprüfung der Applikationen erfolgt bei Apple schon seit Eröffnung der Plattform. Beim Google Play Store erfolgt eine solche Überprüfung erst seit dem Jahr 2015 (Perez, 2015). Hierbei ist anzumerken, dass die Restriktionen seitens Apple sehr viel höher sind als bei Google. Unter anderem versucht Apple pornographisches Material aus seinem Inventar zu verbannen (Apple, 2016).

Obwohl die Nutzenden eine große Anzahl an Applikationen nutzen können um alltägliche Aufgaben zu lösen, führt die Entscheidung der Freigabe von persönlichen Daten, die für den Gebrauch dieser Applikationen erforderlich sind, zu Eingriffen in die Privatsphäre (Acquisti et al., 2015); (Gross & Acquisti, 2005); (J. Watson et al., 2015). Die verschiedenen App-Märkte bieten eine auf Popularität basierende Bewertungsmethode an, welche vor allem auf der Meinung der Nutzenden basiert. Hauptsächlich wird hierbei die Benutzerfreundlichkeit, die Funktionsvielfalt sowie die Funktionalität zur Bewertung der Applikation verwendet (Hatamian et al., 2019). Die Bewertung der Datenschutzfreundlichkeit fließt zu diesem Zeitpunkt nicht in die Bewertungsmethoden ein.

Gu et al. (2017) kategorisiert darüber hinaus in nicht-invasive und invasive Applikationen. Dabei sammeln invasive Applikationen persönliche Informationen, ohne diese für ihre eigentliche primäre Funktion zu benötigen, verwenden diese für nicht autorisierte Zwecke, oder leiten diese ohne Berechtigung weiter. Bereits eine Studie aus dem Jahr 2012 brachte hervor, dass mehr als 100.000 Android Applikationen den Standort und die Kontakte der Nutzenden abfragen, obwohl dies für ihre eigentliche Funktion nicht notwendig gewesen wäre (Robertson, 2012). Darüber hinaus berichtet eine weitere Studie, dass die Anzahl von Android Applikationen, die im Stande sind Informationen über die Finanzen der Nutzenden weiterzugeben, in der zweiten Hälfte des Jahres 2013 um das Fünffache

gestiegen ist (FireEye, 2015). Vor allem im Google Playstore findet weder eine Überprüfung noch eine Beschränkung der Applikationen hinsichtlich des Eindringens in die Privatsphäre statt. Stattdessen wird bei der Installation ein Hinweis mit den entsprechenden Zugriffsberechtigungen gezeigt, welche die Applikation einfordert, um den Nutzenden über den Eingriff in die Privatsphäre und die Sicherheit der App zu informieren. Sollten die Nutzenden mit den angeforderten Zugriffsberechtigungen der Applikation nicht einverstanden sein, bleibt ihnen lediglich der Abbruch der Installation. Im Falle der Zustimmung erfolgt kein erneuter Hinweis zu den Zugriffsberechtigungen (Felt, Ha et al., 2012).

2.1.7 Behaviorismus

Der Begriff Behaviorismus wurde 1913 von Watson geprägt und beinhaltet die Beschäftigung mit den beobachtbaren Aspekten des Verhaltens. Nach Snethlage (1929) definiert der Behaviorismus die Psychologie als die Lehre von Verhalten. Verhalten ist nach Brand (wie in Kitchener (1977) benannt) ferner definiert als jegliche physiologische Reaktion oder Prozess, z. B. Herzschläge, Nervenimpulse oder das Heben eines Armes.

Genauer gesagt geht der Behaviorismus davon aus, dass sich das Verhalten aus Reaktionen zusammensetzt, die beobachtet werden können und mit anderen beobachtbaren Vorgängen zusammenhängen, wie beispielsweise Bedingungen, die vor oder nach dem Verhalten herrschen und voneinander abhängig sind. Beobachtet werden kann nun das Verhalten, also das, was gesagt oder getan wird. Das eigentliche Ziel einer behavioristischen Psychologie ist das Ableiten von Gesetzen, „die die Beziehungen zwischen den verschiedenen, dem Verhalten vorrausgehenden Bedingungen (Reize), dem Verhalten (Reaktionen) und den Konsequenzen (Belohnung, Bestrafung oder neutralen Effekten) erklären“ (Lefrancois, 2013). Diese Gesetze sind auch unter dem Begriff Reaktionstrias bekannt. Sie ermöglichen die Vorhersage der Reaktion aus Perspektive des Behaviorismus, also das Verhalten eines Organismus auf einen bestimmten Reiz in einer bestimmten Umgebung (J. B. Watson, 1998).

Der Behaviorismus ist darüber hinaus die Grundlage sowohl für frühere als auch moderne Lernprogramme. Wichtigster Ausgangspunkt ist hierbei die Veränderung des beobachteten Verhaltens. Es wird davon ausgegangen, dass äußere Hinweisreize das Verhalten steuern lassen und es somit zu einer Bildung von Reiz-Reaktions-Ketten kommt. Die eigentlichen Denkprozesse gelten jedoch als nicht fassbar. Der Mensch wird somit als Black-Box interpretiert. Größte Vertreter dieser Theorie waren Burrhus F. Skinner und Robert G. Crowder (Meier, 2006).

2.1.8 EU-Datenschutzgrundverordnung

Mit der neuen Datenschutzgrundverordnung (DSGVO, 2018) treten umfassende neue Richtlinien in Bezug auf den Umgang mit Datenschutz in Kraft. Vor allem der Schutz personenbezogener Daten und deren Verarbeitung stehen hierbei im Vordergrund. Eine grundlegende Maßnahme zur Einhaltung folgender Richtlinien ist die Einführung von höheren Sanktionen bei Zuwiderhandlungen. Unter anderem sind zwei technische Aspekte, Privacy by Design und Privacy by Default, hervorzuheben. Ersterer bezieht sich auf die technischen Maßnahmen zum Schutz personenbezogener Daten, welche bereits bei der Entwicklung von Vorgängen einbezogen werden sollen. Letzterer besagt, dass Voreinstellungen bereits datenschutzfreundlich sein sollten. Hierbei wird es den Unternehmen beispielsweise untersagt, bei einer Einverständniserklärung bereits vordefiniert einen Haken im Akzeptanzfeld zu setzten. Darüber hinaus gehen folgende Verbesserungen für den Verbraucher mit der neuen Verordnung einher:

Die Datenportabilität für die Betroffenen soll garantiert werden, sodass diese die Möglichkeit haben ihre personenbezogenen Daten von einem zum anderen Anbieter mitzunehmen. Hinzu kommt die Einwilligung in die Datenverarbeitung, welche stets freiwillig erfolgen muss. Ein Beispiel hierfür ist das Kopplungsverbot, welches besagt, dass ein Vertrag nicht von einer Einwilligung in eine nicht erforderliche Verarbeitung abhängen darf. Darüber hinaus ist es dem Betroffenen gestattet die Einwilligung im Nachhinein zu widerrufen. Eine weitere Verbesserung ist das Recht auf Löschung, welches besagt, dass die verarbeitenden Stellen die Daten zu löschen haben, sobald der Zweck entfällt oder die Einwilligung widerrufen wird. Außerdem wurde das Auskunftsrecht eingeführt, welches zum einen die Auskunft über den Zweck der Datenvereinbarung beinhaltet und zum anderen den Betroffenen die Informationsauskunft über die Aufbewahrungsdauer und bestehende Rechte garantiert. Über die Rechte der Betroffenen hinaus, werden auch technische und organisatorische Maßnahmen vorgeschrieben. Ein entscheidender Unterschied zwischen der Datenschutzgrundverordnung und dem Bundesdatenschutzgesetz ist die Pseudonymisierungspflicht. Somit können die Daten im Verlust- oder Missbrauchsfall nicht persönlich zugeordnet werden. Eine weitere Verpflichtung ist die regelmäßige Überprüfung und Evaluierung der Datensicherheit.

Insgesamt gibt es sieben Prinzipien, in denen gemäß des Artikels 5 der Datenschutzgrundverordnung auf die Verbreitung von personenbezogenen Daten Bezug genommen wird. Das erste Prinzip der Transparenz besagt, dass die personenbezogenen Daten rechtmäßig nach dem Grundsatz von Treu und Glauben und in einer nachvollziehbaren Weise verarbeitet werden. Das zweite Prinzip der Zweckbindung besagt, dass die Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und andernfalls nicht weiterverarbeitet werden dürfen. Das dritte Prinzip der Datenminimierung

besagt, dass die Daten dem Zweck angemessen sein müssen. Das vierte Prinzip der Richtigkeit besagt, dass die Daten sachlich richtig und auf dem neusten Stand sein müssen. Dabei sind angemessene Maßnahmen zu treffen, um fehlerhafte Daten löschen oder korrigieren zu können. Das fünfte Prinzip der Speicherbegrenzung besagt, dass die Daten in einer Form gespeichert werden, welche die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Ausgenommen hiervon sind die längere Abspeicherung der Daten für technische und organisatorische Maßnahmen, Archivzwecke, wissenschaftliche und historische Forschungszwecke sowie statistische Zwecke. Das sechste Prinzip der Integrität und Vertraulichkeit besagt, dass die Verarbeitung der Daten in einer Weise stattfindet, welche die Sicherheit dieser Daten gewährleistet. Darunter fällt auch der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigten Verlusten, Zerstörungen oder Schädigungen durch technische und organisatorische Maßnahmen. Das siebte Prinzip der Rechenschaftspflicht besagt, dass die oben genannten Prinzipien durch Verantwortliche nachweislich eingehalten werden müssen (DSGVO, 2018).

2.2 Grundlagen

Im folgenden Kapitel werden die Grundlagen über das Sammeln und Verwenden von Daten sowie die Ertragseinbringung mit Applikationen aufgezeigt und näher erläutert. Hierunter fällt ebenfalls die Erläuterung der In-App Werbung. Darüber hinaus werden die Thematik der Rechte und deren Abtretung behandelt. Im darauffolgenden Abschnitt werden das Sicherheitsverhalten und die Lerntheorien der Konditionierung beschrieben und es erfolgt eine genauere Betrachtung des Verhaltens der Endnutzenden gegenüber den AGBs und EULAs. Die Einschätzung der Wichtigkeit der Nutzerdaten wird hierbei auch mit den Konsequenzen für die Endnutzenden in Verbindung gebracht. Weiterhin wird ein Einblick in den Umgang von Unternehmen mit der Datensicherheit gegeben. Darüber hinaus werden die Auswirkungen von verfügbaren Informationen über den Schutz der Privatsphäre auf das Kaufverhalten betrachtet und verschiedene Strategien zur Schaffung von Privatsphäre vorgestellt. Letztendlich werden bereits gewonnene Erkenntnisse anderer Studien bezüglich der Einflüsse auf datenschutzrechtliche Bedenken beim Herunterladen von Applikationen aufgezeigt.

2.2.1 Sammeln und Verwenden von Daten

Unternehmen betreiben viel Aufwand, um die Daten der Nutzenden zu sammeln und zu analysieren. Der hohe Wert der Daten könnte darauf zurückgehen, dass der Markt zunehmend gesättigt ist und die

Unternehmen das Ziel haben, Kunden „im Sinne des «One-to-one»-Marketing mit zusätzlichen Informationen über deren Verhalten“ (Baeriswyl, 2000) an das Unternehmen zu binden und diese Verbindung zu festigen. Verschiedene Konzepte und Techniken in diesem Bereich steigern somit die Effizienz und ermöglichen zielgerichtete Marketingstrategien und Verkaufsprogramme (Baeriswyl, 2000). Beratungsfirmen werben mit dem Sammeln und der Verwendung von Nutzerdaten folgendermaßen:

> *„Customer Relationship Management wird Marketing und Verkauf revolutionieren und zu Quantensprüngen in Produktivität und Profitabilität führen. Das Fokussieren auf investitionswürdige Kunden und das konsequente Ausschöpfen des Ertragspotentials jedes einzelnen Kunden durch systematisches Beziehungsmanagement kann auch in ihrem Unternehmen grosse Produktivitäts- und Profitabilitästreserven mobilisieren“ (Born, 2001).*

Wie schon in der Einleitung erwähnt, war die Einführung von Kundenkarten der erste Schritt des Sammelns von Kunden- bzw. Nutzerdaten, mit denen das Kaufverhalten einzelner Personen verfolgt werden konnte (RL 95/46/EG (Datenschutzrichtlinie), 1995). Damals wie heute ist das Ziel, das Konsumverhalten einer Person zu analysieren und zu steuern, sodass die vom Unternehmen beworbenen Produkte erworben werden. Über das Konsumverhalten hinaus werden Persönlichkeitsprofile erstellt, welche unter anderem auch eine Beurteilung der Kreditwürdigkeit erlauben. Durch den technischen Fortschritt und die weite Verbreitung von mobilen Endgeräten besaßen 2015 86 % der Haushalte in Deutschland einen Computer (Statistisches Bundesamt, 2020) und 65 % der deutschsprachigen Wohnbevölkerung ein Smartphone bzw. 40 % ein Tablet (Bitkom, 2016). In Verbindung mit dem rasanten Anstieg der Haushalte in Deutschland, die über einen Internetzugang verfügen, von 46 % im Jahr 2002 hin zu 90 % im Jahr 2015 (Eurostat, 2016), hat sich die Anhäufung von Daten um ein Vielfaches multipliziert. Insbesondere Smartphones ermöglichen es, das Verhalten der Kunden sehr genau nachzuverfolgen und deren Interessen somit zu ermitteln.

Um die Masse an Daten, welche heutzutage zu Verfügung stehen, sortieren, analysieren und verwenden zu können, wurden verschiedene Methoden entwickelt, etwa Data-Mining und Data-Warehousing. Data-Mining definiert Fayyad et al. (1996) als „ die Anwendung spezifischer Algorithmen um Muster aus Daten zu extrahieren“. Darüber hinaus ist Fayyad der Meinung, dass Data-Mining nur ein spezifischer Bestandteil der Wissensextraktion aus Datenbeständen (engl. knowledge discovery in databases) sei. Der gesamte Prozess der Wissensextraktion besteht aus den folgenden Schritten: Recherche von Hintergrundwissen, Definition der Ziele der Wissensfindung, Auswahl und Bereinigung von Daten, Datenreduktion durch Modellierung und Auswahl eines Modelles, in dem das gefundene

Wissen repräsentiert werden soll. Daraufhin erfolgt das eigentliche Data-Mining. Im Anschluss ist eine Interpretation der so extrahierten Daten notwendig (Fayyad et al., 1996).

Ein Data-Warehouse ist eine Ansammlung einheitlicher Datenbanken, welche erstellt wurden, um das Entscheidungsunterstützungssystem zu verbessern (Dedić & Stanier, 2016). Laut Inmon (1992) bestehe ein Data-Warehouse somit aus einer eingebundenen, zeitlich unbestimmten und beständigen Ansammlung von Daten, die hauptsächlich genutzt werde, um organisatorische Entscheidungen zu fällen.

2.2.2 Ertragseinbringung durch Applikationen

Der Vertrieb von Software an Privatanwender begann etwa 1970. Bereits 1983 gab es etwa 35.000 Programme von 3000 Softwareanbietern, die im Bereich der Produktivität, Industrie, Konsum und Bildung eingesetzt wurden und dessen Preise sich auf einen Bereich von 50 bis 500 US-Dollar erstreckten. Der Beginn des Vertriebs von Applikationen, wie in 2.1.6 definiert, lässt sich 2008 mit der Eröffnung des Apple App Stores und dem zugehörigen Software Development Kit für das iPhone festmachen. Die Preise für Applikationen liegen mit durchschnittlich ungefähr 2 US-Dollar (Trefis.com, o.D.) deutlich unter denen der klassischen Software. Dies liegt maßgeblich daran, dass Applikationen meist darauf ausgelegt sind eine spezifische Funktion zu erfüllen, klassische Software jedoch eine Fülle von Funktionen bietet (Wade Morris & Elkins, 2015). Von April 2014 bis Juni 2017 wurden im App Store von Apple Inc. 120 Milliarden Downloads verzeichnet (Apple, o.D.), während im Google Play Store im Zeitraum 2014 bis 2017 291 Milliarden Applikationen (VentureBeat, o.D.) heruntergeladen wurden.

Im Folgenden werden fünf Erlösmodelle für Applikationen vorgestellt. Dabei schließen sich die Erlösmodelle App-Verkauf, Kostenlos und Spende gegenseitig aus. In-App-Verkauf und In-App-Werbung sind jedoch mit diesen und untereinander kombinierbar.

App-Verkauf

Beim Erlösmodell des App-Verkaufes wird die Anwendung in dem jeweiligen Store zu einem bestimmten Preis angeboten. Die durchschnittlichen Ausgaben der Nutzenden unter 18 Jahren betragen etwa 1 Euro pro Monat (Holdampf-Wendel et al., 2014). Die höchsten Ausgaben werden in der Altersgruppe der 25- bis 34-jährigen getätigt. Hierbei sind Männer beim Kauf einer Applikation, die sie vorher nicht testen konnten, freizügiger als Frauen. Bei einem reinen Verkaufserlös wird der

potenzielle Marktanteil nur mittelmäßig bis gering ausfallen. Grund hierfür ist die Bereitschaft seitens der Nutzenden nur bei sehr ausgereiften Applikationen und jenen mit einer hohen Nachfrage finanziellen Aufwand zu betreiben. Dies führt zu einer Kaufbereitschaft von durchschnittlich 7,40 US-Dollar pro Quartal, welche in den Industrieländern als gering anzusehen ist. Dieses Erlösmodell dient somit der Umsatzmaximierung und ist weit verbreitet (Barton et al., 2017). Es herrscht eine generelle Akzeptanz gegenüber diesem Vertrieb, der bei etwa 30 % der angebotenen Apps im Google Play Store verwendet wird (Statista, o.D.). Diese Vertriebsform ist allerdings nur bei nativen und hybriden Anwendungen verwendbar und schließt somit die Web-Applikationen aus. Der Betreiber des App Stores behält meist einen Anteil von 30 % ein. Darüber hinaus ist ein Mehrwertsteuersatz von 19 % üblich (Barton et al., 2017).

In-App-Verkauf

Beim Erlösmodell In-App-Verkauf werden virtuelle Güter, wie z. B. Verbesserungen für den Avatar oder das Freischalten von Funktionen innerhalb einer Anwendung, verkauft. Dabei ist die eigentliche Applikation kostenfrei. Hauptzielgruppe dieses Erlösmodells ist ebenfalls die Altersgruppe ab 25 Jahren aufwärts. Durch die Möglichkeit der kostenlosen Nutzung werden zusätzlich Gruppen mit geringem Einkommen adressiert. Darüber hinaus soll das Angebot durch eine kostenfreie Testnutzung für Frauen attraktiver gestaltet sein, weil es die Möglichkeit gibt das Produkt vor dem Erwerb zu testen (Barton et al., 2017). Das kostenlose Herunterladen soll zu einer weiten Verbreitung der Anwendung führen, um somit ein möglichst hohes Marktpotenzial abzuschöpfen (Spencer, 2016). Dieses Erlösmodell ist bei Unternehmen sehr beliebt, weil es einen regelmäßigen Umsatz generieren kann.

In-App-Werbung

Dieses Erlösmodell beinhaltet das Einblenden von Werbung innerhalb einer kostenlosen Applikation. Hierbei ist vorteilhaft, dass den Nutzenden keine Kosten entstehen und keine Einschränkungen hinsichtlich des Alters, Einkommens, Geschlechts und somit dem potenziellen Marktanteil in Kauf genommen werden müssen. Durch die finanziellen Einnahmen, welche durch die Einbindung der Werbung erlangt werden, ist es möglich die mobile Anwendung zu monetarisieren ohne den Nutzenden eine finanzielle Gegenleistung abzuverlangen (Mayerhofer, 2012). Der Vorzug eines kostenlosen Produktes leidet jedoch meist unter der Anzeige von Werbung (Wächter, 2016). Auf In-App-Werbung wird im folgenden Abschnitt noch einmal genauer eingegangen.

Kostenlos

Ähnlich wie bei dem Erlösmodell mit In-App-Werbung ist bei dem kostenlosen Modell ebenfalls nicht von Einschränkungen in Bezug auf die Zielgruppenkategorisierung auszugehen. Die Erlöse werden bei diesem Modell stets indirekt erworben. Die Anwendung geschieht hier meist als Promotion eines neuen Produktes oder komplettiert ein Produkt. Hierbei lassen sich alle strategischen Führungsziele bis auf die Umsatzmaximierung unterstützen (Mayerhofer, 2012).

Spende

Bei diesem Modell kann die Anwendung kostenfrei heruntergeladen werden, wobei es den Nutzenden freisteht einen gewissen Betrag an das Unternehmen zu spenden, um dessen Aufwände zu refinanzieren. Die Alterszielgruppe liegt bei 25 bis 44 Jahren (Barton et al., 2017). Allerdings verbieten sowohl der Apple App Store (Apple, 2017) als auch der Google Play Store (Google, 2017) das Spenden von Geldern innerhalb ihres Marktplatzes.

2.2.3 In-App Werbung

Aus ökonomischen Gründen werden diverse Applikationen oftmals mit Werbung versehen. Diese wird über verschiedene Programmpakete (engl. Libraries) eingebunden. Die Libraries werden von Werbefirmen zusammengesetzt und den entsprechenden App-Entwicklern zu Verfügung gestellt. Problematisch hierbei sind die von der Applikation gesammelten Informationen über die Endnutzenden, die nicht nur für die Entwickler der Applikation, sondern darüber hinaus auch für die Firma, welche die Werbung in die Applikation integriert, zur Verfügung stehen. Im Gegensatz zu App-Entwicklern ist das Interesse an persönlichen Daten bei den Werbefirmen deutlich höher, was zu einem sehr umfangreichen Sammeln von Informationen führt, das unabhängig von der eigentlichen Funktion der einzelnen Applikationen stattfindet (Krunz, 2012). Beispielsweise verkauft das Unternehmen Schober Adressen von Personen, die mit einem Filter nach Soziodemographie, Wohnsituation, Region und Interessen selektiert bzw. sortiert werden können. Dabei enthält die Preisspanne pro Adresse Werte von 0,35 Euro bis 1,65 Euro. Je genauer der Filter eingestellt wird, bzw. je geringer die Anzahl der Adressen ist, desto höher ist der Preis (Schober Information Group GmbH, 2017). Das Unternehmen bezieht seine Informationen unter anderem durch Kundenkarten, Kontoeröffnungen,

Preisausschreiben und sowohl Kredit- als auch EC-Karten. Insgesamt hat die Wirtschaft 80 % aller Daten gespeichert, während der Staat nur 20 % der Daten verwahrt (Griesenbrock, 2014).

2.2.4 Rechte und deren Abtretung

Wie schon bei der Beschreibung von Data Mining (2.2.1) erwähnt, werden die Nutzerdaten verwendet, um sich etwa ein präzises und individuelles Bild vom Kaufverhalten einer Person zu machen. Dies ermöglicht ein zielgerichtetes Marketing, durch das die individuellen Bedürfnisse und Vorzüge beim Werben für Produkte berücksichtigt werden (Thurm & Kane, 2010). Darüber hinaus werden die Daten meist nicht nur vom Hersteller der Applikation verwendet, sondern auch weiterverkauft, sodass die Nutzenden weder die Kenntnis darüber haben, wer ihre Daten einsehen kann, noch für was sie verwendet werden. Wie bereits erläutert ist die Selbstbestimmung über die Weitergabe und Verwendung von persönlichen Daten ein zentraler Bestandteil der rechtlichen Auffassung von Privatsphäre in Deutschland.

2.2.5 Sicherheitsverhalten und Konditionierung

Um zu verstehen, weshalb die Nutzenden mobiler Endgeräte so freizügig mit der Weitergabe ihrer Daten umgehen, werden nun verschiedene Lerntheorien vorgestellt, die dem Behaviorismus zugeordnet werden.

Eine wichtige Grundlage des Behaviorismus entwickelte der russische Physiologe Pavlov. Dieser untersuchte die Veränderung des Speichelflusses bei Hunden bei der Futterausgabe. Dabei konnte beobachtet werden, dass bei Hunden, welche sich schon länger im Labor befanden, bereits vor der visuellen oder olfaktorischen Wahrnehmung des Futters eine erhöhte Speichelabsonderung auftrat. Zur wissenschaftlichen Erklärung dieses Verhaltens entwickelte Pavlov das Modell der klassischen Konditionierung. Dieses Modell wurde in Folge als Basis für viele Theorien genutzt und repräsentiert heute noch einen wichtigen Bestandteil im psychologischen Wissen. Mit dem Modell zeigte Pavlov, dass nicht nur die visuelle Wahrnehmung des Futters zur erhöhten Speichelabsonderung führte, sondern auch bestimmte andere Reize dieselbe Wirkung hatten, wenn sie oft genug mit der Einnahme der Nahrung einhergingen. Das Futter wurde somit als unkonditionierter Reiz (UCS) definiert, wobei die ursprüngliche Speichelabsonderung bei der Einnahme der Nahrung als unkonditionierte Reaktion (UCR) definiert wurde. Der unkonditionierte Reiz und die unkonditionierte Reaktion bilden zusammen eine Reiz-Reaktions-Einheit. Ein konditionierter Reiz (CS) entsteht, wenn ein bestimmter neutraler Reiz

mit einem bestimmten Ereignis gekoppelt wird, indem dieser mehrmals zeitlich simultan bzw. davor erfolgt. Dieses Phänomen wird als Reiz-Substitution bezeichnet, welche eine Art des Lernens darstellt, wobei der konditionierte Reiz nach mehrmaliger Paarung mit dem unkonditionierten Reiz für diesen eingesetzt werden kann, um die unkonditionierte Reaktion hervorzurufen. Dabei ruft der konditionierte Reiz eine ähnliche jedoch etwas schwächere konditionierte Reaktion (CR) hervor. Dieses Phänomen wird auch als Signal-Lernen bezeichnet.

Der Erwerb klassisch konditionierter Reaktionen und deren Leichtigkeit hängen von diversen Variablen ab, vor allem von der Deutlichkeit der konditionierten Reize. Aus diesem Grund haben sich Töne und Gongschläge als sehr geeignet erwiesen, da sich diese besonders von anderen abheben. Eine weitere entscheidende Variable ist die zeitliche Nähe des konditionierten und des unkonditionierten Reizes. Die schnellste Konditionierung einer Reaktion erfolgt, wenn der konditionierte Reiz unmittelbar vor dem unkonditionierten Reiz eintritt und während des unkonditionierten Reizes andauert (Pavlov, 1927).

Im folgenden Abschnitt wird die Methode der Spurenkonditionierung, der rückwirkenden Konditionierung und der operanten Konditionierung genauer betrachtet.

Das Spurenkonditionieren, bei der der konditionierte dem unkonditionierten Reiz unmittelbar vorausgeht, ist eine effektive Methode zur Konditionierung. Eine Methode, die als sehr uneffektive Lernmethode eingestuft wird, ist die rückwirkende Konditionierung. Dabei gibt es jedoch Ausnahmen (z.B. Keith-Lucas & Guttman, 1975). Bei dieser Methode wird der unkonditionierte Reiz präsentiert und der Wahrnehmung wieder entzogen, bevor der konditionierte Reiz präsentiert wird, weil die klassische Konditionierung meist nicht auftritt, wenn der bedingte Reiz nach dem unbedingten präsentiert wird (Lefrancois, 2013). Das Experiment von Keith-Lucas und Guttman (1975) war eines der wenigen, bei denen die rückwirkende Konditionierung glückte. In dem Experiment wurde unmittelbar (10 Sekunden) nach den Elektroschocks von Ratten ein Plastikigel in dem Käfig platziert. Am nächsten Tag war zu beobachten, dass die Ratten den Plastikigel fürchteten. Wurde der Igel jedoch erst 40 Sekunden nach der Verabreichung des Elektroschocks in den Käfig gestellt, so war bei den Ratten am nächsten Tag deutlich weniger Angst vor dem Igel zu beobachten. Mit Hilfe dieser Studie sollte bewiesen werden, dass einige Arten von Lernen bestimmten Lebewesen leichter fallen als andere Arten von Lernen. Das Erforschen biologischer Beschränkungen bildet somit ein stetig anwachsendes Gebiet in der Psychologie.

Neben der klassischen Konditionierung stellten Edward Lee Thorndike und John Watson die Lerntheorie der operanten Konditionierung auf, welche von Burrhus Frederic Skinner weiterentwickelt wurde (Lefrancois, 2013). Dabei wurde ein Experiment mit Ratten in einem Käfig, der sogenannten

„Skinner-Box“, mit drei verschiedenen Bedingungen durchgeführt. Bei der ersten Bedingung erhielt die Ratte Futter, sobald sie einen Hebel betätigte (positive Verstärkung). Während der zweiten Bedingung wurde ein Gitter, auf welchem sich die Ratte befand, unter Strom gesetzt, der durch Betätigung des Hebels abgeschaltet werden konnte (negative Verstärkung). Unter der dritten Bedingung wurde der Ratte ein Stromschlag erteilt, sobald sie den Hebel betätigte (Bestrafung). Die positive Verstärkung verkörpert somit eine Belohnung nach der Durchführung einer erwünschten Tätigkeit. Die negative Verstärkung hat ebenfalls eine belohnende Wirkung, indem ein negativer Reiz nach der Durchführung der erwünschten Tätigkeit entfernt wird. Nach mehreren Durchführungen betätigte die Ratte in der ersten und zweiten Bedingung weiterhin den Hebel, während bei der dritten Bedingung die Betätigung unterlassen wurde. Als Resultat konnte ein Lernergebnis vorgewiesen werden, bei dem positive Konsequenzen zu einer Wiederholung der Tätigkeit führten, während negative Konsequenzen zu einem Unterlassen dieser führten. Hierbei wird das Bedürfnis (Hunger stillen) durch die Konsequenz des Verhaltens befriedigt (Futter bekommen durch Hebel drücken) und somit verstärkt sich das Verhaltensmuster. Dieser Lerneffekt wird auch Lernen durch Verstärkung bzw. Lernen am Erfolg genannt. Wichtig ist hierbei die Berücksichtigung des Kontiguitätsprinzips und des Kontingenzprinzips.

Das Kontiguitätsprinzip setzt eine zeitlich unmittelbare Reaktion auf die zuvor getätigte Aufgabe voraus (ideal: 500 Millisekunden), um einen möglichst hohen Lernerfolg zu erzielen (Birbaumer & Schmidt, 2000). Dabei sagt das Kontingenzprinzip aus, dass die Aufgabe die Ursache der Reaktion sein muss (Skinner, 1984) bzw. zwei Ereignisse assoziiert werden, wenn das eine das andere vorhersagt (Holland, 1984). Eine nicht kontingente Verstärkung ist beispielsweise eine positive Verstärkung, die nach einem bestimmten Zeitintervall zugeführt wird, unabhängig vom Verhalten des Versuchsobjekts. Wird unmittelbar vor der positiven Verstärkung eine zufällige Aktion seitens des Versuchsobjektes durchgeführt, so ist die Wiederholung dieser Aktion sehr wahrscheinlich, weil das Versuchsobjekt von einer Abhängigkeit ausgeht (Skinner, 1948). Ein ähnliches Phänomen ist bei Verhalten in Bezug auf Arbeitssicherheit zu sehen. Insbesondere hoher Leistungsdruck fördert hierbei sicherheitskritisches Verhalten, beispielsweise durch mangelnde Ausführung von Sicherheitsmaßnahmen oder Nichtanwendung von bewegungseinschränkender Schutzausrüstung. Dies hat zur Folge, dass unsichere, jedoch rationelle Vorgehensweisen den aufwendigen, sicheren Methoden vorgezogen werden (Hofmann et al., 1995). Ein konstanter Zeitdruck führt bei den Mitarbeitenden zu einer Situation, bei der das Eingehen von Risiken als normaler Zustand angesehen wird, vor allem, wenn dieses Verhalten keine Sanktionen nach sich zieht. Somit führt eine Überlastung der Mitarbeitenden zur Vernachlässigung der Sicherheitsziele und zur Priorisierung der zu erreichenden Arbeitsergebnisse (Schaper, 2011). Ähnlich ist das Verhalten bei der Installation bzw. der Nutzung einer Applikation. Durch die uneinsichtigen Konsequenzen wäre es möglich, dass die Endnutzenden über kein

Bewusstsein über die potentiell langfristigen Nachteile der Weitergabe von persönlichen Daten verfügen. Um einen möglichst schnellen Zugriff auf den Dienst der Applikation zu erhalten, wird die abstrakte und mittelbare Gefahr durch die Weitergabe und Nutzung der eigenen Daten eingegangen.

2.2.6 Verhalten der Endnutzenden gegenüber den AGBs und EULAs

In dem Artikel „Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts“ von Bakos et al. (2014) wird behauptet, dass eine sogenannte „informierte Minderheit“ genüge, um die Anbieter eines Produkts daran zu hindern, nutzerunfreundliche AGBs oder EULAs mit ihren Produkten zu verknüpfen. Diesbezüglich wird jedoch kein empirischer Nachweis in dem Artikel vorgestellt. Eine weitere Feststellung von Bakos et al. (2014) ist, dass ein unwesentlicher Anteil der Nutzenden sich näher mit den AGBs auseinandersetzt. Dabei wird das Online-Verhalten von Kunden verschiedener Software-Firmen näher untersucht und darauf geachtet, wie viele von ihnen sich über die AGBs der dazugehörigen Software erkundigen. Das Ergebnis dieser Studie zeigt, dass nur sehr wenige Kunden sich über Online-Verträge informieren. Schätzungsweise 0,05 % bis 0,22 % der Konsumenten öffnen zwar die AGBs, bringen dennoch nicht genügend Zeit auf, um sich diese komplett durchzulesen. Die Autoren dieses Artikels kommen zu dem Schluss, dass der Anteil an Personen, welcher sich mit den AGBs näher beschäftigt, zu klein ist, um eine informierte Minderheit zu bilden, welche das System im Gleichgewicht halten soll.

Eine weitere Studie von Plaut und Bartlett (2012) beschäftigt sich mit dem Verhalten bei sogenannten „Click-Through-Agreements“ (CTAs), wobei es sich um Dialogfenster handelt, bei denen ein einfaches Zustimmen von Nöten ist, um sich mit den AGBs einverstanden zu erklären. Vor allem in den App-Märkten als auch beim Installieren von Applikationen begegnet man diesen Dialogfenstern. Die Kernfragen dieses Artikels sind: Werden die CTAs gelesen und wird der Anbieter nach den erwünschten Vertragsbedingungen gewählt? Wenn dem nicht so ist, stellt sich die Frage, ob das Nichtlesen der CTAs durch die sozialen Repräsentationen der CTAs psychologisch erklärt werden kann. Die sozialen Repräsentationen wurden im Artikel von Plaut und Bartlett folgendermaßen definiert:

1. CTAs sind lang und zeitaufwendig (Olson & Olson, 2003).
2. CTAs sind in einer schwer verständlichen Juristensprache formuliert (Hartley, 2008).
3. Die Kunden müssen die CTAs akzeptieren, wenn sie das zugehörige Produkt erwerben wollen (Rakoff, 1983).
4. Die CTAs haben allesamt den gleichen Inhalt (Epstein, 2006).

5. Vor Gericht werden erdrückende Bedingungen im Nachhinein für ungültig erklärt (Gillette, 2004).
6. Die Bedingungen der Anbieter in den CTAs sind generell fair und vernünftig (Gillette, 2004).
7. Anbieter mit einem gewissen Ansehen haben keine ökonomischen Gründe, unvernünftige oder unfaire Bedingungen anzubieten bzw. zu erzwingen (Gillette, 2004).
8. Niemand anderes liest die CTAs (Gillette, 2004), deshalb lese ich die auch nicht.

Die Studie gliedert sich dabei in zwei Experimente. Im ersten Experiment, einem Fragebogen, sollen der Vorgang des Nichtlesens von CTAs und die sozialen Repräsentationen dieser CTAs untersucht werden. Über 80 % der Befragten geben an, CTAs nicht zu lesen, 16,5 % geben an, die CTAs zu überfliegen. Die von den Befragten angegebenen Gründe für das Nichtlesen decken sich mit den zuvor herausgearbeiteten sozialen Repräsentationen. Beim zweiten Experiment müssen die Versuchspersonen mit einem Onlineshop interagieren. Auch hier wird im Anschluss ein Fragebogen genutzt, welcher das Leseverhalten und das Verständnis der CTAs erhoben hat. Darüber hinaus soll dabei die Verbindung zwischen den sozialen Repräsentationen und dem Leseverhalten untersucht werden. Es wird vermutet, dass wenn die Annahmen über die CTAs manipuliert wird und somit nicht den Erwartungen aus der ersten Studie entsprechen, sich das Leseverhalten verändert. Insbesondere wird davon ausgegangen, dass wenn die CTAs in einer kurzen Zusammenfassung präsentiert werden, sie eher gelesen werden. Für das Experiment wird ein 2 x 6 Design gewählt, welches aus einem kurzen und einem langen CTA sowie sechs Manipulationen der sozialen Repräsentationen besteht. Die Manipulationen wird über eine Variation des einleitenden Textes des CTA erreicht. Darin wird der Versuchsperson erklärt, dass über 80 % der Nutzenden das CTA gelesen hätten. Im Experiment zeigt sich, dass wenn den negativen Erwartungen gegenüber CTAs widersprochen wird, diese eher gelesen werden. Insbesondere Einleitungstexte mit Argumenten, die suggerieren, dass das Lesen der CTAs weder lang noch zeitaufwendig sei und dass die Nutzenden mehrere Optionen zur Wahl hätten, förderte das Leseverhalten, was sich in der investierten Lesezeit zeigt. Obwohl durch die Manipulation der Erwartung Versuchspersonen dazu gebracht werden die CTAs zu lesen, zeigt nur die kurze Version des CTAs einen signifikanten Effekt auf das Verständnis des Inhaltes und die Rate der Ablehnung (Plaut & Bartlett, 2012). Ferner ist jedoch davon auszugehen, dass das Verständnis des Inhaltes sowie die Lesebereitschaft zwischen der Präsentation als digitales CTA und als ausgedrucktes Dokument in Papierform keine Unterschiede aufweist (Schwabe et al., 2020).

2.2.7 Einschätzung der Wichtigkeit der Daten seitens der Endnutzenden

Der Kurzbericht der IFH Köln (2015) beinhaltet über 9000 Verbraucherinterviews aus neun europäischen Staaten. Die Befragung dient zur Erfassung des Stellenwertes des Datenschutzes im

Bereich des Online-Kaufverhaltens. Darüber hinaus soll die Strenge der Datenschutzvorschriften und -durchsetzung sowie der eigene Umgang mit Datenschutz eingeschätzt werden. Zunächst wird ermittelt, wie häufig Produkte online erworben werden. Dabei resultiert, dass sechs von zehn europäische Nutzende das Internet für den Kauf von Waren und Dienstleistungen mindestens einmal pro Monat verwenden. Nur jede zehnte Person tätigt einmal pro Halbjahr oder gar nicht Einkäufe im Online-Shop. Vor allem in den jüngeren und mittleren Altersgruppen hat sich das Online-Shopping etabliert.

Darüber hinaus wird von den Befragten angegeben, dass der Datenschutz und die Datensicherheit eine hohe Relevanz haben und die Auswahl des Online-Händlers davon abhänge. Vor allem die Nachvollziehbarkeit der Datenschutzbestimmungen habe eine große Bedeutung. Als Grund für diese Bewertung seitens der Nutzenden wird einerseits die mediale Berichterstattung über Datenmissbrauch angegeben. Auf der anderen Seite zeigen sich die Verbrauchenden gleichzeitig gerne bereit, persönliche Daten freizugeben, um bessere Dienstleistungen zu erhalten.

Die Meinungsforschung hat ergeben, dass Verbrauchende die Datensicherheit signifikant wichtiger einstufen als materielle Fragen oder die allein informativen Datenschutzbestimmungen, welche von zwei Dritteln der Befragten nur selten bis nie gelesen wird. Dem hingegen werden Datenschutz und Datensicherheit grundsätzlich als wichtig erachtet, wobei auch digitale Dienstleistungen gerne genutzt werden.

Zu der Frage, ob die Datenschutzbestimmungen beim Herunterladen, Bestellen oder Anmelden bei sozialen Netzwerken durchgelesen werden, variieren die Ergebnisse von Nation zu Nation. In Deutschland gaben 17,7 % an, die Datenschutzbestimmungen zu lesen, wobei es in Schweden nur 7,5 % waren. Auch in diesem Kurzbericht wird die These aufgestellt, dass Datenschutzbestimmungen nicht gelesen werden, "[…] weil diese von den Verbrauchern als zu komplex und zu umfangreich wahrgenommen werden" (IFH Köln, 2015, S. 11). Darüber hinaus wird festgestellt, dass die Verbrauchenden nicht den Staat, sondern das Unternehmen für den Datenschutz verantwortlich machen. Lediglich 25 % der Verbrauchenden sehen den Staat als Hauptverantwortlichen, wohingegen 27 % die Verantwortung sich selbst zuschreiben.

Ferner wird in einer Studie, die in Italien von Staiano et al. (2014) durchgeführt wurde, die Wertzuweisung der Endnutzenden bezüglich ihren eigenen Informationen untersucht. Die Studie beinhaltete insgesamt 60 Versuchspersonen zwischen 28 und 44 Jahren (M = 38, SD = 3,4). Der Bildungshintergrund dieser Personen war sehr breit gefächert und variierte von einem sekundären Schulabschluss bis zu Doktorgraden. Alle Teilnehmenden waren aus dem alltäglichen Gebrauch mit den Android Betriebssystem vertraut. Ihr durchschnittliches Einkommen pro Jahr betrug 21.169 Euro.

In dieser Studie werden über sechs Wochen Informationen über die Endnutzenden durch die Nutzung der Smartphones gesammelt. Während der Studie wurden den Nutzenden wöchentlich die gesammelten Daten und Informationen vorgelegt und es wurde die Möglichkeit geboten, diese mit einem Wert zu beziffern und somit zu versteigern. Dabei wurde, wie schon bei einer Studie von Carrascal et al. (2013), auf der die Studie von Staiano et al. (2014) aufbaut, eine Reverse Second Price Auction verwendet. Hierbei bekam nur die Person des niedrigsten Gebotes die Summe des zweitniedrigsten Gebotes ausgezahlt. Die Methode wurde gewählt, weil sie gemäß den Autoren die beste Strategie für die Teilnehmenden ist, bei der Wertzuweisung ihrer subjektiven Einschätzung zu folgen. Darüber hinaus ist sie den Teilnehmenden direkt verständlich und einfach zu erklären. Außerdem wurde die Methode schon vorher von Carrascal et al. (2013) erfolgreich angewendet. Die Studie hat gezeigt, dass die Nutzenden unterschiedlichen Daten einen unterschiedlichen Wert zuweisen. So werden zum Beispiel Positionsdaten als am wertvollsten eingestuft. Darüber hinaus werden Ansammlungen von Informationen wertvoller eingeschätzt als einzelne. Dies gilt jedoch nicht für Informationen im Bereich der Mediennutzung. Eine Korrelation zwischen den Wertzuweisungen der Daten und den sozio-demographischen Eigenschaften kann nicht gefunden werden, anders als bei der Mobilität und dem Nutzen von Applikationen. Personen, die eine hohe tägliche Entfernung zurücklegen, bewerten ihre Daten höher. Personen mit einer hohen Nutzung an Applikationen weisen ihren Daten einen eher geringen Wert zu. Darüber hinaus geht aus einer Studie von Milne und Rohm (2000) hervor, dass jüngere Endnutzende eher dazu geneigt sind, ihre persönlichen Informationen für Unternehmen zugängig zu machen. Ferner zeigt die Studie von Midha (2012), dass weibliche Nutzende größere Bedenken in Bezug auf das Einschreiten in ihre Privatsphäre haben als männliche Nutzende.

Weitere empirische Studien zeigen, dass die Nutzenden Schwierigkeiten bei der Einschätzung von Konsequenzen durch die Rechtefreigabe an Applikationen haben (Kelley et al., 2012; Kelley et al., 2013; Peng et al., 2012). Dementsprechend werden ihre Entscheidungen basierend auf Missverständnissen und falscher Einschätzung der Auswirkungen auf ihre Privatsphäre getroffen, was dazu führen kann, dass sie ihre sensiblen Daten versehentlich aushändigen. Der Mangel an Regularien und technischen Maßnahmen, die versichern sollen, dass die kleinste mögliche Freigabe an Rechten gestattet wird, ist dafür verantwortlich, dass sensible Nutzerdaten nicht genügend geschützt sind (Chin et al., 2012; Hammad et al., 2017; Nauman et al., 2010). Das Verhalten von Applikationen sollte in der jetzigen Zeit, in der Applikationen mehr Informationen denn je anfordern (Au et al., 2012; Qiao et al., 2016), genauer betrachtet werden. Um dies zu tun und den Endnutzenden eine gewisse Privatsphäre zu gewähren, soll untersucht werden, wie häufig die Zugriffsberechtigung bei installierten Applikationen in Anspruch genommen wird.

2.2.8 Privacy Paradox

Während die Endnutzenden häufig behaupten, dass die Privatsphäre ihrer Daten sehr wichtig für sie sei, ist jedoch ihr eigentliches Verhalten gegenüber dem Teilen ihrer Daten und Rechte sowie dem Installieren von Applikationen widersprüchlich. Allerdings zeigen einige Studien, dass die Privatsphäre eine relevante Rolle bei der Installation von Applikationen spielt. Good et al. (2005) behaupten in einer Studie, dass die Nutzenden stets eine Applikation nutzen würden, welche anwenderfreundlichere Datenschutzbestimmungen hat, solange keine Kompromisse in der Funktionalität gemacht werden müssen. Der Unterschied zwischen der Intention private Daten zu schützen und dem eben beschriebenen widersprüchlichen Verhalten ist bekannt unter dem Begriff Privacy Paradox. Dieses Paradoxon wird oft mit dem Privacy-Calculus erläutert, welcher besagt, dass Individuen in einer Situation, in der sie bei Offenlegung ihrer privaten Daten eine entsprechende Entschädigung erhalten, stets eine Kosten-Nutzen-Berechnung durchführen. Dieser Ansatz wurde von Acquisti et al. (2015) weiterentwickelt, indem Faktoren wie unzureichende Information und die sofortige Belohnung berücksichtigt werden. Somit fällt dieses Phänomen in den Bereich der Verhaltenswissenschaften, weil ein rein rational-basierter Erklärungsansatz nicht mehr ausreicht. Die AGBs sind eindeutige Indikatoren für die Maße Sicherheit und Privatsphäre, denen nur wenige Benutzende Aufmerksamkeit schenken. Überraschenderweise geben 60 % der Endnutzenden an, dass ihnen die Abtretung ihrer Rechte manchmal oder immer bewusst ist, dennoch wird diese Abtretung als nahezu unwichtig eingestuft. Diese Erkenntnisse lassen vermuten, dass Endnutzende sich mehr auf die Bewertung und Empfehlung Dritter als auf die schwer zu verstehenden Sicherheits- und Privatsphärekonditionen verlassen, welche durch Endnutzervereinbarung, allgemeine Geschäftsbedingungen und Datenschutzvereinbarungen bedingt sind. Allerdings tätigen die Teilnehmenden nur ungern Einkäufe auf ihren Smartphones, bei denen sie ihre Sozialversicherungsnummer, Gesundheitsinformationen oder Bankdaten angeben müssen. Darüber hinaus sind die Nutzenden sich in Situationen, in denen Sie Dialogfeldern begegnen, meistens nicht bewusst welches Ausmaß das Akzeptieren dieser haben kann. Ein angebrachtes Maß an Aufmerksamkeit und kognitiver Leistung wäre für eine angebrachte Entscheidung von Nöten. Beides ist oft nicht vorhanden, weil die Nutzenden meist in diese Situation geraten, während sie eine andere Primäraufgabe ausführen möchten, welche durch die Zustimmung an Zugriffrechten unterbrochen wird (Felt, Egelman et al., 2012; Good et al., 2005; Grossklags & Good, 2007).

2.2.9 Konsequenzen für die Endnutzenden

Wie bereits in den vorherigen Kapiteln mehrfach erwähnt, ist die Haupteinnahmequelle der größten Dienstleister im Bereich der Medien der Verkauf von personalisierten Daten und das Schalten von personalisierter Werbung. Dabei sind die meisten Internetplattformen untereinander verknüpft, sodass Informationen nach einem Kauf in einem Onlineshop oder auf einer Versteigerungsplattform

an soziale Netzwerke weitergeleitet werden und anschließend entsprechende Werbung geschaltet werden kann. Facebook ist beispielsweise imstande diese Daten 180 Tage lang zu speichern bzw. zu verwenden. Darüber hinaus hat Fuchs herausgearbeitet, dass es sich bei personalisierter Werbung „[…] nicht einfach um Informationen über brauchbare Angebote und Produkte [handelt], wodurch sowohl Konsumenten als auch Unternehmen Vorteile erlangen […]“ (Fuchs, 2010, S. 455), sondern sie folgende Probleme mit sich bringt:

Zu Beginn beschreibt Fuchs die Komplexität der Nutzungs- und Datenschutzbedingungen. Oft umfassen diese mehrere Seiten und sind in juristischer und komplexer Sprache gehalten. Hierbei ist anzuzweifeln, dass die Mehrheit der Nutzenden diese liest bzw. umfassend versteht. Darüber hinaus sind die Einstellungen der Privatsphäre bzw. das Abstellen der Werbeeinstellungen meist schwer verständlich und nicht sofort ersichtlich, sodass Laien kaum imstande sind die Weitergabe ihrer Informationen zu unterbinden. Problematisch hierbei ist, dass die Datenschutzeinstellungen bereits so konfiguriert sind, dass eine höchstmögliche Weitergabe der Nutzerdaten ermöglicht wird und diese bestenfalls deaktiviert werden kann. Dies wird als Opt-Out-Prozess bezeichnet (Fuchs, 2010).

Um das Sammeln und die Weitergabe von Daten zu unterbinden, scheint die einzige Möglichkeit der Nichtbesitz eines Smartphones zu sein. Dies jedoch ist für den größten Teil der Bevölkerung nicht mehr denkbar. Insbesondere die Angewiesenheit auf ein Smartphone in der heutigen Zeit, welche in Zusammenhang mit Berufen im Sektor der Dienstleistungen und der ständigen Erreichbarkeit steht, macht den Verzicht unmöglich. Zudem sind die Vorteile bei der Nutzung eines Smartphones im Alltag, sei es als Navigationsgerät oder Terminkalender, erheblich. Aufgrund der Tatsache, dass das vorherrschende Vertriebsmodell für Applikationen auf entgeltlose Programme setzt, sind die Unternehmen gezwungen die Finanzierung über andere Wege zu erlangen, welche meistens der Verkauf von Nutzerdaten und die Einbindung von Werbung sind.

2.2.10 Umgang mit der Datensicherheit in Unternehmen

In den vergangenen Jahren ist ein stetiger Zuwachs der Ausgaben für Datensicherheit im Bereich Business to-Business E-Commerce zu verzeichnen. Weltweit wurden in diesem Bereich im Jahr 2003 11,26 Milliarden Euro ausgegeben. Fünf Jahre später erhöhten sich die Ausgaben auf 13,59 Milliarden Euro. Die größten Ausgaben im Jahr 2008 tätigten die USA mit einer Summe von 6,52 Milliarden Euro. Westeuropa wendete dagegen nur knapp die Hälfte, 3,14 Milliarden Euro, im Bereich der Datensicherheit auf. Darauf folgten Asien und der Pazifik mit 0,89 Milliarden, Japan mit 0,84 Milliarden, Kanada mit 0,69 Milliarden und Lateinamerika mit 0,22 Milliarden Euro (BMWi, o.D.). Eine aktuelle

Erhebung aus dem Jahr 2020 ergab, dass seit dem Jahr 2017 die Ausgaben für die IT-Sicherheit allein in Deutschland von 3,7 auf 4,9 Milliarden im Jahr 2019 gestiegen ist und für das Jahr 2021 eine weitere Steigerung auf 5,7 Milliarden erwartet wird (Tenzer, 2020c). Weltweit lagen die Ausgaben für die IT-Sicherheit bei 124,12 Milliarden US-Dollar. Davon wurden im Jahr 2018 58,92 % und im Jahr 2019 64,24 % für Sicherheitsdienstleistungen aufgewandt. Vor allem die Ende-zu-Ende-Verschlüsselung wurde bei den meisten Unternehmen eingeführt (Guide, 2019). Eine Umfrage von Hiscox (o.D.b) aus 2016 bestätigt nach Aussagen von Fachkräften die Erhöhung der Ausgaben für Präventionstechnologien und begründet diese mit dem Anstieg von Cyber-Angriffen. Eine Befragung unter IT-Experten zur Entwicklung der Ausgaben für IT-Sicherheit hat eine Prognose des Anstieges der Ausgaben um sechs Prozent ergeben (Eco, o.D.). Darüber hinaus hat eine Studie von Hiscox (o.D.a) ergeben, dass knapp ein Drittel der befragten Unternehmen sich vorgenommen hat eine Cyber-Versicherung im Laufe des nächsten Jahres abzuschließen. Einer österreichischen Studie nach büßt jedes zweite geschädigte Unternehmen einen Schaden von bis zu 50.000 Euro pro Datendiebstahl ein (EY, o.D.). Eine weitere Erhebung aus dem Jahr 2018 hat ergeben, dass in den letzten zwei Jahren rund 3,7 Milliarden Euro aufgrund von Datendiebstahl, Industriespionage oder Sabotage für Rechtsstreitigkeiten aufgewandt wurden. Die hochgerechnete Gesamtschadenssumme in Deutschland belief sich auf 43,4 Milliarden Euro (Bitkom, o.D.). Grund hierfür ist sowohl die steigende Häufigkeit und auch die steigende Qualität der Cyber-Angriffe (Bartelt & Rieger, 2015). Ein Fünftel der befragten Unternehmen aus der Studie von Mester (2014) „muss sich täglich oder mehrmals in der Woche gegen Hacker-Angriffe wehren“ (Mester, 2014). Dabei haben insgesamt 76 % der Entscheidenden von Konzernen über gestiegene Kosten in diesem Bereich berichtet (Mester, 2014). Die Mehrheit der Konzerne (56 %) gab an, sich so gut wie möglich geschützt zu fühlen und über eine umfassende Strategie zum Umgang mit Cyber-Gefahren zu verfügen. Dabei gaben Konzerne nach einer Studie der Zeitschrift CIO, welche im November 2015 durchgeführt wurde, etwa 15 % ihres gesamten IT-Budgets für die Sicherheit aus, wobei 23 % der Unternehmen etwa 20 % des gesamten IT-Budgets aufwenden (C. I.O., 2019). Die Marktgröße des Bereichs Cyber-Sicherheit konnte im Jahr 2016 auf 122,45 Milliarden US-Dollar geschätzt werden und wird für 2021 auf 202,36 Milliarden US-Dollar prognostiziert (Payne, 2017). Nach einer Studie von Suhr (2020) zählt der Schutz der IT im Mittelstand zu den vier wichtigsten Herausforderungen. Ferner geht aus der Studie hervor, dass sich 40 % der befragten Geschäftsführer mittelständischer Unternehmen um die Sicherheit der IT sorgen. Trotzdem wenden mittelständische Unternehmen nur 10 % des IT-Budgets für Aufgaben der IT-Sicherheit auf, was nur etwa 3 % des Jahresumsatzes ausmacht (Hillebrand et al., 2017).

2.2.11 Auswirkungen von verfügbaren Informationen über den Schutz der Privatsphäre auf das Kaufverhalten

In der Studie von Tsai et al. (2011) wird eruiert, ob Unternehmen die Privatsphäre nutzen können, indem sie den Schutz von privaten Informationen erhöhen, um einen Vorteil im Wettbewerb zu erlangen. Hierbei wurden die Teilnehmenden gebeten, Produkte online zu kaufen, indem sie eine neue Suchmaschine nutzten, deren Ergebnisse mit bestimmten Symbolen versehen war. In dem Experiment wurden die Teilnehmenden unterschiedlichen Konditionen ausgesetzt, in denen die Bedeutung der Symbole variierte. In der Bedingung, in welcher das Symbol als Datenschutzinformation angesehen werden sollte, wurde den Teilnehmenden erläutert, dass die Symbole eine Bewertung der AGBs der jeweiligen Internetpräsenz sind. In zwei weiteren Kontrollbedingungen wurde vermittelt, dass die Symbole entweder scheinbar irrelevante Informationen enthalten oder die Symbole wurden erst gar nicht angezeigt. Die AGBs konnten in allen Bedingungen abgerufen werden. Die oben genannten Symbole wurden markant dargestellt. Dabei konnte eruiert werden, dass die Teilnehmenden in der Bedingung der Privatsphäreninformation eher von Internetpräsenzen Einkäufe tätigten, die eine mittlere bis hohe Privatsphäre anboten, selbst wenn der Preis höher ist als auf den anderen Webseiten. Die Teilnehmenden in der Kontrollbedingung tätigten generell Einkäufe beim Anbieter, der den niedrigsten Preis offerierte. Die Teilnehmenden in der Bedingung der irrelevanten Symbole berücksichtigten mit geringerer Wahrscheinlichkeit die Symbole bei ihrer Kaufentscheidung als die Teilnehmenden in der Privatsphäreinfomationsbedingung.

Die Ergebnisse lassen schließen, dass Personen einen höheren finanziellen Aufwand aufbringen würden, um eine gewisse Privatsphäre zu erlangen, wenn die Information salient und intuitiv ist.

Basierend auf der Communication Privacy Management Theorie (CPM) (Petronio, 2002) wurde in der Studie von Xu et al. (2012) die Measuring mobile user´s concerns for information privacy (MUIPC) entwickelt. Die CPM beinhaltet die Koordination dreier essenzieller Aspekte innerhalb der Grenzen darüber, welche Informationen Menschen bereit sind zu teilen. Dazu gehören Durchlässigkeit, Eigentum und Verbindungen aus denen sich die drei Dimensionen *Wahrgenommene Überwachung, Wahrgenommener Eingriff (in die Privatsphäre)* und *Sekundärer Gebrauch von persönlichen Informationen* ableiten. Der Fragebogen kann in Anhang A eingesehen werden.

Wahrgenommene Überwachung

Eine Studie von Malhotra et al. (2004) stellte einen positiven Zusammenhang zwischen der Besorgnis im Bereich des Datenschutzes und der Menge an Informationen, die von anderen verlangt wird, fest.

Die Sammlung von Daten löst eine Koordination von Durchlässigkeitsregeln aus, die sich auf die Parameter beziehen, die das Ausmaß der Weitergabe von privaten Informationen innerhalb der Grenzen von sogenannten Mitbesitzern von Informationen an Dritte bestimmen. Mitbesitzer einer Information wird man, indem man Zugriff auf private Informationen einer anderen Person erhält. Dadurch wird die persönliche Grenze zu einer kollektiven, womit auch die Verantwortung über die Information geteilt wird (Petronio, 2010). Die rasante Weiterentwicklung mobiler Technologien bietet leistungsfähigere Überwachungsmethoden seitens der Anbieter, die eine offene Grenzstruktur mit hoher Informationspermeabilität schafft. Bedingt durch die Aggressivität der Datenerfassung mittels Applikationen und Betriebssystemen auf mobilen Endgeräten entsteht die Wahrnehmung einer intensiven Datenprotokollierung sowie der Eindruck des ständigen Überwachens des Nutzungsverhaltens auf dem mobilen Endgerät. Wie schon in Abschnitt 2.1.3 beschrieben, beinhalten Smartphones variable Funktionen und Applikationen und können wesentlich mehr persönliche invasive Daten sammeln als konventionelle Computer. Dies lässt den Begriff der Überwachung immer wichtiger erscheinen, welcher nach Solove (2006) als das Beobachten, Hören und Aufnehmen von Tätigkeiten von Individuen definiert ist. Nicht selten machen Anbieter und Unternehmen Gebrauch von diesem mächtigen Überwachungswerkzeug, um Nutzende zu profilieren und zu verfolgen. Um die Bedenken der Nutzenden zu messen, wurde aus den Dimensionen der Fragenbögen „Concern for Information Privacy“ (CFIP) und „Internet Users Information Privacy Concerns“ (IUIPC) der Fragebogen „Mobile Users' Information Privacy Concerns“ (MUIPC) erstellt. Während der CFIP die Bedenken der Einzelnen im Bereich des organisationalen Datenschutzes erfasst, reflektiert der daraus abgewandelte IUIPC die Bedenken von Internetnutzenden über Privatsphäreinformationen. Der MUIPC spezifiziert sich auf die Bedenken der Internetnutzenden im Bereich der mobilen Endgeräte.

Wahrgenommener Eingriff (in die Privatsphäre)

Die CPM-Theorie beinhaltet Eigentumsregeln, die festlegen, in welchem Ausmaß Miteigentümer von privaten Informationen anderer, also Datenempfänger, unabhängige Entscheidungen über Besitz oder Einhalten von Informationen treffen können (Child et al., 2009; Petronio, 2010). Darüber hinaus hat Child et al. in derselben Studie eruiert, dass die Eigentumsregelungen sich leicht beobachten lassen, sobald diese verletzt werden oder wenn beim Nutzenden Bedarf besteht, die Datenschutzbestimmungen zu ändern, um unerwünschtes Eindringen vorzubeugen. Die Wahrnehmung von Eindringlingen wird bei den Nutzenden somit ausgelöst, wenn der Datenempfänger eine unabhängige Entscheidung über die persönlichen Informationen der Nutzenden treffen könnte. Der Eingriff in die Privatsphäre wird oft mit dem Konzept des persönlichen Raums von

Solove (2006) in Verbindung gebracht, welcher mit dem Begriff der Grenze des CPM übereinstimmt. Durch die leistungsstarke Überwachungstechnik zur Verfolgung und Profilerstellung wurde der Begriff des persönlichen Raums auf den physischen und informativen Raum ausgeweitet. Laut Solove (2006) ist ein Eingriff ein invasiver Akt, der die Ruhe und Einsamkeit einer Person stört, was das ungewollte Eindringen in das Erscheinungsbild oder in Aktivitäten eines anderen beinhaltet. Das Eingreifen in die Aktivitäten oder Routinen des Opfers unterbricht dessen Ruhe oder ruft ein unwohles Gefühl hervor.

Ein besonders stark heranwachsendes Problem im Bereich der Smartphones ist die Malware. Die Entwickler dieser können auf eine Vielzahl von Daten zurückgreifen, wie beispielsweise den Browserverlauf, das Verwendungsmuster von Apps, Tastaturkürzel, Telefonnummern, Kontakte, geografische Standorte, etc. So ist die Anzahl von Malware im Android App Store innerhalb von einem Jahr zwischen September 2011 und September 2012 um 580 % gestiegen (Kabakus & Dogru, 2018). Weiterhin stellte ein Bericht von McAfee Labs aus dem Jahr 2016 heraus, dass die Anzahl an bösartiger Android Software jährlich um 2,5 Millionen stieg (McAfee Labs, 2016). Aufgrund der Tatsache, dass die Nutzenden demnach nicht davon ausgehen können, dass die App-Märkte frei von Malware sind, können sie Applikationen ablehnen, weil sie deren bösartige Absichten befürchten, die eventuell die gewollten Handlungen unterbrechen könnten. Das Eindringen in die Privatsphäre kann Unwohlsein und Leid hervorbringen, weswegen es den Einsatz der Nutzenden benötigt, um ihr Wohlbefinden sicherzustellen und den Fluss von persönlichen Informationen über bestimmte Grenzen zu unterbinden. In der Tat werden die Dimensionen des Eindringens durch die Dimensionen des CFIPs als unangebrachter Zugriff und Fehler wie auch als Dimension der Kontrolle im IUIPC impliziert. Dennoch wurde von Xu et al. angenommen, dass die Eingriffsdimension, welche auf der CPM Theorie basiert, die Bedenken der Nutzenden von mobilen Endgeräten über den physischen als auch informativen Raum prägnant vermittelt (Xu et al., 2012).

Der sekundäre Gebrauch von persönlichen Informationen

Die sekundäre Verwendung von persönlichen Informationen bezieht sich nach Smith et al. (1996) auf Situationen, in denen Informationen über Einzelpersonen für einen bestimmten Zweck gesammelt werden, jedoch für einen anderen verwendet werden (z.B. Profilerstellung von Personen und Marketingmaßnahmen), ohne dass eine Genehmigung der Einzelpersonen vorliegt. Die sekundäre Nutzung von persönlichen Informationen durch eine Firma kann nach Culnan und Williams (2009) die Fähigkeit von Personen vermindern, den Zugriff auf ihre persönlichen Daten einzuschränken. Außerdem kann es den Personen Schaden zufügen und die Legitimität der Organisation im Umgang mit ihren Verbrauchern, Anteilseignern und Aufsichtsbehörden gefährden.

Die sekundäre Verwendung personenbezogener Daten löst die Koordinierung von Verknüpfungsregeln aus, welche auf die Festlegung einvernehmlich vereinbarter Datenschutzregeln verweisen. Dieser Aufbau wird genutzt, um Dritte auszuwählen, die in die gesammelten Informationen eingeweiht werden. Das Herstellen einer Verbindung bedeutet in der CPM Theorie, dass Dritten Datenzugriff gewährt wird, um Miteigentümer von privaten Informationen zu werden. Die Datenschutzbedenken der Nutzenden hinsichtlich der sekundären Verwendung von Informationen werden ausgelöst, wenn eine neue Verknüpfung ohne Kenntnis oder Zustimmung der Nutzenden erfolgt. Die verbundenen Koordinationsregeln werden häufig als Verstoß angesehen, wenn die Verkäufer die gesammelten personenbezogenen Daten unberechtigt offenlegen oder wenn der Anbieter diese ohne Kenntnis und Zustimmung des Verbrauchers für sekundäre Zwecke verwendet. Laut Solove (2006) erzeugt das Potential für den sekundären Gebrauch Angst und Unsicherheit darüber, wie die Informationen zukünftig verwendet werden sowie das Gefühl von Ohnmacht und Verletzlichkeit. Somit ist die sekundäre Verwendung von persönlichen Informationen eine geeignete Schlüsseldimension für den MUIPC, dessen Anwendung für den zweiten empirischen Versuch in Abschnitt 6.6.7 genauer beschrieben wird.

Weitere Dimensionen

Neben den drei soeben beschriebenen Aspekten, die auf der CPM Theorie beruhen, erfasst der MUIPC zwei weitere Dimensionen, um die Struktur der Faktoren höherer Ordnung zu validieren. Diese Dimensionen umfassen vorherige Datenschutzerfahrung und Verhaltensabsichten. Sie wurden in einer Pilotstudie von Xu et al. (2012) validiert.

Kelley et al. (2013) untersuchte in einer Laborstudie mit 20 Teilnehmenden den Einfluss der Darstellung von Datenschutzinformationen im App-Markt auf das Auswahlverhalten beim Herunterladen von Applikationen. Die Oberfläche des App-Marktes von Google ist derzeit so aufgebaut, dass für das Einsehen der Zugriffsberechtigungen die jeweilige Applikation aufgerufen und der Download in einem weiteren Schritt mit der Zustimmung der Zugriffsberechtigung gestartet werden muss. Die Autoren implementierten in ihrer Darstellung direkt beim ersten Einsehen der Applikation eine Datenschutz-Fakten-Checkliste, welche unmittelbar vor dem Herunterladen auf der ersten Seite der Applikation im App-Markt dargeboten wurde. Somit sollte den Nutzenden eine alternative Rechte- und Datenschutzanzeige geboten werden, die dazu dienen sollte, dass Datenschutzinformationen salienter sind, indem sie früher dargeboten werden, bevor die Entscheidung zum Herunterladen bereits gefallen ist. Die Datenschutzanzeige wurde direkt unter der Applikationsbeschreibung platziert. Die Studie belegt, dass die alternative Darstellung der Datenschutzinformation dazu führt, dass die Nutzenden

Applikationen auswählen, die weniger Rechte einfordern, im Gegensatz zu den Nutzenden, welche die ursprüngliche Darstellung vom Google-App-Markt präsentiert bekommen haben. In der Studie wurden den Teilnehmenden jeweils zwei Applikationen in sechs Kategorien präsentiert. Dabei wurde darauf geachtet, dass unbekannte Applikationen verwendet wurden, die zwischen 1000 und 10.000 Downloads hatten. Dabei wurden die Teilnehmenden gebeten sich vorzustellen, dass ihr Freund zum ersten Mal ein Android-Smartphone besäße und sie für ihn Applikationen auswählen sollten.

2.2.12 Strategien zur Schaffung von Privatsphäre

In der Studie von Hoepman (2014) werden zum Thema Datenschutz acht verschiedene Strategien aufgeführt, um die gesetzten Ziele zur Einhaltung der Privatsphäre zu erreichen. Hierunter fällt das

- Minimieren (Begrenzen des Nutzens der persönlichen Daten auf das kleinstmögliche Minimum),
- Separieren (Aufteilen der persönlichen Daten, sodass mehr Zugangsberechtigungsanfragen von Nöten sind und Isolieren, Teile persönlicher Daten getrennt verarbeiten, ohne Zugang zum oder Zusammenhang mit dem Rest des Datensatzes),
- Abstrahieren (Begrenzen des Detailgrades bei den verwendeten persönlichen Daten),
- Verstecken (persönliche Daten möglichst privat halten),
- Informieren (Personen mit adäquater Information über die Verwendung und Verarbeitung ihrer persönlichen Daten versorgen),
- Kontrollieren (Personen Kontrollmöglichkeiten der Verarbeitung ihrer Daten zur Verfügung stellen),
- Durchsetzen (zur privatsphärefreundlichen Verarbeitung von Daten verpflichten und dies durchsetzen) und
- Demonstrieren (Zeigen, dass die persönlichen Daten auf eine privatsphärefreundliche Weise verarbeitet werden).

2.2.13 Einflüsse auf datenschutzrechtliche Bedenken beim Herunterladen von Applikationen

Der gleichgültige Umgang der Nutzenden mit der Freigabe ihrer Daten bevor Sie eine Applikation installieren wurde bereits von Manar Alohaly und Hassan Takabi (2016) sowie Rosen Sanae et al. (2013) gezeigt. Die Nutzenden sind jedoch umso besorgter bezüglich ihrer Privatsphäre sobald sie realisieren, dass ihre Entscheidungen dazu geführt haben, sich dem Risiko ausgesetzt zu haben, Daten an Dritte

auszuhändigen (Felt, Ha et al., 2012; Jaeyeon et al., 2012; Thompson C. et al., 2013). Darüber hinaus konnte festgestellt werden, dass beim Aufdecken des Applikationsverhaltens bezüglich der Datenzugriffe und -weitergabe die Nutzenden erzürnt werden (Felt, Ha et al., 2012); (Shklovski I. et al., 2014) und ein Verlangen nach einer Änderung der Umstände aufkommt (Wijesekera et al., 2015). Ein hohes Niveau an Unwohlsein, welches Nutzende wahrnehmen, wenn eine Applikation Zugriffsberechtigungen einfordert (perceived permission sensivity) erhöht die datenschutzrechtlichen Bedenken der Nutzenden über ihre Privatsphäre beim Herunterladen von Applikationen, während die Popularität der Applikation diese Bedenken verringert (Gu et al., 2017). Ein weiterer Befund ist, dass der Effekt, den Zugriffsrechtfertigung auf Bedenken über die Privatsphäre hat, stark abhängig ist von vorherigen schlechten Erfahrungen, die die Nutzenden im Bereich der Privatsphäre bei mobilen Endgeräten gemacht haben. Darüber hinaus haben Kelley et al. (2012) herausgefunden, dass gewisse Kontexthinweise, zum Beispiel Privatsphäresymbole, wirksam eingesetzt werden können, um den nachfolgenden Umgang mit der Privatsphäre zu beeinflussen.

3 Stand der Forschung

Das Ziel der Sicherheit im Bereich der Mobilen-Endgeräte spielt eine immer größer werdende Rolle. Es gibt zahlreiche Forschungsarbeiten, die sich mit dem Thema auseinandersetzen. Die meisten dieser Arbeiten beinhalten Applikationen, deren Aufgabe es ist, die persönlichen Daten und Informationen auf dem mobilen Endgerät zu schützen. Relevante Arbeiten, die sich mit dieser Thematik beschäftigen, wurden unter anderem von Enck (2009), Nauman (2010), Conti (2011), Ongtang (2012) und Enck (2014) verfasst. Dabei ist jedoch anzumerken, dass sich die Autoren bei ihren Werken nur auf die technische Umsetzung und deren Programmierung konzentrierten, jedoch den Einfluss auf das Nutzerverhalten außer Acht ließen.

Weitere Untersuchungen beschäftigten sich mit dem Einfluss von unterschiedlichen Anzeigeformen der Endnutzervereinbarungen auf das Verhalten der Nutzenden. Nach der Durchführung eines empirischen Experiments, wobei drei verschiedene Darbietungsformen von Endnutzervereinbarungen den Versuchspersonen präsentiert wurden, hat Begole (2007) eruiert, dass kurzgehaltene Mitteilungen zu Beginn des Installationsvorganges den größten Einfluss auf die Entscheidung der Nutzenden haben. Darüber hinaus konnte festgestellt werden, dass Mitteilungen, die nach Installation der Applikation dargeboten werden, zwar durchgelesen werden, jedoch kaum Auswirkungen auf das Verhalten der Nutzenden haben. Schlussendlich wird von einer Studie dargelegt, die sich mit der spezifischen Android Rechtefreigabe näher beschäftigt hat, dass die Nutzenden den Inhalt der Mitteilung nicht verstehen oder verstehen möchten (Kelley et al., 2012). Während sich vorherige Studien hauptsächlich mit Aspekten der Privatsphäre in der Installations- oder Nutzungsphase beschäftigt haben, wurden bis zum Jahre 2010 noch keine systematischen Studien zu datenschutzrechtlichen Bedenken von Nutzenden in der Downloadphase durchgeführt (Barrera et al., 2010). In der Studie von Rajivan und Camp (Rajivan & Jean, 2016) wurden visuelle Reize verwendet, um die Nutzenden bei der Entscheidungsfindung zu unterstützen, bevor sie ihr Einverständnis an die geforderten Genehmigungen erteilen. Hierfür wurden drei verschiedene Symbole (Smiley, Auge, Schloss) genutzt, um das Risiko des Herunterladens der Applikation zu illustrieren. Neben dem Datenschutzrisiko wurden ebenfalls die Anzahl an Downloads und die App-Bewertung angezeigt. Weiterhin sollten die Teilnehmenden vier von acht Applikationen wählen, bei denen mindestens zwei der eben genannten Angaben wünschenswert waren. Aus der Studie resultierte, dass diese Illustrationen von Risikohinweisen neben der Applikationsbewertung zur Folge hatten, dass die Teilnehmenden an der Studie häufiger Applikationen gewählt haben, bei denen sowohl das Risiko als auch die Bewertung der Applikation als positiv eingestuft wurden. In einer weiteren Studie von Kraus et al (2014) wurde eine Erlaubnisskala (Permission-Scale) genutzt, um den Nutzenden das potenzielle Risiko der Applikation zu vermitteln. In einem Laborversuch mit 48 Teilnehmenden konnte eruiert

werden, dass Nutzende von mobilen Endgeräten dazu neigen, Applikationen mit einer geringeren Anzahl von angeforderten Genehmigungen auswählen, sobald die statistische Information zusammen mit einer Grafik dargestellt wird. Darüber hinaus konnte festgestellt werden, dass das Eindringen in die Privatsphäre und das Vertrauen in die Applikation verändert wahrgenommen wird, wenn statistische Informationen zur Verfügung gestellt werden. In einer Studie von Todd und Benbasat (1992) wird darüber hinaus eruiert, dass Entscheidungshilfen wie die Datenschutzskala den kognitiven Aufwand reduzieren. Außerdem führte die Reduktion des Aufwandes durch die Entscheidungshilfe gleichzeitig zu rationaleren und konsistenteren Antworten. In der Studie von Kelley et al. (2013), welche bereits in Abschnitt 2.2.11 beschrieben wurde, wurden in einer Laborstudie 20 und in einem Online-Experiment 366 Teilnehmenden eine Zusammenfassung über den Datenschutz angezeigt. Diese enthielt eine kurze Beschreibung, welche potenzielle Konsequenzen die Freigabe der persönlichen Daten mit sich bringen kann. Aus der Studie konnte geschlossen werden, dass durch das Implementieren von übersichtlichen Informationen bezüglich des Datenschutzes während der Entscheidungsfindung die Nutzenden dabei unterstützt werden, eine datenschutzfreundliche Entscheidung zu fällen. Die bis hierhin erwähnten Studien bezüglich der Illustrierung einer Datenschutzskala nutzen jedoch stets die sekundäre Oberfläche, also die Oberfläche, die erscheint, wenn sich bereits für eine Applikation entschieden wurde, um den Nutzenden die Risiken bezüglich des Datenschutzes zu vermitteln. Hierbei wird jedoch nicht in Betracht gezogen, dass die Nutzenden sich bereits festgelegt haben und es ihnen schwer fällt, sich nach der bereits getroffenen Auswahl noch einmal anders zu entscheiden, selbst wenn auf die Aggressivität der Applikation aufmerksam gemacht wird. Ferner wurden die Studien unter einem älteren Android-Betriebssystem durchgeführt, bei dem die Nutzenden vor der Installation eine Übersicht über die von der Applikation angeforderten Genehmigungen präsentiert bekommen haben.

4 Versuchsübergreifende Fragestellungen

In Rahmen dieser Dissertation soll erforscht werden, in welchen Umfang die Endnutzenden mobiler Endgeräte ihre persönlichen Daten derzeit schützen. Darüber hinaus soll erfasst werden, wie hoch die Bestrebungen sind, die persönlichen Daten zu schützen und welche Möglichkeiten Endnutzenden zur Verfügung stehen, um datenschutzfreundliches Verhalten aufzuzeigen. Ferner gilt es, auf Grundlage vorheriger Studien sowie Erkenntnissen aus dem ersten Versuch, Methoden zu finden, um die Endnutzenden mobiler Endgeräte beim Schutz ihrer persönlichen Daten zu unterstützen. Hierfür wird eine Datenschutzskala für die Benutzeroberfläche eines App-Marktes und eine Applikation, in der eine temporäre Zugriffsberechtigung zur Verfügung steht, entworfen und auf deren Benutzerfreundlichkeit und Anwendung evaluiert.

Der erste empirische Versuch zum Umgang mit den persönlichen Daten und deren Weitergabe wurde durchgeführt, um folgende übergreifende Fragestellung zu beantworten:

In welchem Umfang schützen die Endnutzenden mobiler Endgeräte ihre persönlichen Daten?

Bei diesem Versuch wird besonders darauf eingegangen, welchen Wert die Endnutzenden ihren persönlichen Daten zuschreiben und wie viel Aufwand sie aufbringen, um diese zu schützen. Ein besonderer Fokus liegt bei dieser Studie auf der Gründlichkeit des Durchlesens der Teilnahmebedingung, welche die AGBs im Alltag repräsentieren soll.

Weiterhin werden im zweiten und dritten Versuch die Methoden eruiert, die den Endnutzenden datenschutzfreundlicheres Verhalten ermöglichen sollen.

Im zweiten Versuch wird zu diesem Zweck eine Datenschutzskala in den App-Markt implementiert, welche die Aggressivität der Applikation bezüglich der abgefragten Zugriffsberechtigung und des Risikos der Herausgabe von Daten an Dritte illustrieren soll. Hierfür wird eine Vorstudie durchgeführt, welche die adäquateste Illustration der Skala bezüglich des Verständnisses und der Lesbarkeit feststellen soll. Zur Erstellung verschiedener Illustrationen von Datenschutzskalen werden in einer Fokusgruppe unterschiedliche Darstellungsformen entwickelt, welche anschließend mit Hilfe eines Fragebogens bewertet werden sollen. Ziel der Vorstudie ist somit die Beantwortung der folgenden Frage:

Welche Illustrationsform einer Datenschutzskala ist die adäquateste, um die Aggressivität einer Applikation darzustellen?

Nachfolgend soll die adäquateste Datenschutzskala in einen prototypisierten App-Markt implementiert werden, um einen möglichen Einfluss auf das Auswahlverhalten zu untersuchen. Mit Hilfe dieser Studie soll somit folgende Frage beantwortet werden:

Wird durch die Implementierung einer Datenschutzskala in den App-Markt ein datenschutzfreundlicheres Auswahlverhalten bezüglich der Applikationen hervorgerufen?

Bei diesem Versuch soll besonders darauf geachtet werden, ob sich die Auswahl der Applikation in der Stichprobe mit der implementierten Datenschutzskala von der Stichprobe ohne diese unterscheidet. Darüber hinaus es ist ein weiteres Ziel zu ermitteln, ob die Datenschutzskala Unterschiede bezüglich der Entscheidungszeiten und des Vertrauens in die Applikation zwischen den entsprechenden Stichproben hervorruft.

Im dritten Versuch soll ein weiterer Ansatz zur Förderung eines datenschutzfreundlicheren Verhaltens untersucht werden, indem eine temporäre Zugriffsberechtigung in der Berechtigungsanfrage auf die Daten und Sensoren des Endgerätes hinzugefügt werden soll. Ziel dieser Studie ist es somit, den Endnutzenden neben der binären Auswahlmöglichkeit, der Zustimmung oder Ablehnung der Berechtigungsanfrage, eine dritte Option der teilweisen Zustimmung zu ermöglichen, indem die Zugriffsberechtigung nur für eine bestimmte Zeitspanne erteilt wird. Diese Funktion soll in einer Applikation implementiert werden, um die nachfolgende Frage zu beantworten:

Wird bei der Verfügbarkeit einer Funktion der temporären Zugriffberechtigung diese von den Endnutzenden mobiler Endgeräte verwendet, um ihre Daten zu schützen?

Hierbei liegt ein besonderes Augenmerk auf der Akzeptanz und der Anwendung der temporären Zugriffsberechtigung.

5 Empirischer Versuch 1 – Umgang mit persönlichen Daten und deren Weitergabe

Dieses Kapitel beinhaltet eine empirische Untersuchung, welche den Umgang mit den AGBs und dem damit verbundenen Abtreten der Rechte näher betrachten soll. Der Fokus liegt bei dieser Studie auf der Bereitwilligkeit der Nutzenden, ihre Rechte abzutreten und somit persönliche Information an Dritte auszuhändigen. Ferner soll ermittelt werden, welchen Wert die Nutzenden ihren Daten zuschreiben. Die folgenden Unterkapitel beinhalten die Forschungsfragen, Forschungshypothesen, die Untersuchungsvariablen sowie die Operationalisierung dieser. Abschließend erfolgt eine Beschreibung des durchgeführten Versuchs, der Methode sowie der Ergebnisse.

5.1 Forschungsfragen

Im Rahmen der Dissertation soll unter anderem die Präsenz und das Bewusstsein der Abgabe von Daten und Rechten im Bereich der mobilen Endgeräte der Nutzenden erfasst werden. Darüber hinaus ist es wichtig, eine Erhebung über die subjektive Wichtigkeit des Problems durchzuführen. Hiermit soll festgestellt werden, ob die Nutzenden die Abgabe ihrer Rechte als negativ empfinden und wenn dies der Fall sei, wäre in einem weiteren Schritt zu erfassen, als wie gravierend dieses Problem empfunden wird. Es gilt also festzustellen, wie wichtig es den Nutzenden ist, ihre Rechte zu wahren. Um dies zu ermöglichen, wird ein Täuschungsexperiment durchgeführt, indem den Teilnehmenden mitgeteilt wird, dass es sich um einen Persönlichkeitstest handele. Ziel ist es dabei, die Teilnehmenden in dem Glauben zu lassen, dass möglichst viele persönliche Informationen über sie gesammelt werden. Darüber hinaus wird untersucht, ob die Darstellungsform der Teilnahmebedingungen digital als Dialogfenster oder analog als Papierform einen Einfluss auf das Leseverhalten der Endnutzenden hat. Zusätzlich ist es interessant in Erfahrung zu bringen, welchen finanziellen Aufwand die Nutzenden aufbringen würden, um eine gewisse Sicherheit und Schutz zu erlangen. Bei den eben erwähnten Angelegenheiten sollte zwischen privaten Endnutzenden und dem kommerziellen Sektor unterschieden werden. Somit ist davon auszugehen, dass besonders große Konzerne einen höheren Wert auf die Diskretion der eigenen Daten legen als mittelständische Unternehmen oder private Endnutzende. Somit gilt es, folgende Forschungsfragen zu beantworten:

a. Wie bewusst ist den Endnutzenden die Abgabe ihrer Daten und Rechte?

b. Wie wichtig ist es den Endnutzenden, ihre Daten und Rechte zu schützen?

c. Welche Einbußen erdulden die Endnutzenden, um ihre Rechte und Daten zu wahren?

d. In welchem Ausmaß unterscheidet sich die Datensicherheit zwischen Konzernen, mittelständischen Unternehmen und Endnutzenden?

e. Hat die Darstellungsform der Teilnahmebedingung einen Einfluss auf das Leseverhalten der Endnutzenden?

5.2 Hypothesen

In diesem Abschnitt wird vermutet, dass, wie in 2.2.9 beschrieben, den Nutzenden nicht bewusst ist, welche Konsequenzen die Abgabe ihrer Daten und Rechte hat. Aufgrund der sozialen Repräsentationen sind die Nutzenden abgeneigt, die AGBs bzw. EULAs zu lesen, vor allem, weil diese meist in Form einer CTA mit einem Klick weggedrückt werden können. Ohne den Inhalt der Geschäftsbedingungen zu kennen, kann davon ausgegangen werden, dass die Konsequenzen den Nutzenden nicht bekannt sind. Darüber hinaus wurde dargelegt, dass die entsprechenden Schriftstücke sehr lang und in juristischer Sprache formuliert werden und somit die Nutzenden aufgrund von Zeitmangel oder mangelndem Verständnis keinen genauen Überblick über den Inhalt der AGBs bzw. EULAs haben. Obwohl die Nutzenden eher abgeneigt sind die AGBs und EULAs zu lesen, gaben sie an, dass sie dem Datenschutz und der Datensicherheit, wie in 2.2.7 dargelegt, eine hohe Relevanz zuschreiben. Andererseits sind die Verbrauchenden bereit, ihre persönlichen Daten freizugeben, um eine kundenorientierte Dienstleistung zu erhalten. Gleiches gilt bei der Herausgabe von Informationen gegen eine bestimmte finanzielle Entschädigung. So deckte die Studie von Staiano et al. (2014) auf, dass Endnutzende innerhalb einer Spanne von einem bis fünf Euro sämtliche Informationen einem Dritten aushändigen würden. Darüber hinaus wurde in Abschnitt 2.2.7 dargelegt, dass die Nutzenden Lokalisationsdaten einen höheren Wert zuweisen als anderen Daten und dass Datenbündeln ein höherer Wert zugeschrieben wird als einzelnen Daten. Aus diesem Grund wird von der Annahme ausgegangen, dass die Nutzenden ihre Daten gegen einen geringen finanziellen Aufwand eintauschen. Ferner wurde im Abschnitt 2.2.6 herausgearbeitet, dass zwischen dem Lesen von digitalen Texten am Bildschirm und analogen Texten als Papierform keine Unterschiede bezüglich des Verständnisses und der Lesebereitschaft vorzuweisen sind.

Somit wurden folgende sechs Hypothesen postuliert:

- Hypothese 1: Die Nutzenden wenden nicht genügend Zeit auf, um sich der Konsequenzen der Abgabe ihrer Daten bewusst werden zu können.

- Hypothese 2: Die Nutzenden empfinden es für sehr wichtig, ihre Daten zu schützen.

- Hypothese 3: Die Nutzenden würden nur geringe Einbußen erdulden, um ihre Rechte und Daten zu wahren.

- Hypothese 4: Die Datensicherheit spielt in großen Konzernen eine wichtige Rolle, wobei sie über mittelständische Unternehmen bis zu den Endnutzenden stetig abnimmt.

- Hypothese 5: Die Gleichgültigkeit der Nutzenden bei der Abgabe von Informationen wird durch die uneinsichtigen Konsequenzen bedingt.

- Hypothese 6: Die Nutzenden händigen gegen einen geringen monetären Wert ihre persönlichen Informationen aus.

- Hypothese 7: Zwischen den Nutzenden, welchen die Teilnahmebedingungen als CTA in digitaler Form und denen, welchen die Teilnahmebedingungen als Ausdruck in Papierform präsentiert wurden, besteht hinsichtlich der Lesezeit kein Unterschied.

5.3 Versuchsdesign

Die durchzuführende empirische Untersuchung besteht aus einem 2x1 between-subjects Design. Ziel ist es, den Umgang der Nutzenden mit persönlichen Daten und ihr Bewusstsein für die Weitergabe dieser Daten zu untersuchen. Hierfür soll ein Täuschungsexperiment entworfen werden, wobei den Testpersonen kommuniziert wird, dass sie an einem Entscheidungsfindungsexperiment teilnehmen. Erst nach dem Experiment werden die Teilnehmenden über das eigentliche Ziel informiert. Vor dem Täuschungsexperiment werden die Teilnehmenden randomisiert einer von zwei Versuchsbedingungen zugeteilt. Sie durchlaufen somit nur eine der beiden Versuchsbedingungen, in denen ihnen die Teilnahmevereinbarungen entweder in ausgedruckter Form oder als click-through-Ereignis präsentiert werden. Die Lesezeit und die Bereitschaft, die Bedingungen zu akzeptieren, werden erfasst, um Unterschiede ausfindig zu machen. Für das Täuschungsexperiment soll ein Programm entworfen

werden, das gleichzeitig zwei Begriffe gegenüberstellt, von denen die Teilnehmenden den favorisierten Begriff wählen, und somit sensible Daten wie religiöse und politische Orientierungen erfasst. Anschließend erhalten die Teilnehmenden ein Dokument zur Weitergabe ihrer Daten, in dem sie ankreuzen sollen, ob und in welchem Umfang sie die zuvor gesammelten Daten an Dritte weitergeben würden. Hierbei entspricht eine hohe Freizügigkeit einem gewissen finanziellen Gegenwert. Nach dem Experiment werden die Teilnehmenden zu ihrem alltäglichen Verhalten bezüglich ihrer persönlichen Daten befragt.

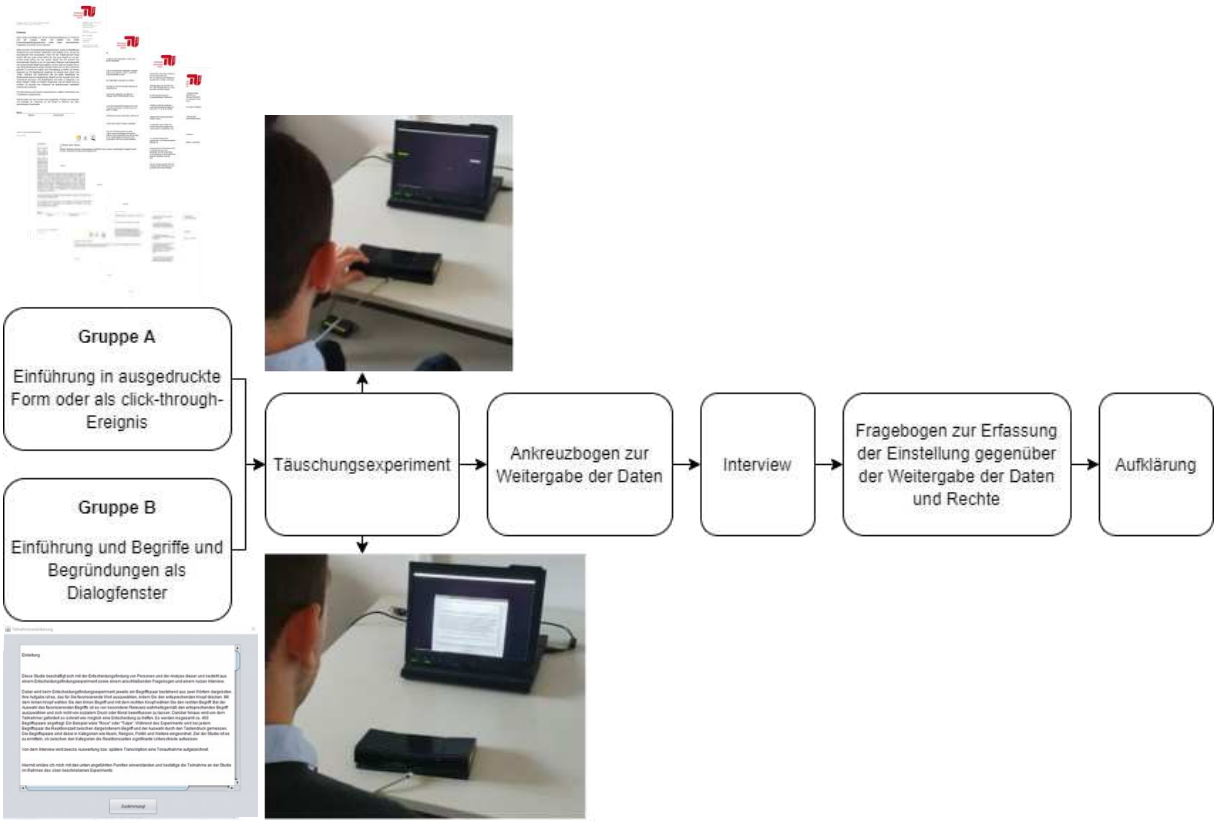


Abbildung 1. Flussdiagramm des ersten empirischen Versuchs bezüglich des Umgangs mit persönlichen Daten.

Dieses Flussdiagramm veranschaulicht den Ablauf der ersten Studie dieser Dissertation zur Erfassung des Einflusses einer Datenschutzskala auf das Auswahlverhalten in einem App-Markt.

5.4 Untersuchungsvariablen

Dieser empirische Versuch enthält eine unabhängige und vier abhängige Variablen, welche in den folgenden Abschnitten näher beschrieben werden.

Unabhängige Variable (UV)

Das Versuchsdesign beinhaltet eine unabhängige Variable zur Erfassung des Umgangs mit verschiedenen Formen der Teilnahmevereinbarungen. Hierbei wird der einen Hälfte der Stichprobe die Teilnahmevereinbarung in ausgedruckter Form vorgelegt. Dabei wird für das Einverständnis mit dieser die Unterschrift gefordert. Die andere Hälfte bekommt die Teilnahmevereinbarungen in digitaler Form als click-through-Ereignis dargeboten und kann das Einverständnis mit einem einfachen Mausklick geben.

- UV1: Darbietung der Teilnahmevereinbarungen in digitaler und ausgedruckter Form.

Abhängige Variable (AV)

Während des Täuschungsexperiments werden mehrere Variablen festgehalten. Die erste abhängige Variable ist die Zeit, die die Teilnehmenden benötigen, um sich mit den Teilnahmevereinbarungen des Versuchs auseinanderzusetzen. Der Anfangspunkt der Zeitmessung entspricht bei der ausgedruckten Form dem Umblättern auf die erste Seite der Teilnahmevereinbarungen, wohingegen das Ende der Zeitmessung durch die Unterzeichnung gesetzt wird. Bei der digitalen Version wird die Zeit automatisch mit Hilfe des Programms gemessen.

Die zweite abhängige Variable erfasste die Zustimmung oder Ablehnung der Teilnahmevereinbarungen. Die dritte abhängige Variable besteht aus der Erfassung der Höhe der Bereitschaft die persönlichen Daten gegen einen monetären Wert auszuhändigen. Dabei steigt die Entschädigung mit der Anzahl an Institutionen, welchen es erlaubt ist, die Daten und Information der Teilnehmenden zu erhalten. Den Versuchspersonen wird also dargelegt, dass ein freizügigerer Umgang mit ihren Daten (Weitergabe an möglichst viele Institutionen) mit einer höheren finanziellen Entschädigung verbunden ist. Die vierte abhängige Variable soll die Übereinstimmung der Ergebnisse des Experiments und des Fragebogens bestimmen (dies erfolgte rein qualitativ).

- AV1: Zeit, welche die Teilnehmenden aufwenden, um die Teilnahmevereinbarungen zu lesen.
- AV2: Zustimmung oder Ablehnung der Teilnahmevereinbarungen.
- AV3: Bereitschaft zur Weitergabe persönlicher Daten gegen finanzielle Entschädigung.
- AV4: Übereinstimmung der Ergebnisse aus dem Experiment und den Antworten aus dem Fragebogen.

5.5 Versuchsvorbereitung und Aufbau

Zur Überprüfung der Hypothesen wurde ein Versuch entwickelt, bei dem berücksichtigt wurde, dass die Antworten von Teilnehmenden zum Datenschutz häufig von sozialen Erwartungen geprägt sind. Im Rahmen eines Täuschungsexperimentes wurde den Teilnehmenden suggeriert, dass sie an einem Experiment zur Entscheidungsfindung teilnehmen. Beobachtet wurde jedoch ihr Verhalten bei der Freigabe von persönlichen Daten gegen einen monetären Vorteil.

Dabei sollte das Experiment folgende Hypothesen überprüfen:

- Hypothese 1: Die Nutzenden wenden nicht genügend Zeit auf, um sich der Konsequenzen der Abgabe ihrer Daten bewusst werden zu können.

- Hypothese 2: Die Nutzenden empfinden es für sehr wichtig ihre Daten zu schützen.

- Hypothese 5: Die Gleichgültigkeit der Nutzenden bei der Abgabe von Informationen wird durch die uneinsichtigen Konsequenzen bedingt.

- Hypothese 6: Die Nutzenden händigen gegen einen geringen monetären Wert ihre Informationen aus.

In dem Experiment wurde auch ein Fragebogen verwendet. Dieser Fragebogen fand auch ohne das Experiment als ein Online-Fragebogen Anwendung. Die Antworten in den verschiedenen Datensätzen (Fragebogen mit Experiment, Fragebogen ohne Experiment) wurden miteinander verglichen. Der Fragebogen diente zur Überprüfung aller oben genannten Hypothesen.

5.5.1 Fragebogen zur Erfassung der Einstellung gegenüber der Weitergabe der Daten und Rechte

Der 22 Fragen umfassende Fragebogen wurde mit dem Online-Portal Lime-Survey erstellt. Somit war es möglich, den Fragebogen online zu verbreiten und ohne Versuchspersonen einzuladen, diesen zahlreich beantworten zu lassen. Zu Beginn wurde ein Willkommenstext verfasst, der kurz darlegte, welche Thematik der Fragebogen behandelt. Des Weiteren wurden die Teilnehmenden über den Umfang informiert und dass das Ausfüllen weniger als zehn Minuten in Anspruch nehmen wird.

Darüber hinaus wurde die Anonymität der Daten gewährleistet, indem eine Datenschutzerklärung eingebettet wurde.

Neben der Online-Umfrage wurde der Fragebogen auch im Entscheidungsfindungsexperiment verwendet. Die Beantwortung der Fragen erfolgte dabei am Computer, ebenfalls über das Portal Lime-Survey. Wie aus dem Aufbau des Experiments, das in Abschnitt 5.5.3 beschrieben wird, hervorgeht, wurde der Fragebogen den Teilnehmenden dabei in einer Situation vorgelegt, in der sie sich unmittelbar davor mit dem befragten Sachverhalt – der Freigabe von Daten – beschäftigt haben. Die Ergebnisse der beiden Stichproben werden im Rahmen der Auswertung auch dahingehend untersucht, ob es hier signifikante Unterschiede zwischen den beiden Stichproben gibt.

Die ersten beiden Fragen dienten der demografischen Einordnung und erfragten das Alter und das Geschlecht der Teilnehmenden. Die dritte Frage diente zur Feststellung des Betriebssystems, was die Teilnehmenden auf ihrem mobilen Endgerät nutzen. Anschließend wurde abgefragt, welche Applikation am meisten genutzt wird, um zu identifizieren, wo der Schwerpunkt beim Gebrauch des mobilen Endgerätes liegt. Die fünfte Frage sollte festhalten, welcher von den genutzten Applikationen die Nutzenden am wenigsten vertrauen, um zu erfassen, ob die Teilnehmenden ein richtiges Gespür für den Umgang mit ihren Daten seitens der Applikationen haben. Die nächste Frage erhob die Häufigkeit der Installationen von neuer Software auf mobilen Endgeräten, um zu erfassen wie häufig die Teilnehmenden in die Situation des Einverständnisses in die allgemeinen Betriebsbedingungen geraten. In der folgenden Frage sollte der prozentuale Anteil der Häufigkeit des Durchlesens der AGBs vor der Installation von Software angegeben werden. Hierbei wurde schon vorher erwartet, dass die Wahl wohl sehr geringe Werte aufweisen wird. Um sicher zu stellen, dass die Teilnehmenden wussten, was allgemeine Geschäftsbedingungen sind, wurde ein kleiner Hilfetext unter den Auswahlmöglichkeiten dargestellt. Mit Hilfe dieser Frage sollte erfasst werden, wie bedeutsam die AGBs für die Teilnehmenden sind. Anschließend wurden die Teilnehmenden gebeten, ihre Antwort qualitativ zu begründen. Hierbei sollte erfasst werden, aus welchen Gründen die AGBs beachtet oder ignoriert werden. In der neunten Fragestellung wurde eine Matrix verwendet, welche die oben in Abschnitt 2.2.6 genannten CTAs untereinander auflistet. Die Teilnehmenden sollten sich dabei in die Situation versetzen, in der sie zuletzt eine Applikation installiert hatten, ohne die AGBs gelesen zu haben. Aus den CTAs sollten sie über eine fünfstufige Skala von „trifft zu“ bis „trifft nicht zu“ auswählen, welche Aussage in diesem Moment dazu geführt hat das Lesen der AGBs zu unterlassen. Anschließend sollte in der nächsten Frage erfasst werden, wie viel Zeit die Teilnehmenden in die nähere Betrachtung der AGBs investieren. Auch diese Frage hatte den Zweck, die Bedeutsamkeit der AGBs für die Teilnehmenden zu erheben. Den gleichen Sinn erfüllte die darauffolgende Frage, welche allerdings nur erschien, wenn die siebte Frage nicht mit „nie“ beantwortet worden war. Sie ermittelte,

ob die Teilnehmenden sich die gesamten AGBs durchlesen oder nur einzelne Ausschnitte. Auch diese Auswahl sollte in der anschließenden Frage begründet werden. Die dreizehnte Frage sollte ausfindig machen, ob die Teilnehmenden Kenntnis von der Rechtezusammenfassung haben, die beispielsweise bei Android vor der Installation den Nutzenden dargeboten wird und ob die eben genannte Zusammenfassung Auswirkungen auf das Verhalten bei der Entscheidungsfindung vor dem Installationsvorgang hat. Ferner sollte in der vierzehnten Frage qualitativ erfasst werden mit welchen Konsequenzen die Teilnehmenden bei der Weitergabe ihrer Daten glauben rechnen zu müssen. Die fünfzehnte Frage sollte festhalten, ob die Teilnehmenden das Installieren einer Software aufgrund der AGBs unterlassen haben. Auch hierbei sollte festgestellt werden, welche Relevanz die AGBs für die Teilnehmenden haben und ob sie als rechtskräftig angesehen werden. Im Falle einer Bejahung dieser Frage wurde in der nächsten der sinngemäße Inhalt der AGBs abgefragt, der zur Unterlassung einer Installation führte. Ferner sollte der Name der Applikation genannt werden. Die 17. Frage sollte erfassen, ob die Teilnehmenden Bedenken an dem Speichern und der Weitergabe ihrer persönlichen Daten hatten. Hierbei konnten sie auswählen, ob sie keine oder nur Bedenken an der Speicherung bzw. an der Weitergabe der Daten oder an Beidem haben. Die achtzehnte Frage sollte erfassen, welche der Dateien nach Meinung der Teilnehmenden weitergegeben werden. In der folgenden Frage sollten die Teilnehmenden den monetären Wert ihrer Daten schätzen. Dabei wurde zwischen Geschlecht, Alter, Adresse, Standortdaten, Kontaktdaten aus dem Adressbuch, persönlichen Bildern und der Browserchronik unterschieden. Hierbei sollte ermittelt werden, ob die Teilnehmenden ein Gespür für den Wert der Daten haben. Die darauffolgende Frage ermittelte den Stellenwert des Schutzes persönlicher Daten von den Teilnehmenden. Hierbei konnten sich die Teilnehmenden auf einer zehnstufigen Skala zwischen den Polen „niedrig“ und „hoch“ festlegen. In der 21. Frage wurden die finanziellen Ausgaben in einem Monat für den Erwerb von Applikationen seitens der Teilnehmenden erfasst. Die Frage zielte darauf ab, zu ermitteln, wie hoch der finanzielle Aufwand war, den die Teilnehmenden allgemein bereit waren für neue Software auf ihrem mobilen Endgerät zu betreiben. Die abschließende Frage ähnelte der Vorherigen und ermittelte den finanziellen Aufwand, den die Teilnehmenden betreiben würden, um ihre Daten auf dem mobilen Endgerät zu schützen. Der Fragebogen befindet sich im Anhang B.

5.5.2 Programm zur Entscheidungsfindung

Das Programm zur Entscheidungsfindung, welches genutzt wurde, um umfangreiche und persönliche Informationen der Versuchsteilnehmer zu sammeln, wurde in Java mit der Entwicklungsumgebung „NetBeans“ geschrieben. Ziel war es, ein Programm zu schaffen, welches den Teilnehmenden

vortäuscht ein Reaktionsversuch zu sein. Der eigentliche Grund war es jedoch, möglichst viele Informationen über die Teilnehmenden zu sammeln. Dabei wurden zwei Begriffe (z.B. „Hamburg“ und „Berlin“) einer Kategorie (in diesem Fall „Städte“) den Teilnehmenden dargeboten.

Diese mussten sich so schnell wie möglich für einen dieser Begriffe entscheiden. Der Begriff leuchtete zwecks Rückmeldungen kurz auf. Anschließend folgte das nächste Begriffspaar. Insgesamt wurden 450 Begriffspaare dargeboten. Die Ergebnisse wurden in Form einer CSV-Datei abgespeichert und beinhalteten die Reaktionszeit, den ausgewählten und den nicht ausgewählten Begriff.

Das Programm wurde ebenfalls genutzt, um die Teilnahmevereinbarungen für den Versuch in Form eines Click-Through-Agreements zu präsentieren, hierbei wurde die Lesedauer gemessen. Neben der Lesedauer wurde auch die Position der Bildlaufleiste gemessen – somit konnte erfasst werden ob und wie die Teilnahmevereinbarung gelesen worden ist. Die Anzeige der Teilnahmevereinbarungen konnte über eine Konfigurationsdatei aktiviert bzw. deaktiviert werden, sodass die erste Stichprobe die Teilnahmebestimmungen in ausgedruckter und die zweite Stichprobe in digitaler Form vorgelegt wurde. Der Quellcode ist dem Anhang C zu entnehmen.

Zur Auswahl des favorisierten Begriffs wurden der Versuchsperson zwei Knöpfe zur Verfügung gestellt. Diese waren über einen USB Key-Controller („KeyWarrior24“, von „Code Mercenaries“) mit dem Computer verbunden (s. Abbildung 1).

5.5.3 Täuschungsexperiment

Dieser Versuch sollte den Umgang mit der Weitergabe von persönlichen Daten untersuchen und mit den Aussagen der Teilnehmenden vergleichen. Ziel war es, zu überprüfen, ob die Verhaltensweisen der Teilnehmenden mit deren Aussage gegenüber der Datensicherheit übereinstimmen. Dazu sollten, wie im oberen Abschnitt beschrieben, Teilnehmende zu einem Reaktionszeitexperiment geladen werden.

Ziel des Täuschungsexperimentes ist es nicht, die Reaktionszeiten der Teilnehmenden zu erfassen, sondern möglichst viele Informationen über diese zu sammeln und im Anschluss die Freizügigkeit der Weitergabe zu beobachten. Hierbei liefert das Reaktionszeitexperiment sowohl eine große Menge an Informationen über die Teilnehmenden und stellt gleichzeitig eine glaubhafte und nachvollziehbare Aufgabe dar.

Das Experiment wurde stets mit einem/einer Teilnehmer/in individuell durchgeführt und nahm etwa 50 Minuten Zeit in Anspruch. Dabei gliederte es sich in die folgenden Schritte: Begrüßung, Bestätigung der Teilnahmevereinbarungen und Durchführung des Entscheidungsfindungsexperimentes, Weitergabe der Daten, Interview, Fragebogen und Aufklärung. Der Fragebogen wurde bereits im Abschnitt 5.5.1. erläutert, weshalb hier nicht noch einmal auf ihn eingegangen wird.

5.5.3.1 Begrüßung und Einleitung

Die Teilnehmenden wurden begrüßt und gebeten sich vor dem Computer, der für die Durchführung des Experiments genutzt wurde, zu setzen. Anschließend wurde eine kurze mündliche Einführung gegeben. In der Einführung wurde erläutert, dass es sich um ein Entscheidungsexperiment handelt, in dem zwei Begriffe gegenübergestellt wurden, und die Teilnehmenden sich möglichst schnell für einen dieser Begriffe entscheiden müssen. Dabei sollten die Teilnehmenden den persönlich favorisierten Begriff auswählen und sich nicht von moralischem und sozialem Zwang leiten lassen. Nachfolgend wurde den Teilnehmenden nahegelegt, die Einleitung gründlich zu lesen, wobei darauf verwiesen wurde, dass die Teilnahmevereinbarung der Einleitung angehangen wurde. Die Hälfte der Teilnehmenden bekam die Teilnahmevereinbarungen in Papierform vorgelegt, die andere Hälfte als Click-Through Agreement. Die standardisierte Einleitung befindet sich im Anhang D.

5.5.3.2 Teilnahmevereinbarungen und Entscheidungsfindungsexperiment

Die eben erwähnten Teilnahmevereinbarungen wurden überspitzt gestaltet, sodass die Teilnehmenden sich beim Durchlesen bewusstwerden konnten, dass sie bei Zustimmung sämtliche Rechte abgeben würden und die Informationen weitergegeben werden könnten. Darüber hinaus sollte festgehalten werden wie lange sich die Teilnehmenden mit den Teilnahmevereinbarungen befasst haben und ob dieser zugestimmt wird. Die Messung erfolgte von den Versuchspersonen unbemerkt. Bei einer Hälfte der Versuchsteilnehmenden über das Computerprogramm selbst, bei der anderen Hälfte manuell mittels Stoppuhr. Die Teilnahmevereinbarungen sind im Anhang E einzusehen.

Nach der Bestätigung der AGB zählte das Programm einen Countdown von zehn Sekunden herunter. Im Anschluss an diesen Countdown erfolgte die Darbietung von Begriffspaaren. Die Reaktionszeit und die Präferenzen waren für dieses Experiment nicht von großem Interesse. Vielmehr ging es darum, den Teilnehmenden zu vermitteln, dass bei dem Experiment eine Vielzahl von persönlichen Daten erfasst wird. Die Fragen wurden dabei so konstruiert, dass teilweise ähnliche Begriffe verglichen wurden, so

dass die Antworten eine möglichst hohe Konsistenz aufweisen. Darüber hinaus wurden die Begriffe mehrfach in verschiedenen Begriffspaaren dargeboten. Es wurden Begriffe zu den Kategorien Politik, Freizeit, Musik, Länder, Kontinente und weitere präsentiert. Eine Liste aller Begriffspaare ist dem Anhang F zu entnehmen.

5.5.3.3 Weitergabe der Daten

Nach dem Abschließen des Entscheidungsfindungsexperiments wurde den Teilnehmenden vorgetäuscht, dass ihre Daten auch für andere Institutionen von Interesse wären und sich danach die Höhe der finanziellen Gegenleistung für die Teilnahme an der Studie richten würde. Die Teilnehmenden sollten ihre Entscheidungen hierzu in einen Ankreuzbogen mit sieben Auswahlmöglichkeiten eintragen. So konnten sich die Teilnehmenden unter anderem dafür entscheiden, dass ihre Daten nicht an Dritte weitergegeben werden, wobei hierfür die niedrigste finanzielle Gegenleistung in Höhe von zwei Euro in Aussicht gestellt wurde. Weiterhin wurden in dem Ankreuzbogen sechs verschiedene Gruppen von Institutionen präsentiert, die ein angebliches Interesse an den Daten hätten. Bei Zustimmung wäre den jeweiligen Institutionen der Zugriff auf die gesammelten Daten gewährt. Zur besseren Übersicht war eine ausführliche Auflistung der Institutionen pro Verbund an den Auswahlbogen angehängt. Um eine höhere Glaubwürdigkeit der Täuschung zu erzeugen, wurden die Namen realer Institutionen gewählt. Die vermeintliche finanzielle Gegenleistung für die Weitergabe der Daten unterschied sich je nach Gruppe. So war sie abhängig von der Art und Reichweite der Institutionen, die von Gruppe zu Gruppe variierte.

Der erste Verbund, für welchen die Daten zugänglich gemacht werden sollten, bestand ausschließlich aus Berliner Hochschulen und beinhaltete neben der Technischen Universität Berlin unter anderem auch die Freie Universität Berlin und die Beuth Hochschule. Hierfür wurde eine Gegenleistung in Höhe von 3 Euro angegeben. Der zweite Verbund beinhaltete die Institute des ersten Verbunds und zusätzlich weitestgehend auf Berlin beschränkte Unternehmen, wie etwa das Fraunhofer Institut und Ecoligo, und sollte mit einer Gegenleistung von 5 Euro vergütet werden. Der dritte Verbund stellte eine Vergütung von 6 Euro in Aussicht und beinhaltete neben den Institutionen aus Verbund 1 andere nationale Universitäten und Hochschulen (zum Beispiel: RWTH Aachen, Universität zu Köln, …). Die Institutionen aus Verbund 1, 2 und 3, sowie nationale Marktforschungsunternehmen sind im vierten Verbund zusammengefasst, welcher mit 8 Euro dotiert wurde. Die Auswahl des fünften Verbundes beinhaltete weltweite Universitäten, worunter auch die deutschen Universitäten aus Verbund 1 und 3 gehören. Bei der Auswahl dieses Verbundes wurde den Teilnehmenden eine Vergütung von 9 Euro in Aussicht gestellt. Der sechste Verbund setzte sich aus allen bisher genannten Institutionen zusammen

und wurde durch internationale Marktforschungsunternehmen ergänzt. Hierbei wurde den Teilnehmenden eine Summe von 10 Euro versprochen.

Wichtig ist hier zu erwähnen, dass auf dem Ankreuzbogen nur eine Möglichkeit ausgewählt werden durfte, also entweder ein Verbund oder die Verweigerung der Weitergabe. Dadurch war keine Aufsummierung der Geldbeträge möglich. Eine genaue Auflistung der aufgezählten Institutionen und Unternehmen, sowie eine Kopie des Ankreuzbogens, befinden sich im Anhang G.

5.5.3.4 Interview

Im Anschluss erfolgte ein kurzes Leitfadeninterview mit den Teilnehmenden. Dieses umfasste sieben Fragen, wobei teilweise Nachfragen gestellt wurden. Von dem Interview wurde eine Audioaufzeichnung erstellt. Es wurde erfragt, ob die Teilnehmenden während des Experiments verunsichert waren. Ist dem so gewesen, wurden sie gebeten genauer zu schildern, weshalb sie sich verunsichert gefühlt haben. Hierbei sollte ermittelt werden, ob Versuchspersonen die Teilnahmevereinbarung gelesen haben, ihnen dabei eigenständig etwas aufgefallen ist oder sie im Laufe des Experiments Bedenken jeglicher Art hatten. Die zweite Frage hatte einen ähnlichen Zweck und sollte ermitteln, ob ihnen während der Teilnahme am Versuch etwas aufgefallen ist. In der nachfolgenden Frage sollten die Versuchspersonen mitteilen, ob sie die Teilnahmevereinbarungen gelesen und wie viel Zeit sie hierfür aufgebracht haben. Hierbei wurde eine Schätzung im Minuten- bzw. Sekundenbereich erwartet. Darüber hinaus sollten sie berichten, ob ihnen während des Durchlesens etwas aufgefallen ist. Zuletzt wurde erfragt, ob die Teilnehmenden ein Gefühl von Unwohlsein hatten, während sie im Laufe des Täuschungsexperiments ihre persönlichen Präferenzen preisgegeben haben. Eine Kopie der Interviewfragen befindet sich im Anhang H.

5.5.3.5 Aufklärung

Schlussendlich wurde den Teilnehmenden offenbart, dass es sich um ein Täuschungsexperiment handelte. Die Teilnehmenden erhielten unabhängig von ihrer getroffenen Auswahl die gleiche finanzielle Gegenleistung respektive Versuchspersonenstunden. Eine Abschrift ist im Anhang I zu finden.

5.5.4 Auswahl der Teilnehmenden

Für das Experiment wurden die Teilnehmenden über das Online-Probandenportal „Prometei“ der Technischen Universität Berlin akquiriert. Um eine valide Aussage der Ergebnisse zu erreichen, wurde eine Mindestteilnehmeranzahl von *N* = 50 Personen festgelegt. Diese Stichprobe sollte bezüglich der demographischen Daten möglichst heterogen sein und alle Altersgruppen einschließen, um auch mögliche Effekte des Alters auf den Umgang mit personenbezogenen Daten zu untersuchen. Die einzige Bedingung zur Teilnahme an der Studie war es, Deutschkenntnisse auf muttersprachlichem Niveau zu haben, weil sämtliche Unterlagen und Fragebögen in der deutschen Sprache verfasst wurden und teilweise komplexe Fachwörter beinhalteten. Dies war vor allem für das Verständnis der Teilnahmevereinbarungen notwendig, welche absichtlich kompliziert verfasst wurden.

Den Teilnehmenden wurde im Online-Portal eine finanzielle Gegenleistung in einer Spanne von 2 Euro bis 10 Euro für die Teilnahme angeboten. Sie konnten sich in dem Zeitraum vom 17.10.2017 bis 30.11.2017 für einen Termin werktags zwischen 10:00 und 17:00 Uhr eintragen.

5.6 Datenaufbereitung

Im folgenden Kapitel wird die Aufbereitung der Rohdaten sowie das weitere Vorgehen zur Analyse der Daten erläutert. Alle Datensätze wurden dafür in eine große Tabelle zusammengeführt. So wurde eine Tabelle, bestehend aus 190 Variablen, mit Hilfe des Programms SPSS von IBM erstellt. Wichtig ist hier zu erwähnen, dass ein Großteil der Variablen durch die Kategorisierung der Antworten entstanden ist.

5.6.1 Demographische Daten

Die demographischen Daten konnten aus dem Umfrageportal LimeSurvey in eine Excel-Datei exportiert werden. Anschließend erfolgte das Importieren der Daten in das Statistik-Programm SPSS. Eine weitere Aufbereitung der Daten war in diesem Fall nicht notwendig.

5.6.2 Teilnahmevereinbarungen

Das Hauptaugenmerk bei dieser Untersuchung lag auf dem Lesen der Teilnahmevereinbarung und der dabei aufgewandten Gründlichkeit. Aus diesem Grund wurde bei den Versuchspersonen der Stichprobe, welche die schriftliche Version der Teilnahmevereinbarungen erhalten haben, vermerkt,

wie lange sie diese gelesen haben und ob die Teilnahmevereinbarungen vor oder nach der Unterzeichnung angeschaut wurden. Hierbei ist wichtig zu erwähnen, dass die Zeit ab dem Umblättern, von der Einführungsseite auf die erste Seite der Teilnahmevereinbarungen bis zum Tätigen der Unterschrift, gemessen wurde. Falls das Dokument vor dem Lesen unterschrieben wurde, so galt das Weglegen des Dokuments als Messendpunkt. Bei der zweiten Stichprobe, welche die Teilnahmevereinbarungen in digitaler Version als Click-Through-Agreement präsentiert bekommen hat, wurde die Anzeigedauer der Teilnahmevereinbarungen automatisch festgehalten. Darüber hinaus wurde registriert, welche Passage der Teilnahmevereinbarung zu welchem Zeitpunkt im Dialogfeld angezeigt wurde. Somit war es möglich die reine Zeit, die in das Lesen der Teilnahmevereinbarungen investiert wurde, zu messen, indem die für die Einleitung aufgewandte Zeit von der Gesamtzeit subtrahiert wurde. Die Zeiten wurden für die jeweiligen Teilnehmenden in die SPSS Tabelle eingetragen.

5.6.3 Fragebogen

Der Fragebogen wurde über ein Portal des Fachgebiets Mensch-Maschinen-Systeme der Technischen Universität Berlin am Computer ausgefüllt. Somit war es möglich, sämtliche Daten in SPSS zu importieren. Mehr Aufwand wurde beim Kategorisieren der Freitextantworten benötigt. Zur Bildung einer Kategorie wurde wie folgt vorgegangen: Sämtliche Stichwörter aus den Antworten wurden zunächst herausgeschrieben. Anschließend wurde gezählt, wie oft das Stichwort in der Gesamtstichprobe vorkam. Tauchte ein Stichwort bei mehr als drei Teilnehmenden (etwa 8 %) auf, so wurde eine entsprechende Kategorie erstellt. Erwähnte die Person besagtes Stichwort oder gab sie inhaltlich eine vergleichbare Antwort, so wurde in der entsprechenden Kategorie eine „1“eingetragen, war das Stichwort in ihrer Antwort nicht aufzufinden wurde eine „0“ eingetragen.

Über die Freitextfelder hinaus wurden die im Abschnitt 2.2.6 aufgelisteten sozialen Repräsentationen gegenüber den CTAs den Teilnehmenden vorgelegt. Um die Häufigkeiten der Antworten auf die verschiedenen sozialen Repräsentationen vergleichen zu können, wurde ein Diagramm erstellt, welches die Häufigkeiten der Antworten zu den jeweiligen Aussagen nebeneinanderstellt.

Darüber hinaus wurden teilweise verschiedene Kategorien aufsummiert, um die Häufigkeit der Antworten zu erheben und quantitative Auswertungen möglich zu machen.

5.6.4 Ankreuzbogen zur Weitergabe der Daten

Zur Erfassung der gewählten finanziellen Gegenleistung für die Weitergabe der Daten wurde die Auswahl des Ankreuzbogens manuell in die SPSS-Tabelle eingetragen, welche ebenfalls die Ergebnisse des Fragebogens und der Teilnahmevereinbarungen einhält. Die manuelle Übertragung der finanziellen Gegenleistung war von Nöten, weil diese auf ein Dokument in Papierform und nicht digital an einem Endgerät erfolgte.

5.6.5 Demographische Daten der Stichprobe

In der siebenwöchigen Laufzeit der Studie haben insgesamt 51 Personen teilgenommen. Davon waren 20 Personen männlichen (39,22 %), 31 weiblichen Geschlechts (60,78 %). Das durchschnittliche Alter der Versuchspersonen betrug *M* = 31,27 Jahre (*SD* = 10,224), wobei die jüngste Versuchsperson 18 Jahre alt und die älteste 64 Jahre alt war. Zur besseren Übersicht wurde eine Illustrierung der Verteilung des Geschlechtes erstellt (s. Abbildung 2. Verteilung des Geschlechtes der Stichprobe).

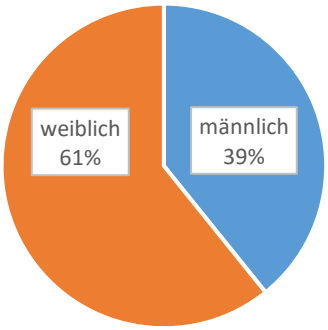


Abbildung 2. Verteilung des Geschlechtes der Stichprobe.

Dieses Kreisdiagramm illustriert die Verteilung des Geschlechtes im Versuch zu dem Umgang mit persönlichen Daten. Insgesamt umfasste die Stichprobe ca. 39 % männliche und ca. 61 % weibliche Teilnehmende.

5.6.6 Interview

Nach dem Täuschungsexperiment wurden den Teilnehmenden die im Anhang H aufgeführten Fragen gestellt. Diese wurden mit einem Diktiergerät der Marke *Youthink* aufgenommen und später

transkribiert. Ähnlich wie bei den Freitextfragen im Fragebogen wurden die Antworten kategorisiert. Häufig wurden auch mehrere Antworten aggregiert, beispielsweise die verschiedenen Messengerapplikationen.

5.7 Ergebnisse

Das folgende Kapitel beinhaltet die Ergebnisse der Untersuchung in Hinblick auf die Hypothesen. Nachdem die Daten, wie im vorherigen Abschnitt 5.6 beschrieben, adäquat aufbereitet wurden, war es möglich die Daten deskriptiv und bei herrschender Notwendigkeit auch inferenzstatistisch zu analysieren. Hierbei ist zu erwähnen, dass bei der Inferenzstatistik von einem Signifikanzniveau von $p < .05$ ausgegangen wird, sofern kein anderes Signifikanzniveau angegeben wird.

5.7.1 Vergleich mit dem Umgang der Teilnahmevereinbarungen

Die Teilnahmevereinbarungen wurden zwei Stichproben in unterschiedlicher Präsentationsform vorgelegt. Die erste Stichprobe, welche die Teilnahmevereinbarungen in Papierform erhielt, umfasst eine Teilnehmerzahl von $N = 26$ Personen, wohingegen die zweite Stichprobe, der die Teilnahmevereinbarungen digital in einem Dialogfenster präsentiert wurde, $N = 25$ Personen umfasst. Die Betrachtungsdauer der Teilnahmevereinbarungen in Papierform wurde mit Hilfe einer Stoppuhr verdeckt gemessen, sodass die Teilnehmenden die Zeitnahme nicht wahrnehmen konnten. Startpunkt der Messung war das Umblättern der Einführung auf die erste Seite der Teilnahmevereinbarungen. Endpunkt war jeweils das Ansetzen zur Unterschrift. Erfolgte die Unterschrift vor der Betrachtung der Teilnahmevereinbarungen, so wurde dies vermerkt und das Beiseitelegen der Einführung mit angehefteten Teilnahmevereinbarungen als Endpunkt der Zeitmessung angesehen.

Die durchschnittliche Lesedauer beider Gruppen beträgt $M = 52{,}94$ Sekunden ($SD = 52{,}48$). Der Mittelwert für die erste Stichprobe, welche die Teilnahmevereinbarungen in Papierform erhalten hat, beträgt 56,05 Sekunden ($SD = 53{,}41$), wobei die zweite Stichprobe, welche die digitale Form erhalten hat, einen Mittelwert von 49,72 Sekunden ($SD = 52{,}4$) erreicht. Mit Hilfe des Kolmogorov-Smirnov-Tests (Lilliefors, 1967) kann eine Normalverteilung der Lesedauern im Datensatz ($p < .002$; $df = 26$) für die erste Stichprobe und für die zweite Stichprobe ($p < .006$; $df = 26$) ausgeschlossen werden. Aus diesem Grund wird ein nicht parametrischer Mann-Whitney-U-Test durchgeführt (McKnight & Najab, 2010). Dieser ergibt keine signifikanten Unterschiede. Die entsprechenden Ergebnisse des nicht-parametrischen Signifikanztestes sind in Tabelle 2 im Anhang J aufgeführt.

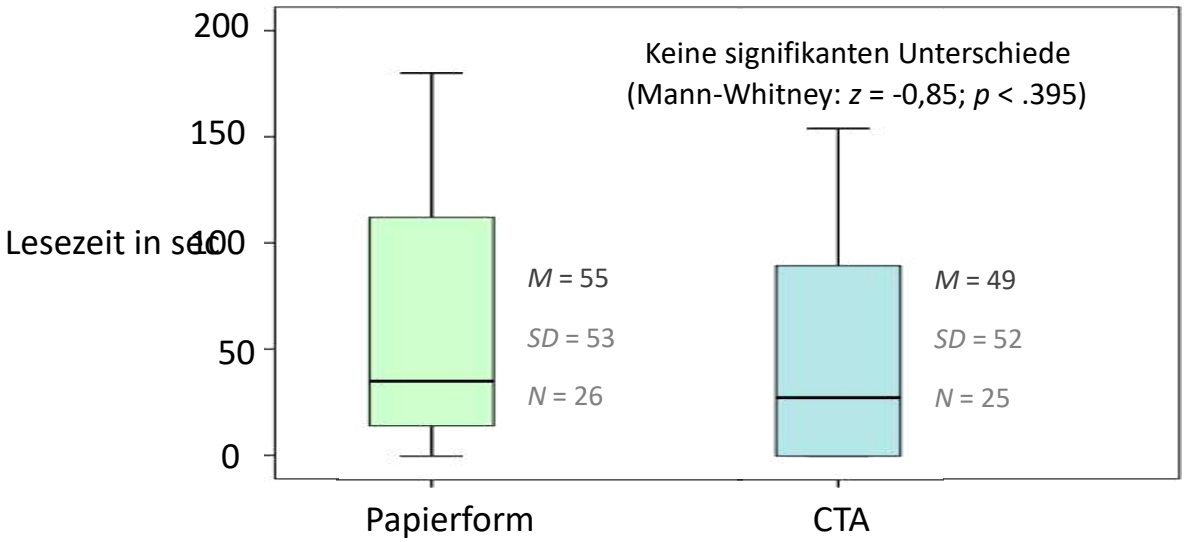


Abbildung 3. Vergleich der Lesedauer zwischen den unterschiedlichen Präsentationsformen.

Aufgrund der Robustheit des t-Tests, die in mehreren Studien bestätigt wird (Pagano, 2010; Salkind, 2010; Wilcox, 2011), wird ein weiterer Vergleich der Lesezeiten der beiden Stichproben mit Hilfe des t-Tests durchgeführt. Dieser zeigt jedoch, bei angenommener Varianzgleichheit nach Levene-Test mit $p < .786$, mit einem Wert von t (49) = 0,427, $p < .671$ und r = 0,06, ebenfalls keine signifikanten Unterschiede auf (s. Tabelle 3 im Anhang J).

Als nächstes wird geprüft, ob ein geschlechtsspezifischer Unterschied in der Lesedauer existiert. An der Untersuchung nahmen N = 20 Männer mit einem Mittelwert von 37,98 Sekunden (SD = 45,55) Lesedauer und N = 31 Frauen mit einem Mittelwert von 62,60 Sekunden (SD = 55,06) teil. Der Kolmogorov-Smirnov-Test kann weder bei den Frauen mit einem Wert von $p < .002$ noch bei den Männern mit einem Wert von $p < .031$ eine Normalverteilung nachweisen. Aus diesem Grund wird ein Mann-Whitney-U-Test durchgeführt, auch dieser ergibt keinen signifikanten Unterschied, U = 227, z = -1,606, $p < .108$ und r = 0,22 (s. Tabelle 4 im Anhang J). Weiterhin ergibt der t-Test für unabhängige Stichproben keinen signifikanten Unterschied (t(49) = -1,664, $p < .102$) bei angenommener Varianzgleichheit, welche durch die mangelnde Signifikanz des Levene-Tests bedingt ist ($p < .08$) (s. Tabelle 5 im Anhang J).

Im nächsten Abschnitt wird geprüft, ob die Gruppe (N = 5), die angegeben hat, Social-Media-Applikationen am häufigsten zu nutzen, einen signifikanten Unterschied hinsichtlich der Lesedauer gegenüber den restlichen Teilnehmenden N = 46 aufweist. Dabei kann keine Normalverteilung der Lesedauer nachgewiesen werden ($p < .001$). Ebenso kann mit Hilfe des Mann-Whitney-U-Tests kein

signifikanter Unterschied der Lesedauer zwischen den beiden Gruppen festgestellt werden (U = 107; z = -0,254, p < .799). Die Ergebnisse sind in Tabelle 6 im Anhang J dargestellt.

Dasselbe Vorgehen wird für die Teilnehmenden mit $N = 20$ angewandt, die angegeben haben, Messenger-Applikationen am häufigsten zu nutzen. Da die Lesedauer nicht normalverteilt ist, erfolgt auch hier ein Mann-Whitney-U-Test, der ebenfalls keine signifikanten Unterschiede feststellen kann (U = 291; z = -0,368; p < .713) (s. Tabelle 7, Anhang J).

Ebenso erfolgt eine Untersuchung von Alter und Lesedauer. Auch hier kann sowohl für das Alter als auch die Lesedauer mittels eines Kolmogorov-Smirnov-Tests mit jeweils p < .000 keine Normalverteilung nachgewiesen werden. Aus diesem Grund wird sich für eine Korrelationsanalyse nach Spearman-Rho-Test (Puth et al., 2015) entschieden, welcher einen negativen Zusammenhang von r = -0,201 ergibt. Allerdings kann hier keine Signifikanz mit p < .156 aufgewiesen werden, sodass nur von einer Tendenz ausgegangen werden kann (s. Tabelle 8 im Anhang J).

Ferner wird untersucht, ob ein Zusammenhang zwischen der gewählten Vergütung und der Lesedauer vorherrscht. Der Mittelwert für die Vergütung beträgt 9,59 Euro (SD = 1,577) mit einem Minimum von 2 Euro und einem Maximum von 10 Euro. Der Test auf Normalverteilung lässt weder bei der Lesedauer noch bei der Vergütung mit jeweils p < .000 auf eine solche schließen. Auch hier erfolgt eine Korrelationsanalyse mit Spearman-Rho-Test, welche einen positiven Zusammenhang von r = 0,200 ergab. Somit kann ebenfalls nur von einer Tendenz gesprochen werden, da das Ergebnis mit p < .159 nicht signifikant ausfällt. Die Ergebnisse sind in Tabelle 9 im Anhang J dargestellt.

Ebenso wird mittels eines Spearman-Rho-Tests mit N = 51 untersucht, ob es eine Korrelation zwischen der Häufigkeit des Lesens der AGB und deren Lesedauer gibt. Hierbei kann keine signifikante Korrelation nachgewiesen werden (r = -0,084; p < .556). Die detaillierten Ergebnisse befinden sich in Tabelle 10 im Anhang J.

Im Anschluss wird mit ebenfalls N = 51 geprüft, ob ein Zusammenhang zwischen den Begründungen für die Häufigkeit der Befassung mit den AGBs und der Lesedauer vorzufinden ist. Hierzu werden, wie schon in Abschnitt 5.6.5 beschrieben, aus den Freitextantworten der Versuchspersonen auf die Frage 8 des Fragebogens 11 Kategorien gebildet.

Zu den Begründungen des Nichtlesens gehören:

- Das Vertrauen in die Anbieter der Applikation, eine zu geringe Motivation,
- der Fakt, dass in jedem Fall zugestimmt werden müsse, wenn das Produkt verwendet werden möchte,

- dass die AGBs in einer zu komplizierten Sprache geschrieben seien,
- dass die AGBs zu lang seien und
- dass der Text immer gleich sei.

Zu den Begründungen des Lesens gehören:

- Die Kontrolle der AGBs,
- mögliche versteckte anfallende Kosten,
- die Wahrung des Datenschutzes, weil den Anbietern misstraut wird und
- das Beruhigen des Gewissens.

Im Falle der Antwortkategorie „Zu komplizierte Sprache“ mit $n = 9$ Personen liegt eine signifikante Korrelation mit $r = 0{,}333$ und $p < .017$ vor. Für die anderen 10 Kategorien kann keine signifikante Korrelation mit der Lesedauer festgestellt werden. Die Ergebnisse hierzu befinden sich in Tabelle 11 und Tabelle 12 in Anhang J.

Im nächsten Schritt erfolgt eine Analyse der Lesedauer. Hierbei werden die Angaben der geschätzten allgemeinen Lesedauer von AGBs (Frage Nr. 10 des Fragebogens) mit der Angabe zur geschätzten Lesedauer der Teilnahmevereinbarungen für das Täuschungsexperiment im Interview und deren tatsächlicher Messung verglichen. Um möglichst valide Ergebnisse zu erhalten, wurden die Personen, welche im Interview zur Frage der geschätzten Lesedauer der Teilnahmevereinbarungen keine Angabe gemacht haben, aus der Stichprobe entnommen. Die verbleibende Stichprobe hat eine Größe von $N = 46$. Zum besseren Vergleich wurde ein Boxplot-Diagramm erstellt (Abbildung 4). Zusätzlich wurden Mittelwerte und Standardabweichungen zu den entsprechenden Zeiten angegeben. Die Zeiten, die sich jeweils signifikant unterscheiden, wurden mit einer Klammer und einem Asterisk gekennzeichnet.

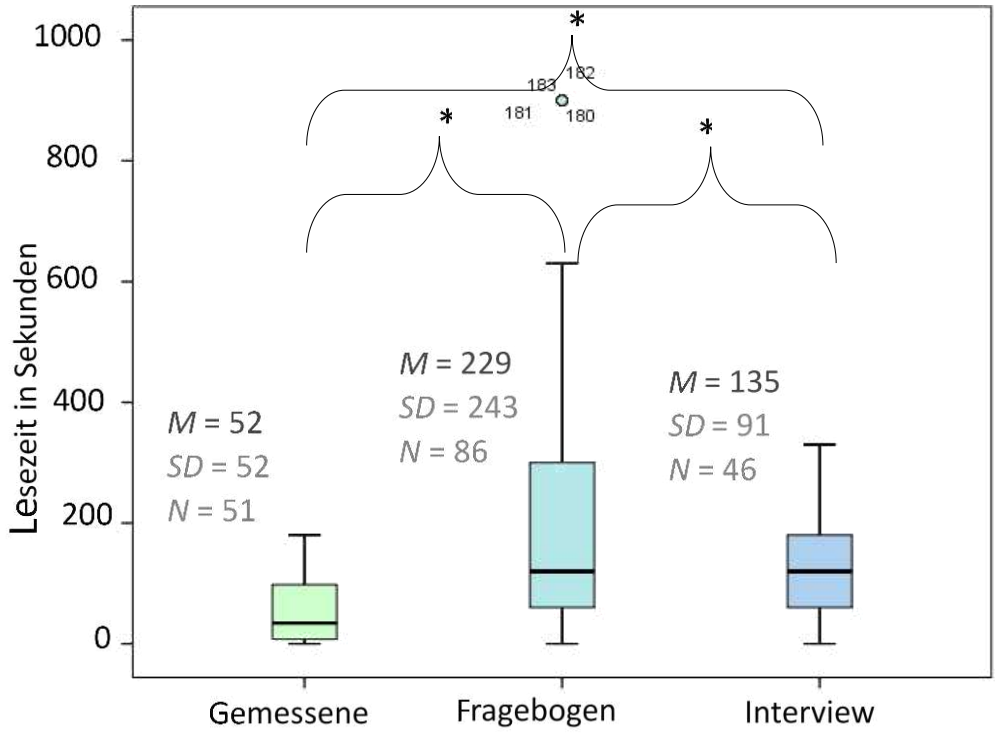


Abbildung 4. Vergleich der gemessenen, angegebenen und abgefragten Zeiten zum Lesen der Teilnahmevereinbarungen.

Diese Abbildung illustriert die durchschnittlichen Lesezeiten in Sekunden, welche die Teilnehmenden benötigt haben, um die Teilnahmevereinbarungen durchzulesen. Dabei entspricht die gemessene Lesezeit der Zeit, die im Rahmen der Studie von den Teilnehmenden investiert wurde, um die Teilnahmevereinbarungen zu durchsichten, während die Zeiten des Fragebogens und des Interviews eigenständig von den Teilnehmenden angegeben wurden.

Bei dem Vergleich der gemessenen Lesedauer (M = 53,38; SD = 53,46) mit den Angaben der N = 46 Versuchspersonen zur geschätzten durchschnittlichen Lesedauer von 135,76 Sekunden (SD = 91,62), lässt sich mittels eines Wilcoxon-Tests (Fix & Hodges Jr, 1955) ein signifikanter Unterschied mit einem großen Effekt feststellen (z = -5,545; p < .000; r = 0,58). Somit liegt die tatsächlich gemessene Lesedauer der Teilnahmevereinbarungen deutlich unter der geschätzten Lesedauer.

Bei dem Vergleich der geschätzten allgemeinen Lesedauer von AGBs werden die Ausreißer mit einer geschätzten Lesedauer von über 2100 Sekunden aus der Stichprobe entfernt. Die Entscheidung basiert auf der durchschnittlichen Lesedauer von 211 (±32) Wörter pro Minute bei deutschsprachigen Texten (Radner et al., 1998). Die durchschnittliche Länge der AGBs im Bereich der Social Media beträgt 7444 Wörter (Forbrukerrådet, 2016). Wird die Anzahl der Wörter von 7444 durch die Anzahl der gelesenen

Wörter pro Minute, 211, dividiert, resultiert ein Wert von 2100 Sekunden. So werden alle Ausreißer, die deutlich über diesem Wert lagen, entfernt.

Ebenso lässt sich mit Hilfe des Wilcoxon-Tests mit *N* = 44 ein signifikanter Unterschied mit einem großen Effekt zwischen der gemessenen Lesedauer (*M* = 52,9; *SD* = 52,5) und der im Fragebogen zu Frage 10 angegebenen aufgewendeten Zeit (*M* = 229,1; *SD* = 243,8) feststellen (*z* = -4,995; *p* < .00; *r* = 0,75).

Ferner wird ein weiterer Wilcoxon-Test durchgeführt, um zu überprüfen, ob sich die im Interview geschätzte Lesedauer direkt nach dem Täuschungsexperiment mit *N* = 46 *(M* = 135,76; *SD* = 91,62) signifikant mit den Angaben der *N* = 46 Versuchspersonen zur angegebene Lesedauer (*M* = 215,57; *SD* = 204) Sekunden unterscheidet (*z* = -2,119; *p* < .034; *r* = 0,31). Zwischen der im Interview geschätzten Lesedauer und der gemessene Lesedauer wird ebenfalls eine Signifikanz festgestellt (*z* = -5,545; *p* = .000). Eine Zusammenfassung der Ergebnisse ist in Tabelle 13 im Anhang J wiederzufinden.

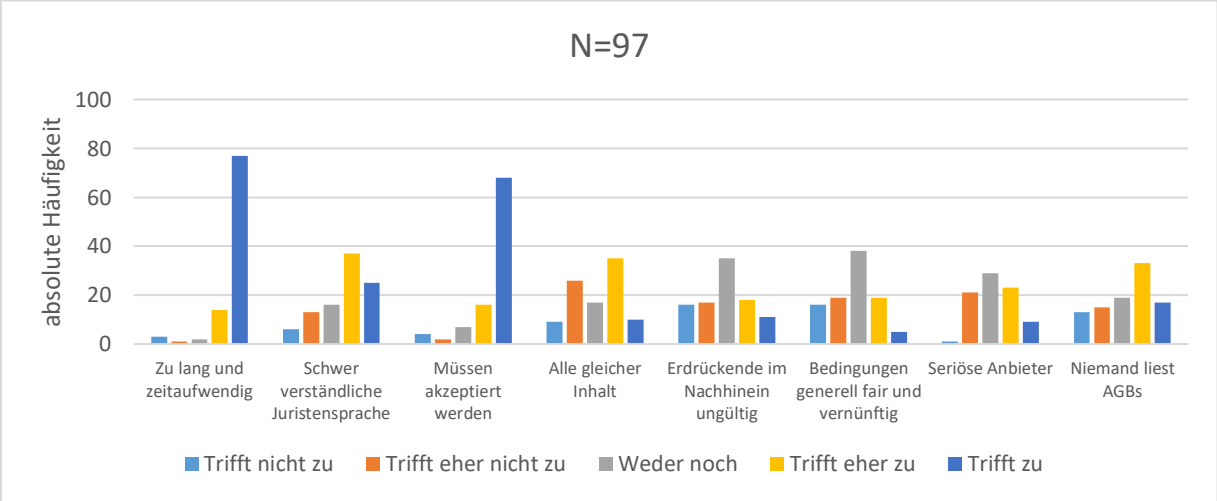


Abbildung 5. Verteilung der Antworten zu den sozialen Repräsentationen.

Das Diagramm zeigt die Häufigkeiten der Übereinstimmung mit den sozialen Repräsentationen seitens der Teilnehmenden (*N* = 97). Auffällig hierbei ist, dass der sozialen Repräsentation „AGBs sind zu lang und zeitaufwendig“ (*n* = 77) sowie „Die Kunden müssen die AGBs akzeptieren, wenn sie das zugehörige Produkt erwerben wollen“ (*n* = 68) am meisten als zutreffend gewählt wurden. Der sozialen Repräsentation, welche besagt, dass vor Gericht erdrückende Bedingungen im Nachhinein für ungültig erklärt werden (*n* = 18), sowie der Repräsentation, welche besagt, dass die Bedingungen der Anbieter in den AGBs generell fair und vernünftig sind (*n* = 19), wurde am wenigsten zugestimmt. Insgesamt ist jedoch zu sehen, dass die sozialen Repräsentationen den Meinungen der Versuchsteilnehmenden entsprechen.

5.7.2 Zusammenhang zwischen dem Alter und den Begründungen für den Umgang mit den Teilnahmevereinbarungen sowie der Nutzung von bestimmten Applikationskategorien

In diesem Abschnitt soll näher untersucht werden, ob Zusammenhänge zwischen dem Alter und den Begründungen des Lesens bzw. nicht Lesens, welche im Abschnitt 5.7.1 aufgeführt wurden, herrschen. Die entsprechenden Korrelationen ergeben allesamt kein signifikantes Ergebnis.

Darüber hinaus wird getestet, ob das Alter mit der Nutzung von bestimmten Applikationskategorien korreliert. Die Applikationen werden kategorisiert in Messenger, Social Media, Kartendienste, Wetter, E-Mail, Nachrichten, Browser, Sonstige und keine Applikationen.

Es kann ein signifikanter Zusammenhang zwischen der Nutzung von Messenger Applikationen mit dem Alter (N = 97; M = 28,13; SD = 8,96) festgestellt werden. Das Alter korreliert negativ mit der Nutzung von Messenger Applikationen (r = -0,349; p < .000). Alle weiteren zuvor erwähnten Tests sind nicht signifikant ausgefallen. Eine detaillierte Tabelle mit den Ergebnissen befindet sich im Anhang J (s. Tabelle 14, Anhang J).

5.7.3 Zusammenhang zwischen Geschlecht und Begründung

In diesem Abschnitt soll näher untersucht werden, ob Zusammenhänge zwischen dem Geschlecht und den Begründungen des Lesens bzw. nicht Lesens bestehen.

Es werden die Korrelationen zwischen dem Geschlecht und den Begründungen, warum die Teilnehmenden die AGBs lesen bzw. nicht lesen, getestet. Auf Grund der dichotomen Eigenschaften bei den Datensätzen werden die Korrelationen mit Hilfe des Cramers V berechnet.

Darüber hinaus wird mit Hilfe punktbiserialer Korrelationen getestet, ob das Geschlecht mit der Nutzung von bestimmten Applikationskategorien zusammenhängt. Die Applikationen werden kategorisiert in Messenger, Social Media, Kartendienste, Wetter, E-Mail, Nachrichten, Browser, Sonstige und keine Applikationen.

Keiner dieser Tests ergibt ein signifikantes Ergebnis. Detaillierte Tabellen (s. Tabelle 25, Tabelle 26 und Tabelle 27) mit den Ergebnissen befinden sich im Anhang J.

5.7.4 Zeitpunkt der geleisteten Unterschrift und Begründungen für den Umgang mit den Teilnahmevereinbarungen

In diesem Abschnitt wird der Zeitpunkt der geleisteten Unterschrift mit einer Vielzahl von anderen Faktoren verglichen. Die Teilnehmenden, denen die Teilnahmevereinbarung in Papierform vorgelegt wurde, *N* = 26, haben das Dokument teilweise erst nach der geleisteten Unterschrift betrachtet (*N* = 16). Demnach findet die Gruppe der Teilnehmenden, denen die digitale Teilnahmevereinbarung vorgelegt wurde, hierbei keine Beachtung.

Zuerst wird betrachtet, ob es einen signifikanten Unterschied bezüglich des Alters und des Zeitpunktes der geleisteten Unterschrift gibt. Das durchschnittliche Alter der Gruppe, welche die Unterschrift vor dem Durchlesen der Teilnahmevereinbarungen geleistet hat, beträgt *M* = 34,31 (*SD* = 12,126). Der Altersdurschnitt der Gruppe, welche die Unterschrift nach dem Durchlesen der Teilnahmevereinbarungen geleistet hat, beträgt *M* = 33,30 (*SD* = 8,858). Die Verteilung des Alters der Gruppenteilnehmenden, welche die Teilnahmevereinbarungen schriftlich vorgelegt bekommen haben, entspricht einer Normalverteilung, welches mit dem Kolmogorov-Smirnov-Test nachgewiesen werden kann ($p < .140$). Somit wird sich dazu entschieden, einen t-Test für unabhängige Stichproben anzuwenden. Dieser ergibt keinen signifikanten Unterschied ($t(24) = -0{,}228$; $p < .299$; $r = 0{,}047$) (s. Tabelle 15, Anhang J).

Anschließend wird mit Hilfe der Pearson-Korrelation (Benesty et al., 2009) geprüft, ob ein Zusammenhang zwischen dem Geschlecht und dem Zeitpunkt der geleisteten Unterschrift besteht. Der Test kann keine signifikante Korrelation mit $r = 0{,}098$ und $p < .635$ feststellen (s. Tabelle 16, Anhang J).

Ferner wird geprüft, ob ein signifikanter Unterschied in der Lesezeit zwischen den beiden Gruppen zu finden ist. Mit einem Mittelwert von 82,66 Sekunden (*SD* = 60,94) liegt der Mittelwert der Lesedauer von den Teilnehmenden, die erst nach dem Betrachten der Teilnahmevereinbarungen die Unterschrift geleistet haben, deutlich über denen, welche vor dem Lesen unterschrieben haben *(M* = 39,40 Sekunden, *SD* = 41,93). Der Kolmogorov-Smirnov-Test auf Normalverteilung ergibt normalverteilte Daten bei der Stichprobe, welche den Text nach dessen Betrachtung unterschrieben hat ($p < .200$), jedoch nicht für die Stichprobe, welche zuerst unterschrieben und dann gelesen hat ($p < .011$). Somit bedarf es der Durchführung des nicht parametrischen Mann-Whitney-U-Tests, um auf einen signifikanten Unterschied zwischen den Mittelwerten zu prüfen. Hier kann ebenfalls kein signifikanter Unterschied ($U = 46{,}5$; $z = -1{,}766$; $p < .077$) festgestellt werden (s. Tabelle 17, Anhang J).

5.7.5 Gewählte Vergütung

Aus dem Ankreuzbogen zur Weitergabe der persönlichen Daten resultiert ein Mittelwert von 9,59 Euro (*SD* = 1,58) bei einer Skala von 2 bis 10 Euro. Bei näherer Betrachtung der Häufigkeitsverteilung ist festzustellen, dass nur zweimal die geringste Vergütung gewählt wurde, welche gleichzeitig bedeutet, dass die Daten nur für diese Studie verwendet werden und an keinerlei Dritte ausgehändigt werden. Die meistgewählte Vergütung wurde von insgesamt 44 Teilnehmenden gewählt und entspricht mit 10 Euro der höchsten und somit auch der freizügigsten Weitergabe der persönlichen Daten. Lediglich fünf Teilnehmende wählten 9 Euro als finanzielle Gegenleistung und schlossen somit internationale Unternehmen von dem Erhalt ihrer privaten Daten aus. Nur zwei Teilnehmende wählten 2 Euro als finanzielle Gegenleistung und gaben somit ihre Daten nur für die Verwendung innerhalb dieser Dissertation frei.

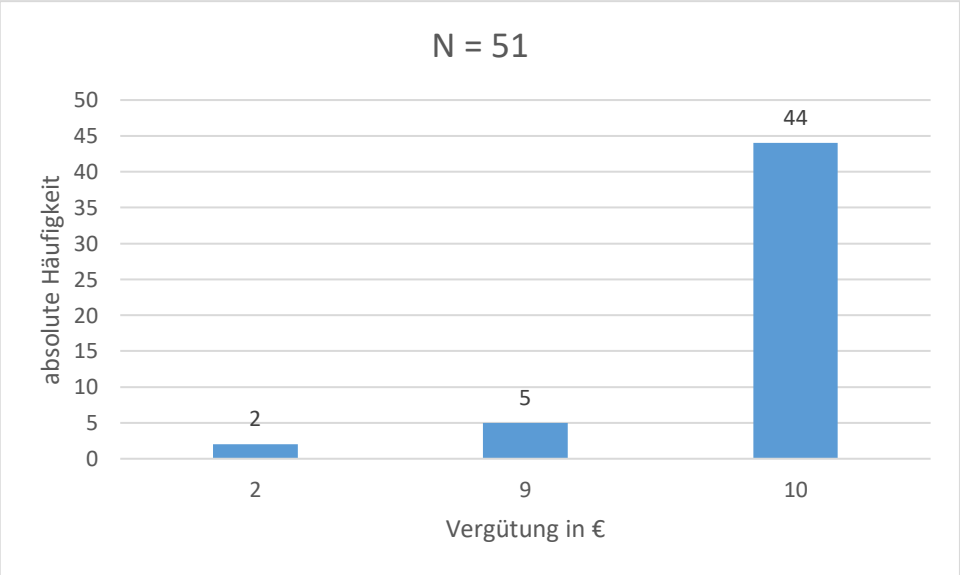


Abbildung 6. Absolute Häufigkeiten der von den Teilnehmenden angegebenen Vergütung.

Dieses Balkendiagramm zeigt die absoluten Häufigkeiten der von den Teilnehmenden angegebenen Vergütung. Die fehlenden Werte der Vergütungen wurden von keinen Teilnehmenden gewählt, sodass diese im Diagramm nicht aufgeführt wurden.

In einem folgenden Schritt wird untersucht, ob es geschlechtsspezifische Unterschiede bei der gewählten Vergütung gibt. Bei Frauen liegt der Mittelwert bei 9,39 Euro (*SD* = 0,308), während er bei Männern bei 9,90 Euro (*SD* = 1,995) liegt. Für beide Geschlechter kann mittels Kolmogorov-Smirnov-Test keine Normalverteilung der Vergütung nachgewiesen werden, jeweils $p < .001$. Ein signifikanter Unterschied zwischen Geschlecht und gewählter Vergütung kann mittels Mann-Whitney-U-Test nicht nachgewiesen werden, $U = 289$, $z = -0{,}678$ und $p < .498$ (s. Tabelle 18 im Anhang J).

Anschließend wird geprüft, ob altersspezifische Unterschiede hinsichtlich der gewählten Vergütung vorliegen. Der Altersdurchschnitt beträgt 31,27 Jahre (*SD* = 10,224). Der Test auf Normalverteilung lässt weder beim Alter noch bei der Vergütung mit jeweils $p < .001$ auf eine solche schließen. Die Korrelationsanalyse nach Spearman-Rho ergibt einen negativen Zusammenhang von $r = -0{,}112$, wobei das Ergebnis nicht signifikant ist ($p < .434$) und nur als Tendenz angesehen werden kann (s. Tabelle 19 im Anhang J).

Es wird untersucht, ob signifikante Unterschiede hinsichtlich der Vergütung zwischen den Teilnehmenden, denen die Einverständniserklärung als CTA und denjenigen, denen diese in Papierform präsentiert wurde, bestehen. Der Mittelwert für die Stichprobe, welche die Einverständniserklärung als CTA erhalten hat, *N* = 25, ergibt 9,52 Euro (*SD* = 1,610), wobei das Minimum hier 2 Euro und das Maximum 10 Euro beträgt. Die zweite Stichprobe, mit der Einverständniserklärung in Papierform, *N* = 26, ergibt einen Mittelwert von 9,65 Euro (*SD* = 1,573), wobei Minimum und Maximum gleichbleiben. Da für die Vergütung keine Normalverteilung vorliegt, wird ein Mann-Whitney-U-Test durchgeführt. Dieser kann keinen signifikanten Unterschied hinsichtlich der Vergütung und der Form der Einverständniserklärung feststellen, $U = 286{,}5$, $z = -1{,}214$ und $p < .225$ (s. Tabelle 20, Anhang J).

Weiterhin wird geprüft ob, es einen signifikanten Unterschied bezüglich der Vergütung zwischen den Teilnehmenden, *N* = 26, die vor dem Durchlesen bzw. nach dem Durchlesen die Unterschrift für die Einverständniserklärung geleistet haben, besteht. Der Mittelwert für die Gruppe, welche die Unterschrift erst nach dem Lesen der Einverständniserklärung geleistet hat, *N* = 10, beträgt 9,20 Euro (*SD* = 2,530), mit einem Minimum von 2 Euro und einem Maximum von 10 Euro. Bei der Gruppe, welche die Unterschrift bereits vor dem Lesen der Einverständniserklärung leistete, *N* = 16, beträgt der Mittelwert 9,94 Euro (*SD* = 0,250) mit einem Minimum von 9 Euro und einem Maximum von 10 Euro. Auch hier liegt keine Normalverteilung der Vergütung vor ($p < .001$). Zur Überprüfung der Signifikanz wird ein Mann-Whitney-U-Test durchgeführt, welcher zu einem negativen Ergebnis diesbezüglich führt, $U = -0{,}399$ und $p < .856$ (s. Tabelle 21, Anhang J).

Im folgenden Abschnitt wurde mit *N* = 51 geprüft, ob es einen signifikanten Unterschied bezüglich der Vergütung und der Nutzung bestimmter Applikationsgruppen bzw. dem Misstrauen in diese gibt. Bei den Applikationsgruppen handelt es sich um Messenger, also Applikationen, die überwiegend zur Kommunikation verwendet werden, wie etwa WhatsApp, und um Social Media Applikationen, bei denen das Teilen und Bewerten von Inhalten im Vordergrund steht, beispielsweise Facebook und Instagram. Bei keinem der ausgeführten Mann-Whitney-U-Tests kann ein signifikantes Ergebnis festgestellt werden. Eine übersichtliche Auflistung der Ergebnisse ist in Tabelle 22 im Anhang J angehangen.

Auch wird mit *N* = 51 untersucht, ob es Korrelation zwischen den Begründungen für die Häufigkeit der Befassung mit den AGBs und der gewählten Vergütung gibt. Hierzu werden, wie schon in Abschnitt 5.6.5 beschrieben, aus den Freitextantworten der Versuchspersonen 11 Kategorien gebildet. In keinem der Fälle kann eine signifikante Korrelation festgestellt werden. Eine übersichtliche Auflistung der Ergebnisse ist in Tabelle 23 (s. Anhang J) angehangen.

Zwischen der Gruppe, die Messenger Applikationen am häufigsten nutzt, und der Gruppe, die diese nicht am häufigsten nutzt, kann mit dem Mann-Whitney-U-Test kein signifikanter Unterschied bezüglich der Vergütung festgestellt werden. Ein ähnliches Ergebnis kann zwischen der Gruppe, die Social Media Applikationen am häufigsten nutzt, und der Gruppe, die diese nicht am häufigsten nutzt, mit Hilfe des Mann-Whitney-U-Tests gefunden werden. Auch hier resultiert kein signifikanter Unterschied. Ebenso kann kein signifikanter Unterschied bezüglich der Vergütung zwischen der Gruppe, die den Messenger Applikationen am wenigsten vertraut, und der Gruppe, die diesen nicht am wenigsten vertraut, mit dem Mann-Whitney-U-Test festgestellt werden. Dasselbe gilt für die Gruppe, die den Social Media Applikationen am wenigsten vertraut, und der Gruppe, die diesen nicht am wenigsten vertraut. Auch hier kann kein signifikanter Unterschied bezüglich der Vergütung mit Hilfe des Mann-Whitney-U-Tests festgestellt werden. Tabelle 24 im Anhang J zeigt die Ergebnisse.

Es werden die Zusammenhänge zwischen der Vergütung und den gebildeten Kategorien der Freitextantworten, welche die Begründungen des Lesens bzw. nicht Lesens enthalten und bereits im Abschnitt 5.7.1 aufgeführt wurden, getestet. Keiner dieser Tests ergibt ein signifikantes Ergebnis. Eine detaillierte Tabelle (s. Tabelle 23) mit den Ergebnissen befindet sich im Anhang J.

Die Durchführung weiterer Tests betreffend das Vertrauen in die Anbieter der Applikation und der Tatsache, dass in jedem Fall zugestimmt werden muss, wenn das Produkt verwendet werden möchte, ist nicht möglich, weil hierfür die Daten aufgrund der Nichtangabe seitens der Teilnehmenden, fehlen. Ähnlich verhält es sich mit den Tests bezüglich möglicher versteckter anfallender Kosten und bezüglich des zu beruhigenden Gewissens.

5.7.6 Interview

Im folgenden Abschnitt werden die Antworten der *N* = 51 Teilnehmenden auf das Interview direkt nach dem Täuschungsexperiment dargestellt.

18 Teilnehmende (35,3 %) gaben an, verunsichert zu sein, wobei diese alle das Experiment selbst als Grund für ihre Verunsicherung anführten. Ebenso gaben 23 Teilnehmende (45,1 %) an, dass ihnen in

Bezug auf das Experiment etwas merkwürdig vorgekommen ist. Bei beiden Fragen wurden die Teilnahmevereinbarungen nicht als Ursache für das Empfinden angegeben.

Ebenso wurden die Teilnehmenden gefragt, ob sie die Teilnahmevereinbarungen gelesen haben. Dies beantworteten 26 Personen (51,0 %) mit Ja, weitere 21 (41,2 %) gaben an, die Teilnahmevereinbarungen zumindest überflogen zu haben, nur drei Personen (5,9 %) gaben an, die Teilnahmevereinbarungen nicht gelesen zu haben. Eine Person (2,0 %) hat keine präzise Antwort zu dieser Frage gegeben. Einige der Teilnehmenden begründeten ihr Leseverhalten, wobei sieben (13,7 %) erklärten, dass die Texte in AGBs immer die gleichen seien, weitere vier Personen (7,8 %) empfanden den Text als zu lang, um ihn ganz zu lesen. Eine Übersicht der absoluten Häufigkeiten zeigt die Abbildung 7.

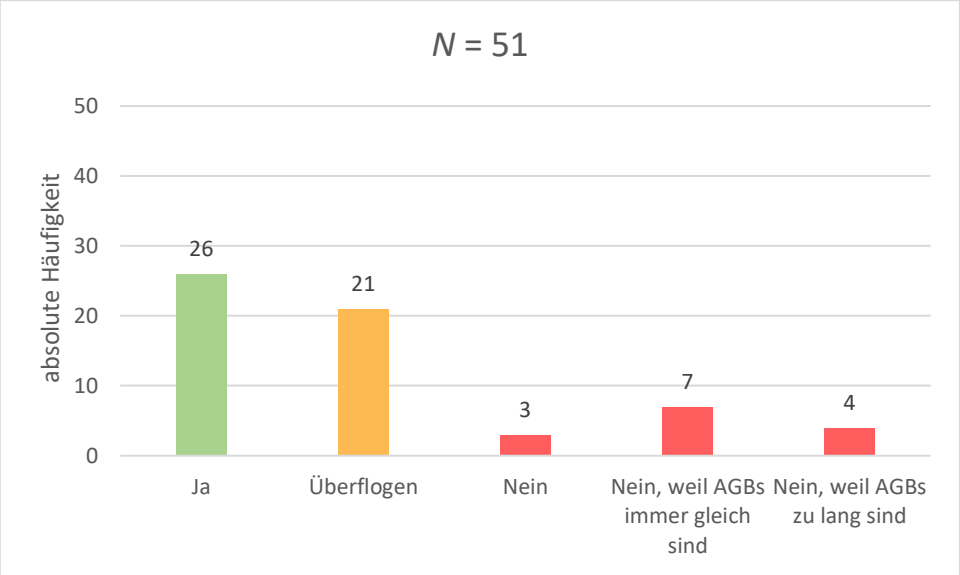


Abbildung 7. Absolute Häufigkeiten der Teilnehmenden, welche angaben, die Teilnahmevereinbarung gelesen, nicht gelesen oder überflogen zu haben.

Dieses Balkendiagramm bietet einen Überblick über die absolute Häufigkeit der Teilnehmenden, welche angegebenen haben, die Teilnahmevereinbarung gelesen, nicht gelesen oder überflogen zu haben. Darüber hinaus wurden die zwei häufigsten Gründe implementiert, welche nach den Teilnehmenden ausschlaggebend für das Unterlassen des Lesens der Teilnahmevereinbarung waren.

Darüber hinaus wurde an dieser Stelle nach einer Einschätzung der zum Lesen der Teilnahmevereinbarungen aufgewendeten Zeit gebeten. Die Auswertung dieser Einschätzung erfolgte bereits im Abschnitt 5.7.2.

Weiterhin wurden die Teilnehmenden gefragt, ob ihnen an den Teilnahmevereinbarungen etwas aufgefallen sei. Insgesamt 10 Personen (19,6 %) beantworteten dies positiv, wobei drei Personen (5,9 %) angaben, dass die Teilnahmevereinbarungen detaillierter als üblich sein, nur eine Person (2,0 %) empfand die Regelungen zur Datenweitergabe als auffällig, eine weitere Person (2,0 %) gab an, dass ihr viele Teile der Teilnahmevereinbarungen als unwichtig erschienen bzw. sich wiederholten, weitere fünf Personen (9,8 %) erwähnten besondere Stellen der Teilnahmevereinbarungen, die ihnen aufgefallen sind. Eine Übersicht der absoluten Häufigkeiten zeigt die Abbildung 8.

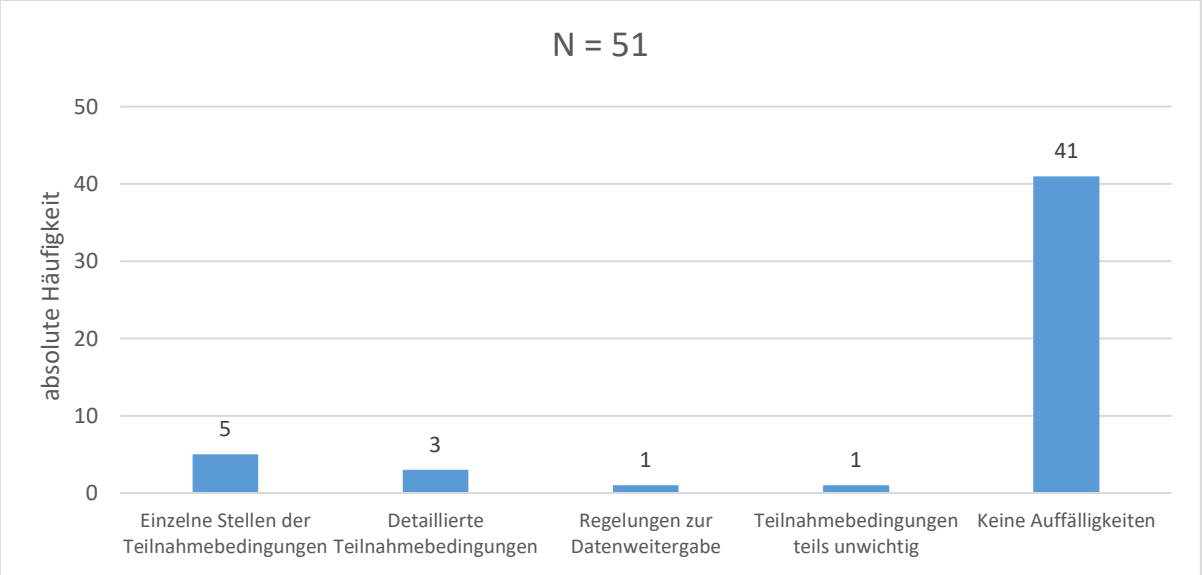


Abbildung 8. Absolute Häufigkeiten der von den Teilnehmenden angegebenen Auffälligkeiten in den Teilnahmevereinbarungen.

Dieses Balkendiagramm bietet einen Überblick über die absolute Häufigkeit der Antworten seitens der Teilnehmenden auf die Frage, ob ihnen an den Teilnahmevereinbarungen etwas aufgefallen ist.

Auf die Frage, ob sie beim Unterschreiben der Einverständniserklärung gezögert hätten, antworteten vier Personen (7,8 %) mit Ja. Zuletzt wurden die Teilnehmenden gefragt, ob sie sich beim Preisgeben ihrer persönlichen Daten während des Täuschungsexperimentes unwohl fühlten. 14 Personen (27,5 %) gaben an, dass dies der Fall war. Als Grund für das Unwohlsein gaben acht der Personen (15,7 %) die Preisgabe ihrer persönlichen Präferenzen an, weitere vier Personen (7,8 %) gaben an, dass der Mangel an Alternativen bzw. der Zwang sich für einen Begriff zu entscheiden zu Unwohlsein geführt hat. Von den Teilnehmenden, die angegeben hatten, kein Unwohlsein zu empfinden, begründeten dies sechs (11,8 %) damit, dass ihrer Meinung nach keine sensiblen Daten erhoben worden sind, weitere zwei Personen (3,9 %) gaben an, dass die Daten bereits woanders erhoben worden sind, eine Person (2,0 %) verwies auf die zugesicherte Anonymität.

5.7.7 Fragebogen

Im Folgenden wird die deskriptive Auswertung des Fragebogens, der insgesamt von 97 Teilnehmenden ausgefüllt wurde, näher betrachtet. Hiervon füllten 51 Personen (52,3 %) den Fragebogen im Anschluss an das Täuschungsexperiment aus, die anderen 46 (47,4 %) als alleinstehenden Internetfragebogen. Von den 97 befragten Personen waren 44 männlich (45,4 %) und 53 weiblich (54,6 %).

Die Teilnehmenden wurden gefragt, welches Betriebssystem sie auf ihren mobilen Endgeräten verwenden. Hierbei standen die Antworten „Android“, „iOS“ und „Windows“, sowie „Andere/Unbekannt“ zur Auswahl. Mehrfachantworten waren möglich, wovon 19 Personen (19,6 %) Gebrauch machten. „Android“ wurde hierbei mit 66 Nennungen (68 %) am häufigsten als verwendetes Betriebssystem angegeben, gefolgt von „iOS“ mit 27 Nennungen (27,8 %) und „Windows“ mit 23 Nennungen (23,7 %). Nur drei Personen (3,1 %) gaben an, ihr Betriebssystem nicht zu kennen oder verwendeten ein anderes.

Es folgte eine Frage nach der meistgenutzten Applikation, wobei hier ein Freitextfeld Verwendung fand und sich nicht alle teilgenommenen Personen auf die Angabe nur einer Applikation beschränkten. 49 Personen (50,5 %) gaben an, den Messenger-Dienst „WhatsApp“ zu nutzen. Sieben Personen (7,2 %) gaben die Antwort „keine“ an, was somit die zweithäufigste Antwort ist. Da jenseits von der Antwort „WhatsApp“ die Häufigkeiten sehr gering ausfallen, viele Applikationen aber nahezu dieselbe Funktion erfüllen, werden sie in Kategorien zusammengeführt. Demnach nutzen 54 Personen (55,7 %) am häufigsten Messenger-Dienste, welche auch die Applikation „WhatsApp“ inkludiert, also Applikationen, die überwiegend dem Übersenden von Textnachrichten dienen. Weitere 10 Antworten (10,3 %) werden der Kategorie Social-Media zugeordnet. In diesen Applikationen besteht die Möglichkeit, Inhalte zu veröffentlichen und zu bewerten. Gefolgt wird dies von der Kategorie Browser mit sechs Antworten (6,2 %) und der Kategorie E-Mail-Applikationen mit fünf Antworten (5,2 %). Weitere vier Antworten (4,1 %) werden Kartendiensten zugeordnet, also Applikationen, die der Navigation dienen. Um einen besseren Überblick über die Verteilung der Kategorien zu schaffen, werden die kategorisierten Antworten in ein Balkendiagramm eingebettet (s. Abbildung 9). Eine komplette Auflistung der Antworten befindet sich in Anhang M.

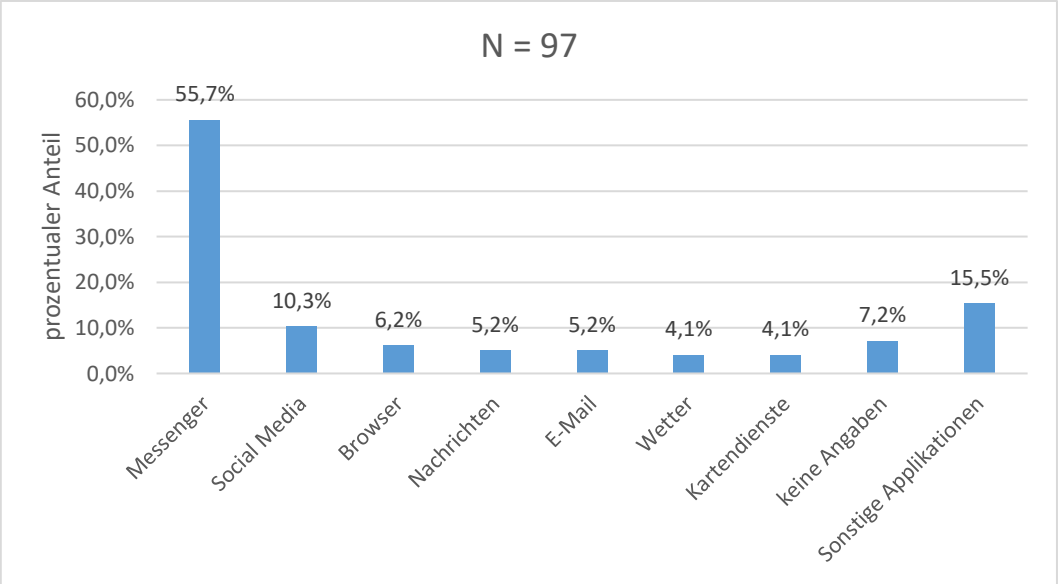


Abbildung 9. Kategorien, der auf dem eigenen mobilen Endgerät am häufigsten verwendeten Applikationen.

Dieses Balkendiagramm bietet einen Überblick über den prozentualen Anteil der Applikationen, bei denen angegeben wurde, dass sie am häufigsten auf dem eigenen mobilen Endgerät verwendet werden. Hierbei wird der Prozentsatz von 100 überschritten, da es den Teilnehmenden möglich war, im Freitextfeld Mehrfachangaben zu tätigen.

Im Anschluss wurde nach dem Namen der Applikation gefragt, welcher am wenigsten vertraut wird. Die Antwort wurde wieder über ein Freitextfeld gegeben. „Facebook“ stellt sich hier mit 29 Nennungen (29,9 %) als die Applikation heraus, der am wenigsten vertraut wird, gefolgt von „WhatsApp“ mit 22 Nennungen (22,7 %). Zehn Personen (10,3 %) gaben bei dieser Frage keine Antwort an. Die komplette Auflistung der Antworten befindet sich in Anhang N. Auch hier werden die Antworten in Kategorien zusammengefasst. 34 Personen (35,1 %) vertrauen demnach Social-Media Applikationen am wenigsten, gefolgt von Messenger Applikationen mit 28 Nennungen (28,9 %). Lediglich 6 Personen (6 %) misstrauen den Kartendiensten wobei 20 der Personen (20,6 %) sonstigen Applikationen misstrauen, die hier jedoch nicht einzeln aufgeführt werden. Zu besseren Übersicht werden die Ergebnisse in der Abbildung 10 illustriert. Eine Auflistung aller Antworten ist im Anhang N zu finden.

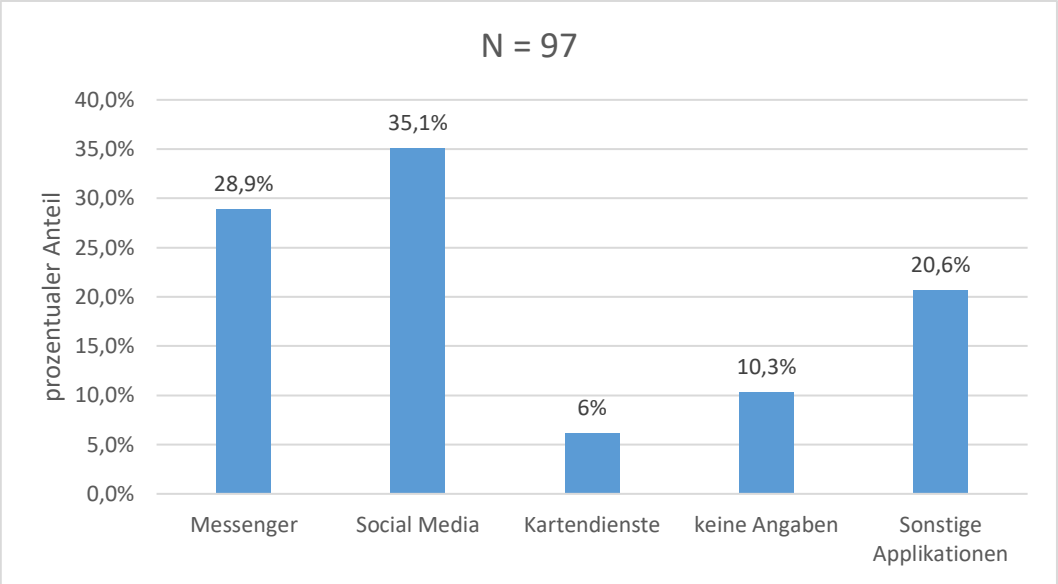


Abbildung 10. Kategorien der Applikationen, denen auf dem eigenen mobilen Endgerät am meisten misstraut wird.

Dieses Balkendiagramm bietet einen Überblick über den prozentualen Anteil der Applikationen, denen am meisten misstraut wird. Hierbei wird der Prozentsatz von 100 ebenfalls überschritten, weil es den Teilnehmenden möglich war, im Freitextfeld Mehrfachangaben zu tätigen.

Weiterhin wird erhoben, wie häufig die Teilnehmenden Applikationen auf ihren Endgeräten installierten. Hierbei wurde darauf hingewiesen, dass Neuinstallationen von Interesse sind, nicht Updates von bereits installierten Applikationen. Als überwiegende Mehrheit gaben 65 Personen (67 %) an, monatlich neue Installationen durchzuführen, gefolgt von 17 Personen (17,5 %), welche angaben, niemals neue Applikationen zu installieren. 13 Personen (13,4 %) antworteten, dass sie wöchentlich neue Applikationen installierten. Nur zwei der befragten Personen (2,1 %) gaben an, täglich neue Applikationen zu installieren.

Die Frage 7 des Fragebogens soll erheben, wie oft sich die Teilnehmenden die AGBs vor dem Installieren von Software durchgelesen haben. Insgesamt 32 Personen (33 %) tun dies seltener als in 1% der Fälle, weitere 35 Personen (36,1 %) tun dies in 1% bis 20 % der Fälle. Fünf Personen (5,2 %) wählten die Antwort „21 % bis 40 %“, 7 Personen (7,2 %) wählten „41 % bis 60 %“, acht Personen (8,2 %) wählten „61% bis 80 %“ und zehn Personen (12,19 %) gaben an, die AGBs in 81 % bis 100 % der Fälle zu lesen. Die Teilnehmenden wurden aufgefordert ihre Antwort zu Frage 7 zu begründen. Hierzu stand ihnen ein Freitextfeld zur Verfügung. Die Antworten lassen sich in negative Antworten, die begründen, warum die AGBs nicht gelesen werden und positive Antworten, die begründen, warum sie gelesen werden, einordnen. Insgesamt 66 befragte Personen (68,0 %) führten hier Gründe auf, warum sie die AGB nicht lesen, dem gegenüber stehen 33 Personen (34,0 %), die Gründe für das Lesen der

AGB aufführten. Hierbei ist anzumerken, dass zwei Personen (2,1 %) sowohl Gründe für als auch gegen das Lesen der AGB aufführten.

Aus Frage 8 wird deutlich, dass die häufigste Begründung das Lesen der AGB zu unterlassen ist, dass diese als zu lang angesehen werden. Diese Ansicht wird von 44 Personen (45,4 %) geteilt. Der von 19 Personen (19,5 %) am zweithäufigsten angeführte Grund für die Nicht-Befassung mit den ABGs ist die als zu kompliziert empfundene Sprache. 16 Personen (16,5 %) gaben den Mangel an Motivation als Grund an, gefolgt von elf Personen (11,3 %) nach deren Ansicht die Texte von verschiedenen AGBs zu ähnlich sind, als dass sie sich erneut mit ihnen befassen müssen. Fünf Personen (5,2 %) führten als Grund für die Nicht-Befassung an, dass den AGBs in jedem Fall zugestimmt werden muss. Nur drei Personen (3,1 %) führten als Begründung an, dass sie den Applikationen und ihren Anbietern soweit vertrauen, dass sie keinen Grund darin sehen, die AGBs zu lesen.

Die Begründungen für die Befassung mit den AGBs sind weit gefächert, wobei die Häufigkeiten der Begründungen nah beieinander liegen. Dabei gaben elf Personen (11,3 %) als Grund für das Lesen der AGBs Kontrolle an, gefolgt von neun Personen (9,3 %), die mögliche versteckten Kosten meiden möchten und somit geneigt sind die AGBs zu lesen. Acht Personen (8,2 %) führten als Grund für die Befassung mit den AGBs Datenschutz an. Weitere sieben Personen (7,2 %) erklärten, dass sie erst bei Misstrauen mit der Applikation oder dem Anbieter die AGBs näher betrachten. Der am wenigsten von nur zwei Personen (2,1 %) aufgeführte Grund für das Lesen der AGBs ist schließlich das Bedürfnis, das Gewissen zu beruhigen.

Es folgte Frage 9, eine Fragebatterie mit neun Ansichten zu AGBs, die hier formulierten Ansichten stammen aus der Studie von Plaut & Bartlett (2012), welche im Abschnitt 2.2.6 bereit erläutert wird. Die Antwortmöglichkeiten sind als fünfstufige Likert-Skala konstruiert, wobei die 97 Versuchspersonen folgende Aufforderung erhielten: „Versetzen Sie sich in die Situation, in der Sie zuletzt eine Applikation installiert haben, ohne die AGBs zu lesen. Welche Gründe waren für Sie ausschlaggebend, um sich nicht weiter mit den AGBs zu befassen?“

Die erste Aussage lautet: „AGBs zu lesen ist lang und zeitaufwendig“. Diese Aussage trifft laut 77 Personen (79,4 %) zu, 14 Personen (14,4 %) zufolge trifft sie eher zu, zwei Personen (2,1 %) gaben weder noch an, eine Person (1 %) ist der Meinung, dass diese Aussage eher nicht zutrifft und drei Personen (3 %) sind der Meinung, dass diese Aussage nicht zutrifft.

Die zweite Aussage lautet „AGBs sind in einer schwer verständlichen Juristensprache formuliert“. Hier gaben 25 Personen (25,8 %) an, dass die Aussage zutrifft, 37 Personen (38,1 %), dass sie eher zutrifft und 16 Personen (16,5 %) entschieden sich für weder noch. Die Antwortmöglichkeit trifft eher nicht

zu, wurde von 13 Personen (13,4 %) gewählt, sechs Personen (6,2 %) gaben an, dass diese Aussage nicht zutrifft.

Die dritte Aussage lautet „Die AGBs müssen akzeptiert werden, wenn das zugehörige Produkt benutzt werden möchte“. Hier wählten 68 Personen (70,1 %), dass die Aussage zutrifft, 16 Personen (16,5 %) sind der Ansicht, dass sie eher zutrifft und sieben Personen (7,2 %) entschieden sich für weder noch. Dass die Aussage eher nicht zutrifft, empfanden zwei Personen (2,1 %), vier Personen (4,1 %) sind der Meinung, dass die Aussage nicht zutrifft.

Es folgt die vierte Aussage „Die AGBs haben allesamt den gleichen Inhalt“. Dieser Aussage konnten zehn Personen (10,3 %) vollumfänglich mit trifft zu zustimmen, 35 Personen (36,1 %) konnten der Aussage teilweise mit trifft eher zu zustimmen. 17 Personen (17,5 %) wählten die Antwortmöglichkeit weder noch und 26 Personen (26,8 %) entschieden sich dafür, dass diese Aussage eher nicht zutrifft. Darüber hinaus sind neun Personen (9,3 %) der Ansicht, dass diese Aussage nicht zutrifft.

Die fünfte Aussage beinhaltet die soziale Repräsentation, dass vor Gericht erdrückende Bedingungen im Nachhinein für ungültig erklärt werden würden. Elf der 97 Personen (11,3 %) stimmten dieser Aussage vollständig zu. Insgesamt 18 Personen (18,6 %) sind der Meinung, dass diese Aussage eher zutrifft und 35 Personen (36,1 %) entschieden sich für die Antwortmöglichkeit weder noch. Dass diese Aussage eher nicht zutrifft, vertreten 17 Personen (17,5 %) gefolgt von 16 Personen (16,5 %), die die Aussage als vollständig unzutreffend empfinden.

Die sechste Aussage lautet „Die Bedingungen der Anbieter in den AGBs sind generell fair und vernünftig“. Fünf Personen (5,3 %) sind der Ansicht, dass diese Aussage zutrifft, gefolgt von 19 Personen (19,5 %), die trifft eher zu als Antwort wählten. Die Mehrzahl der Teilnehmenden, nämlich 38 (39,2 %), entschied sich für weder noch. Insgesamt 19 Personen (19,6 %) waren der Ansicht, dass diese Aussage eher nicht zutrifft und 16 Personen (16,5 %) lehnten diese Aussage vollumfänglich ab.

Als siebtes folgt die Aussage „Ich nutze nur Apps von seriösen Anbietern, diese haben keine ökonomischen Gründe, unvernünftige oder unfaire Bedingungen anzubieten bzw. zu erzwingen“. Dieser konnten neun Personen (9,3 %) vollständig und 23 der befragten Personen (23,7 %) teilweise zustimmen. Weitere 29 der Teilnehmenden (29,9 %) entschieden sich für die Antwortmöglichkeit weder noch. Insgesamt 21 Personen (21,6 %) sind der Meinung, dass diese Aussage eher nicht zutrifft und 15 Personen (15,5 %) hielten sie für komplett unzutreffend.

Die achte Aussage „Niemand liest die AGBs“ wurde von 17 Personen (17,5 %) als voll zutreffend gewertet, 33 Personen (34 %) antworten hier mit trifft eher zu. Insgesamt 19 Personen (19,6 %)

wählten die Antwortmöglichkeit weder noch aus, wobei 15 Personen (15,5 %) diese Aussage als eher nichtzutreffend werten und 13 Versuchspersonen (13,4 %) gaben an, dass diese Aussage nichtzutreffend ist.

Die letzte Aussage lautet: „Ich informiere mich aus anderen Quellen (Freundeskreis, Fachzeitschriften, Blogs) über die von mir verwendeten Apps“. Trifft zu wählten zehn Versuchspersonen (10,3 %) als Antwort, die höchste Zustimmung erhielt die Antwortmöglichkeit trifft eher zu mit 37 Personen (38,1 %). Insgesamt 22 der befragten Personen (22,7 %) wählten hier weder noch als Antwort. Dass diese Aussage eher nicht zutrifft, empfanden 17 Personen (17,5 %) und 11 Personen (11,3 %) gaben an, dass diese Aussage nicht zutrifft.

Frage 10 ermittelt die Einschätzung der allgemeinen Lesedauer von AGBs, und wurde bereits im Abschnitt 5.7.2 ausgewertet.

Die 65 Testpersonen, die bei Frage 7, die sich nach der Häufigkeit des Lesens der AGB erkundigt, nicht angegeben hatten, dies nie zu tun, bekamen Frage 11 zu ihrem Leseverhalten gestellt. Insgesamt 56 von ihnen (86,2 %) gaben an, die AGBs in Auszügen zu lesen. Dem gegenüber standen neun Personen (13,8 %), die antworteten, die AGBs komplett zu lesen.

Es folgt in Frage 12 ein weiteres Freitextfeld. Die Personen wurden hier gebeten, ihr Leseverhalten, also ob die AGBs in Auszügen oder komplett gelesen werden würden, zu begründen. Von den neun Teilnehmenden, die angaben, die AGBs vollständig zu lesen, begründeten dies acht (88,89 %) mit der Relevanz von diesen. Von diesen neun Personen haben wiederum zwei (22,22 %) angegeben, die AGBs nur zu überfliegen. Bei den 56 Personen, die angaben, die AGB nur in Auszügen zu lesen, wurden folgende Begründungen abgegeben: Dabei gaben 25 dieser Personen (44,64 %) als Begründung für das in Auszügen lesen an, dass sie die AGBs nur überflogen. 16 Personen (28,57 %) erklärten, dass die AGBs zu lang sind, um sie komplett zu lesen, weitere zehn Personen (17,86 %) verwiesen darauf, dass in AGBs viele Standartformulierungen auftauchen würden, die kein genaues Durchlesen erfordern. Zwei Personen (3,57 %) empfanden Texte in AGBs als zu unübersichtlich, als dass sie sie komplett lesen wollten. Weitere Begründungen zeigen auf, welche Themen beim Überfliegen als wichtig erachtet werden. Als häufigstes Thema wurde hier Datenschutz von sechs Personen (10,74 %) angegeben, gefolgt von Kosten von fünf Personen (8,93 %) und einer einmaligen Erwähnung des Themas Sicherheit von einer Person (1,79 %).

Die dreizehnte Frage beinhaltet drei Unterfragen zum Thema Zusammenfassungen, wie sie etwa beim Installieren von Applikationen beim Betriebssystem Android zum Einsatz kommen. Statt der kompletten AGB bekamen die Nutzenden hier zunächst eine knappe Zusammenfassung der

angeforderten Rechte präsentiert. Dabei kannten 65 der 96 Personen (67 %) diese Zusammenfassungen und 55 der Befragten (56,7 %) gaben an, durch deren Inhalt schon einmal die Installation einer Applikation unterlassen zu haben, darüber hinaus sagten 38 der Befragten (39,2 %), dass diese Zusammenfassung schon einmal dazu geführt habe, die zugrundeliegende AGB zu betrachten.

Die nächste Frage (14) ermittelt mit einen Freitextfeld die Einschätzung der Teilnehmenden, was eine Weitergabe ihrer Daten für Konsequenzen für sie hätte. Insgesamt 22 Antworten können dabei keiner sinnvollen Kategorie zugeordnet werden wie z. B. „schwer einschätzbar“ und „nicht sicher“. Am häufigsten wurde von 30 Personen (30,93 %) der Verlust von Privatsphäre angeführt. Von 24 Personen (24,7 %) wurde angeführt, dass mit der Weitergabe von privaten Daten der Erhalt von als Spam eingeschätzten Nachrichten einherging. Weitere 22 Personen (22,7 %) vermuten, dass dies bedeute, dass ihre Daten verkauft und für ein Profiling ihrer Person bzw. ihres Kaufverhaltens genutzt würden. Insgesamt 17 Personen (17,5 %) halten personalisierte Werbung für eine Konsequenz der Weitergabe ihrer Daten. Außerdem gaben sieben Personen (7,2 %) an, dass Kosten eine mögliche Konsequenz der Datenweitergabe sein könnten und drei Personen (3,1 %) gehen davon aus, dass die Datenweitergabe Hacks ermöglichen würde. Insgesamt acht Personen (8,2 %) führten auf, dass eine Datenweitergabe als Konsequenz die Deinstallation der Applikation und Misstrauen gegenüber dem Anbieter zur Folge haben würde. Diese Antworten suggerieren ein falsches Verständnis der Frage und werden daher nicht weiter betrachtet. Insgesamt 15 Personen (15,46 %) gaben an, dass ihnen keine Konsequenzen der Weitergabe von persönlichen Daten bekannt sei. Eine Übersicht der Häufigkeiten der angegebenen Konsequenzen der Weitergabe der persönlichen Daten ist in Abbildung 11 illustriert.

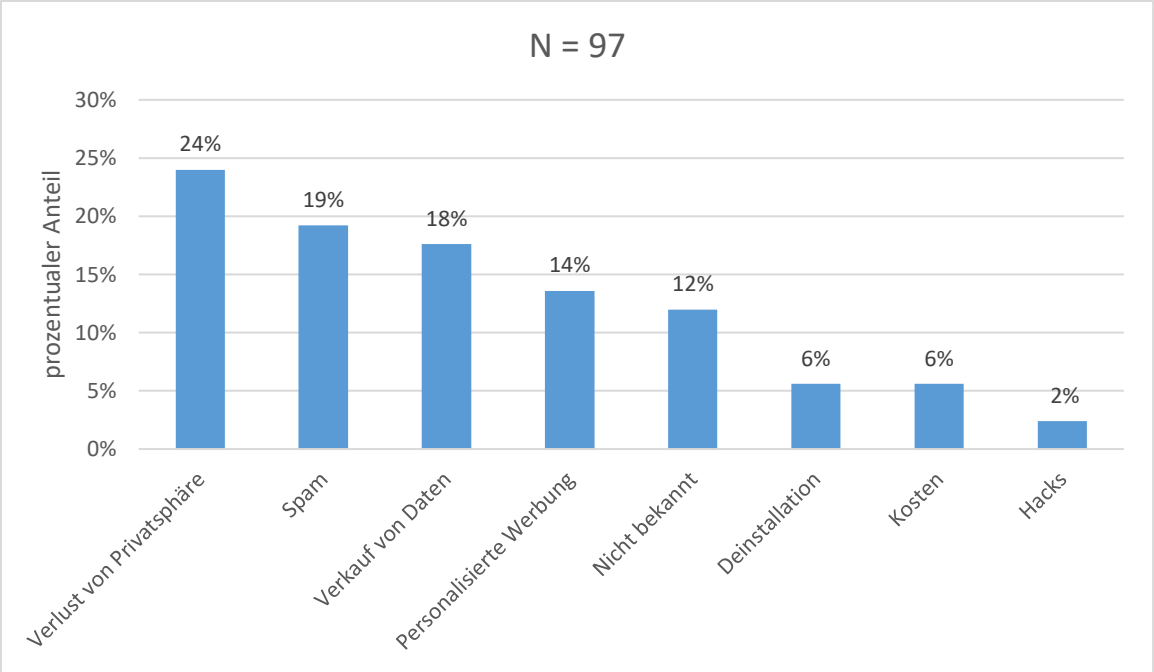


Abbildung 11. Prozentuale Häufigkeiten der angegebenen Konsequenzen der Weitergabe von persönlichen Daten.

Diese Abbildung illustriert die Häufigkeit der angegebenen Konsequenzen der Weitergabe von persönlichen Daten in absteigender Reihenfolge.

Darüber hinaus wird die Stichprobe in zwei Gruppen aufgeteilt: diejenigen, die die Wichtigkeit des Schutzes ihrer Daten als niedrig angaben (*N1* = 15; 1 - 5 auf einer Skala von 1 - 10), und diejenigen, die die Wichtigkeit des Schutzes ihrer Daten als hoch angaben (*N2* = 82; 6 - 10 auf einer Skala von 1 - 10). Zusätzlich wird die Anzahl der aus den im Freitext angegebenen Konsequenzen berechnet und beide Datensätze auf Normalverteilung geprüft. Der Kolmogorov-Smirnov-Test kann keine Normalverteilung in einem der Datensätze feststellen. Anschließend wird ein Mann-Whitney-U-Test durchgeführt, um zu prüfen, ob ein signifikanter Unterschied bezüglich der Anzahl der Konsequenzen zwischen den beiden Gruppen vorhanden ist. Der Test ergibt keinen signifikanten Unterschied ($U = 578$; $z = -0{,}393$ und $p < .694$) (s. Tabelle 28, Anhang J).

Es folgt die 15. Frage, welche erhebt, ob aufgrund einer AGB schon einmal das Installieren einer Applikation unterlassen wurde. Insgesamt 60 der 97 Teilnehmenden (61,9 %) gaben an, dies bereits gemacht zu haben. Im Gegensatz zur Frage 13 bezieht sich diese Frage nicht auf die Kurz-Zusammenfassungen bei der Installation einer Applikation, sondern auf herkömmliche AGBs. In der folgenden Frage sollen die Personen die inhaltlichen Punkte aufführen, die zu einem Unterlassen der Installation geführt haben. Häufigster Grund für die Nicht-Installation ist, dass die Testpersonen der Meinung sind, dass diese zu viele oder für ihre Funktion unnötige Rechte anfordert. Eine solche Begründung gaben zehn Personen (10,3 %) an. Vier der Befragten (4,12 %) gaben als Grund für das Unterlassen der Installation einer Applikation die Weitergabe von Daten an. Drei Personen (3,09 %)

verwiesen auf Kosten als Begründung für das Nicht-Installieren. Zwei Personen (2,06 %) entschieden sich dagegen, eine Applikation zu installieren, weil sie durch das Nutzen der Applikation die Rechte an den mit der Applikation erschaffenen Inhalten abgeben würden.

Die siebzehnte Frage soll erheben, ob die Teilnehmenden Bedenken haben, dass Applikationen bzw. deren Anbieter ihre persönlichen Daten speichern und an Dritte weitergeben. Bei dieser Frage sind Mehrfachantworten möglich. Insgesamt zwölf der Befragten (12,4 %) gaben hier an, dass sie keine Bedenken hätten. Insgesamt 55 (56,7 %) der Befragten haben bereits Bedenken bei der Speicherung von Daten, von diesen hat die überwiegende Mehrheit 50 (90,09 %) auch Bedenken an der Weitergabe von Daten an Dritte. Insgesamt haben 80 der Befragten (92,5 %) Bedenken an der Weitergabe von Daten.

In der folgenden Frage wurden die Testpersonen gebeten, in einem Freitextfeld anzugeben, welche persönlichen Daten ihrer Meinung nach weitergegeben werden. Die häufigste Antwort mit 37 Antworten (38,1 %) ist hier, dass das Nutzungsverhalten aufgezeichnet wird. Von einer Weitergabe von demographischen Daten gehen 33 der Befragten (34,0 %) aus. Dabei gehen 31 (32,0 %) Personen davon aus, dass Applikationen ihre persönlichen Kontaktdaten weitergeben. Für die Annahme, dass Positionsdaten weitergegeben wurden, sprachen sich 22 Personen (22,7 %) aus. Weitere 18 Personen (18,6 %) vermuten, dass ihre persönlichen Vorlieben erfasst und weitergegeben werden, während 16 der Teilnehmenden (16,5 %) davon ausgehen, dass letztendlich alle Daten auch weitergegeben werden. Insgesamt 14 Personen (14,4 %) vermuten, dass Daten zu ihrem Konsumverhalten weitergegeben werden. Die Weitergabe von Bildern halten elf der Befragten (11,3 %) für möglich. Acht der Teilnehmenden (8,2 %) gehen davon aus, dass ihre Kontakte, also die Einträge in ihren Adressbüchern, ausgelesen und weitergegeben werden. Sieben der Testpersonen (7,2 %) gehen davon aus, dass Kommunikationsinhalte weitergegeben werden. Darüber hinaus gehen fünf der Befragten (5,2 %) davon aus, dass ihre Kontodaten weitergegeben werden.

In der neunzehnten Frage werden die Teilnehmenden gebeten einzuschätzen, was für einen monetären Wert verschiedene Datenarten für ein Unternehmen haben. Bei den Datenarten handelt es sich um Alter, Geschlecht, Adresse, Standortdaten, Kontaktdaten aus dem Adressbuch, persönliche Bilder und die Browserchronik. Somit stimmen die Kategorien größtenteils mit denen überein, die vorher im Freitextfeld erwähnt wurden. Die Personen wurden gebeten, die Angaben in Euro zu tätigen, was dazu geführt haben kann, dass weniger Personen einen monetären Wert im Cent-Bereich angegeben haben. Darüber hinaus wurden hohe Werte angegeben, deren Handhabung in der Diskussion näher erläutert werden. Die Minima aller Kategorien bis auf das der Browserchronik, welche 0,01 Euro beträgt, entsprechen 0 Euro. Bei der Kategorie Alter wurde ein Maximum von 3.000

Euro, ein Mittelwert von 103,48 Euro (*SD* = 368,05 Euro), ein Median von 5 Euro, angegeben. Beim Geschlecht betragen die Ergebnisse für das Maximum 6.000 Euro bei einem Mittelwert von 126,01 Euro (*SD* = 636,35 Euro). Der Median beträgt hier 4 Euro. Der monetäre Wert der Adresse wurde auf maximal 10.000.000 Euro geschätzt, wobei der Median 10 Euro und der Mittelwert mit 103.372,98 Euro (*SD* = 1.015.317,83 Euro) beziffert wurden. Auch für die Standortdaten wurde ein maximaler Wert von 10.000.000 Euro angegeben, der Median beträgt hier ebenfalls 10 Euro bei einem Mittelwert von 103.399,74 Euro (*SD* = 1.015.315,37 Euro). Für Kontaktdaten aus dem Adressbuch beträgt das Maximum 1.000.000 Euro, der Median beträgt hierbei 15 Euro, wobei der Mittelwert 1884,62 Euro (*SD* = 11296,63 Euro) beträgt. Der monetäre Wert von persönlichen Bildern wurde auf maximal 5.000.000 Euro geschätzt, der Median beläuft sich hierbei auf 10 Euro und der Mittelwert beträgt 6453,65 Euro (*SD* = 51.642,17 Euro). Für die Browserchronik wurde ein Maximum von 10.000.000 Euro angegeben der Median betrug hier 20 Euro und der Mittelwert 106.498,27 Euro (*SD* = 1.015.453,13 Euro).

Die 20. Frage soll auf einer zehnstufigen unbezifferten Skala den Stellenwert für den Schutz persönlicher Daten ermitteln. Dabei wird für die Auswertung dem niedrigsten Stellenwert die Zahl 1 und dem höchsten Stellenwert die Zahl 10 zugewiesen. Der Median beträgt hier 8 und der Mittelwert 7,6 (*SD* = 1,95), wobei das Minimum bei 2 und das Maximum bei 10 lagen (s. Abbildung 12).

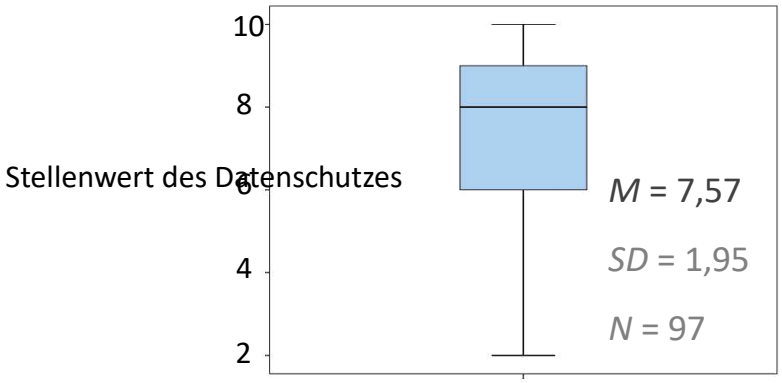


Abbildung 12. Durchschnittlicher Stellenwert des Schutzes persönlicher Daten.

Diese Abbildung illustriert den durchschnittlichen Stellenwert des Schutzes persönlicher Daten mit den Minima und Maxima sowie der Standartabweichung.

Um zu prüfen, ob es einen Geschlechterunterschied gibt, werden zunächst die Mittelwerte bei den Geschlechtergruppen ausgerechnet, dabei resultiert ein Mittelwert von 7,61 (*SD* = 1,83) für das männliche Geschlecht und ein Mittelwert von 7,58 (*SD* = 2, 26) für das weibliche Geschlecht. Auf Grund

der Abwesenheit der Normalverteilung bei beiden Datensätzen wird der Mann-Whitney-U-Test durchgeführt, welcher keinen signifikanten Unterschied feststellen kann (s. Tabelle 29, Anhang J).

Bei der einundzwanzigsten Frage wurden die Teilnehmenden gebeten einzuschätzen, wie viel Euro sie im Monat im Durschnitt für Applikationen auf mobilen Endgeräten ausgeben. Diese Frage wurde von 95 der 97 Befragten beantwortet. Der Median beträgt hier 0 Euro und der Mittelwert 1,89 Euro (*SD* = 3,65), wobei das Minimum hier 0 Euro und das Maximum 35 Euro beträgt.

Als letztes wurde gefragt, welchen finanziellen Aufwand die Befragten bereit wären zu leisten, um die Daten auf ihrem mobilen Endgerät zu schützen. Hierbei wurden Antworten von allen 97 Teilnehmenden abgegeben. Der Median beträgt hier 5 Euro und der Mittelwert 6,99 Euro (*SD* = 12,86 Euro). Als Minimum wurden hier 0 Euro und als Maximum 100 Euro angegeben.

Über die eben erwähnten Tests hinaus werden noch weitere explorative statistische Untersuchungen getätigt, die für diese Studie relevant sein könnten. Dabei kann lediglich ein signifikanter Zusammenhang zwischen dem finanziellen Aufwand, den die Leute betreiben, um Applikationen zu kaufen mit der Bereitschaft finanziellen Aufwand zu betreiben, um ihre Daten zu schützen, nachgewiesen werden. Bei der Frage, wie viel Geld pro Monat für den Erwerb von Applikationen ausgeben wird, resultiert ein Mittelwert von 5,76 Euro (*SD* = 6,866) bei *N* = 51. Der Spearman-Rho-Test ergibt einen signifikanten Zusammenhang, $r = 0{,}369$ mit $p < .008$ (s. Tabelle 30, Anhang J).

5.8 Diskussion

In dem folgenden Kapitel werden die Ergebnisse nach Hypothesen geordnet diskutiert. Hierbei wird zunächst die aufgewandte Zeit zum Lesen der Teilnahmevereinbarung (Hypothese 1) näher besprochen, um anschließend den Stellenwert des Schutzes der persönlichen Daten näher zu betrachten (Hypothese 2). Weiterhin wird die Gleichgültigkeit gegenüber der Abgabe von persönlichen Daten bedingt durch die uneinsichtigen Konsequenzen diskutiert (Hypothese 6). Ferner wird analysiert, weshalb bereits ein geringer finanzieller Gegenwert zum Aushändigen von persönlichen Daten führt. Anschließend erfolgt die Diskussion der explorativen Ergebnisse, welche die Präsentationsform der Teilnahmevereinbarungen, die Geschlechter- und Altersunterschiede, sowie das unterschiedliche Verhalten bzgl. des Zeitpunktes der Einwilligung in die Teilnahmevereinbarung näher betrachtet.

5.8.1 Zur Hypothese 1: Aufgewendete Zeit zum Lesen der Teilnahmevereinbarung

Hypothese 1:

Die Nutzenden wenden nicht genügend Zeit auf, um sich der Konsequenzen der Abgabe ihrer Daten bewusst werden zu können.

Die Studie von Bakos et al. (2014) geht davon aus, dass schätzungsweise 0,05 % bis 0,22 % der Konsumenten die AGBs zwar öffnen, jedoch nicht genügend Zeit aufwenden, um diese vollständig durchlesen zu können. Eine weitere Studie aus dem IFH Köln (2015) stellt fest, dass der prozentuale Anteil der Personen, die die Datenschutzbestimmungen lesen, von Nation zu Nation variiert. In Deutschland gaben etwa 17,7 % der Befragten an, die Datenschutzbestimmungen (fast) immer zu lesen, während es in Schweden lediglich 7,5 % waren. Die Frage 7 des Fragebogens zum allgemeinen Umgang mit den AGBs ergibt, dass 86,2 % der Personen die AGBs nur in Auszügen lesen, wobei 13,8 % angaben, die AGBs stets komplett durchzulesen. Erstaunlicherweise zeigen sich bei den Fragen im direkten Interview mit den Personen, welches sich ausschließlich auf die Teilnahmevereinbarungen im Täuschungsexperiment bezogen hat, deutlich andere Ergebnisse. So gaben 51 % der Personen an, die Teilnahmevereinbarungen vollständig und 41 % die Teilnahmevereinbarungen teilweise gelesen zu haben. Nur 5,9 % der Personen gaben an, die Teilnahmevereinbarungen nicht gelesen zu haben. Allerdings wurde die Teilnahmevereinbarung im Durchschnitt nur 52 Sekunden (*SD* = 52,48) betrachtet. Diese Zeit ist weder annähernd genügend, um die vier Volltextseiten komplett durchzulesen noch um die Seiten zu überfliegen und dabei ausreichend Informationen aus dem Text herauszuziehen. Somit ist davon auszugehen, dass die Antworten der Personen eventuell aufgrund der gegebenen Laborbedingungen durch die soziale Erwünschtheit beeinflusst wurden. Besonders in der Situation eines direkten Interviews ist von diesem Phänomen auszugehen, was sich in der großen Häufigkeit der Behauptung die Teilnahmevereinbarungen zu lesen äußerte. Darüber hinaus ist die geschätzte Lesedauer der Personen, die allgemein für die Teilnahmevereinbarungen aufgewandt wurde, signifikant länger als die geschätzte Lesedauer, welche im Interview direkt nach dem Täuschungsexperiment angegeben wurde. Die unmittelbare Schätzung nach der Konfrontation mit einem AGB-Text (den Teilnahmevereinbarungen) führt zu einer deutlich angemesseneren Schätzung, die jedoch immer noch weit über dem gemessenen Wert liegt. Die tatsächlich gemessene Zeit der Betrachtungsdauer der Teilnahmevereinbarungen liegt bei weniger als der Hälfte der zuvor geschätzten Zeit. Dies führt zu der Schlussfolgerung, dass die Personen zwar denken, sie hätten viel Zeit aufgewandt, um Informationen aus den Teilnahmevereinbarungen zu entnehmen, die gemessene Zeit jedoch belegt, dass ein vollständiges Durchlesen in der Zeit nicht möglich ist. Ein weiterer Befund, welcher dafürspricht, dass die Personen die Teilnahmevereinbarungen entweder nicht durchlesen

oder nicht verstehen, leitet sich aus den Ergebnissen der Auswertung der ersten Frage des Fragebogens ab, welche nach Auffälligkeiten in den Teilnahmevereinbarungen fragt. Mit dieser Frage soll ermittelt werden, ob den Personen aufgefallen ist, dass fragliche Bedingungen in Bezug auf Datenschutz und Ethik in den Teilnahmevereinbarungen enthalten waren. Hierbei gaben zwar 19,6 % an, dass etwas auffällig war, aber keine der Personen zweifelte die fraglichen Bedingungen an. Bei der Einschätzung seitens der Teilnehmenden, was Konsequenzen der Weitergabe ihrer Daten sein könnten, führten nur 30,92 % den Verlust ihrer Privatsphäre an. Dementsprechend sind sich knapp 70 % der Teilnehmenden nicht bewusst, dass bei der Weitergabe ihrer Daten, diese durchaus von Dritten genutzt werden können und werden.

Diese Erkenntnisse stimmen mit denen aus den Studien von Kelley et al. (2012), Kelley et al. (2013) und Peng et al. (2012), die im Abschnitt 2.2.7 erwähnt wurden, überein. Diese besagen, dass die Nutzenden Schwierigkeiten bei der Einschätzung von Konsequenzen durch die Zugriffsberechtigungen an Applikationen haben und somit ihre Entscheidungen basierend auf Missverständnissen und falscher Einschätzung der Auswirkungen auf ihre Privatsphäre getroffen werden, was dazu führen kann, dass sie ihre sensiblen Daten versehentlich aushändigen. Besonders der Mangel an Regularien und technischen Maßnahmen sei dafür verantwortlich, dass sensible Nutzerdaten nicht genügend geschützt sind (Chin et al., 2012; Hammad et al., 2017; Nauman et al., 2010).

Ein deutlich geringerer Prozentsatz von 15,7 % gab bei der Frage im direkten Interview, welche ermitteln soll, ob die teilnehmende Person sich während des Täuschungsexperimentes unwohl fühlten, an, dass der Grund für ihr Unwohlsein die Preisgabe von persönlichen Präferenzen sei. Darüber hinaus wird von 7,8 % das Gefühl des Unwohlseins mit einem Mangel an Alternativen begründet. Besonders bei Begriffen, die beide als sehr kritisch angesehen werden, z.B. im Bereich der Politik wurde die Präferenz zwischen den Parteien AFD und NPD abgefragt, haben die Teilnehmenden angemerkt, dass sie sich bei der Entscheidung sehr schwertaten und dies zu einem Gefühl von Unwohlsein führte. Der Meinung, dass die Weitergabe privater Daten mit dem Erhalt von als Spam klassifizierten Nachrichten zusammenhängt, sind 24,7 % der Testpersonen. Hierbei ist zu erkennen, dass die Befürchtung des Erhalts von unerwünschten Nachrichten knapp der entspricht, die eigene Privatsphäre zu verlieren. Dies verdeutlicht noch einmal, wie trivial das Thema von den Endnutzenden wahrgenommen wird. Insgesamt gehen 17,5 % der Befragten davon aus, dass personalisierte Werbung, 7,2 %, dass finanzielle Kosten und 3,1 %, dass schädigende Angriffe oder Software mögliche Konsequenzen der Weitergabe von privaten Informationen sind. Hierbei handelt es sich ausschließlich um unmittelbare Konsequenzen. Langfristige Konsequenzen wurden weniger genannt. Dieses Phänomen wurde bereits im Abschnitt 2.2.5 beschrieben. In der Freitextfrage, in der die Teilnehmenden angeben sollten, welche ihrer persönlichen Daten ihrer Meinung nach weitergegeben

werden, sind sich nur 16,5 % bewusst, dass alle Daten an Dritte weitergegeben werden. Die am häufigsten erwähnte Befürchtung von 38,1 % der Testpersonen ist, dass ihr Nutzungsverhalten aufgezeichnet und analysiert wird. Darauf folgt mit 34 % die Weitergabe von demographischen Daten und mit 32 % die Weitergabe von Kontaktdaten. Hierbei wäre eine weitere interessante Frage gewesen, ob und inwiefern sich die Person als gläserner Nutzer/in sieht.

Unter der Berücksichtigung der kurzen Lesezeit und der Tatsache, dass nicht eine Person die fraglichen Bedingungen anzweifelte, kann die erste Hypothese aufrechterhalten werden.

5.8.2 Zur Hypothese 2: Stellenwert des Schutzes der Persönlichen Daten

Hypothese 2:

Die Nutzenden empfinden es für sehr wichtig, ihre Daten zu schützen.

Wie schon in Abschnitt 2.2.7 beschrieben, wird ein Großteil der Einkäufe derzeit online getätigt. Dabei gaben die meisten der 9000 Interviewten an, dass Datenschutz und Datensicherheit eine hohe Relevanz bei der Auswahl des Online-Händlers haben und die Nachvollziehbarkeit der Datenschutzbestimmungen dabei von großer Bedeutung wäre (IFH Köln, 2015). In derselben Studie wurde eine Meinungsforschung durchgeführt, welche ergibt, dass Verbraucher europaweit die Datensicherheit signifikant wichtiger einstufen als materielle Fragen des Datenschutzes oder die informativen Datenschutzbestimmung. Ein ähnliches Verhalten konnte auch im Rahmen der empirischen Untersuchung festgestellt werden. Mit Hilfe des Fragebogens, welcher im Rahmen der Studie von den Testpersonen auszufüllen war, konnte ermittelt werden, dass der Stellenwert für den Schutz persönlicher Daten auf einer 10-stufigen Skala (1 = geringer Stellenwert; 10 = hoher Stellenwert) mit einem Mittelwert von 7,6 (*SD* = 2,07) abschnitt. Somit ist davon auszugehen, dass die meisten der Befragten dem Schutz ihrer persönlichen Daten einen hohen Stellenwert zuschreiben. Bei näherer Betrachtung der geschlechtsspezifischen Unterschiede resultiert bei dem Mittelwert des männlichen Geschlechts nur ein leicht höherer Stellenwert, der jedoch nach der Durchführung des Mann-Whitney-U-Testes als nicht signifikant hervorging. Somit können keine Unterschiede zwischen den männlichen und weiblichen Teilnehmenden gefunden werden, was der Studie von Midha (2002), die im Abschnitt 2.2.7 vorgestellt wurde, widerspricht. Diese ergibt, dass weibliche Nutzende größere Bedenken in Bezug auf das Einschreiten in ihre Privatsphäre haben als männliche Nutzende.

Insgesamt gaben 33 % der Testpersonen an, die AGBs seltener als 1 % der Fälle durchgelesen zu haben. 36,1 % der Befragten unterließen das Lesen der AGBs in 1 % bis 20 % der Fälle. Demnach lesen sich

zwei Drittel der Befragten die AGBs nur selten durch. Nur 12,19 % der Personen gaben an, sich die AGBs vollständig durchzulesen. Diese Ergebnisse stimmen größtenteils mit den Ergebnissen der Studie aus Abschnitt 2.2.7 überein, in der ebenfalls zwei Drittel der Befragten nur selten bis nie die Datenschutzbestimmungen gelesen haben. Darüber hinaus variiert der prozentuale Anteil beim Herunterladen von Daten, Bestellen von Artikeln oder beim Anmelden bei sozialen Netzwerken von Nation zu Nation. In dieser Studie gaben 12,19 % der Teilnehmenden an, die AGBs vollständig gelesen zu haben. Vergleichend zu den Ergebnissen der Studie aus dem Kurzbericht in Abschnitt 2.2.7 liegt dieser Anteil zwischen den Werten von Deutschland (17,7 %) und Schweden (7,5 %). Die Differenz der Prozentsätze zwischen der Studie aus dem Kurzbericht und der im Rahmen der Dissertation durchgeführten Studie ist mit der unterschiedlichen Fragestellung zu begründen.

Die Frage im Kurzbericht ist durch die Art ihrer Formulierung im Vergleich zu der Frage in der Dissertation unspezifischer. Dabei wurde im Kurzbericht abgefragt, ob sich bei dem Herunterladen aus dem Internet die AGBs „in der Regel“ durchgelesen werden, während in der Studie dieser Dissertation die Teilnehmenden direkt gefragt wurden, ob sie die Teilnahmevereinbarung im Rahmen des Experiments durchgelesen haben.

Zudem gaben 10,74 % der Testpersonen an, dass sie beim Überfliegen der AGBs besonders die Abschnitte, welche den Datenschutz behandeln, näher betrachten, gefolgt von 8,93 %, welche besonderes Augenmerk auf die Kosten legen. Somit wurde nochmals bestätigt, dass der Datenschutz beim Betrachten der AGBs einen besonderen Stellenwert hat.

Knapp zwei Drittel der Teilnehmenden gaben an, schon einmal das Installieren einer Applikation aufgrund der AGB unterlassen zu haben.

Die häufigsten Gründe für die Unterlassung der Installation sind eine übermäßige Forderung von Rechten, die jedoch für die primäre Funktion der Applikation nicht von Nöten sind, sowie die damit zusammenhängende Weitergabe von Daten.

Obwohl es den Befragten wichtig zu sein scheint, ihre Daten zu schützen, handeln sie nicht entsprechend. Nur ein Bruchteil der Testpersonen gab im Fragebogen den Zugewinn von Kontrolle über seine Privatsphäre als Begründung an, sich die AGBs durchzulesen. Diese Befunde bestätigen das Phänomen des Privacy Paradoxes, welches in Abschnitt 2.2.8 bereits näher erläutert wurde.

Trotz des widersprüchlichen Handelns gab die Mehrheit der Teilnehmenden an, ihren Daten einen hohen Stellenwert zuzuschreiben, womit die zweite Hypothese aufrechterhalten werden kann.

5.8.3 Zur Hypothese 3: Akzeptanz geringer Einbußen zur Wahrung der Rechte und Daten

Hypothese 3:

Die Nutzenden würden nur geringe Einbußen erdulden, um ihre Rechte und Daten zu wahren.

Zwei Drittel der Befragten gaben an, die Datenschutzbestimmungen nur selten bis nie gelesen zu haben. Als Gründe hierfür wurden vor allem von 45,4 % der Teilnehmenden die Länge der AGBs und die Komplexität der Sprache mit 19,5 % angegeben. Diese Bemerkungen werden durch die ersten beiden Aussagen der nächsten Frage bestätigt, wobei 93,8 % die AGBs als zu lang und 63,9 % als zu komplex erachten. Hierbei ist zu erwähnen, dass die Teilnehmenden die nachfolgenden Fragen nicht einsehen konnten und somit davon ausgegangen werden kann, dass die Aussagen in der Freitextfrage nicht von den vorgegebenen Aussagen in der nachfolgenden Frage beeinflusst wurden. Aus den beiden eben genannten Gründen zum Unterlassen des Lesens der AGBs kann hergeleitet werden, dass die Mehrheit der Teilnehmenden eine höhere Lesebereitschaft aufzeigen würde, wenn sie nicht so viel Zeit und kognitiven Aufwand investieren müsste, um ein Verständnis der Abtretung der Rechte ihrer privaten Daten und die daraus folgenden Konsequenzen zu verstehen. Demzufolge wird der Lese – und Verständnisaufwand als große Einbuße bewertet, welche dazu führt, das Lesen der AGBs zu unterlassen und somit die Rechte und Daten ohne Kenntnis über deren Verwendung abzutreten und weiterzuleiten. Ferner gaben 56,7 % der Teilnehmenden an, auf Grund der Zusammenfassung der freizugebenden Daten und Rechte die Installation einer Applikation unterlassen zu haben. Außerdem hat die eben genannte Zusammenfassung bei 39,2 % der Teilnehmenden dazu geführt, die entsprechende AGB näher zu betrachten. Somit kann davon ausgegangen werden, dass eine intuitive und einfache Methode, die AGBs zu vermitteln bzw. deren Konsequenzen aufzuzeigen, die Teilnehmenden dazu verleiten würde, diese bei dem Erteilen des Einverständnisses oder der Ablehnung mit einzubeziehen.

Somit kann die dritte Hypothese bestätigt werden, weil die meisten Teilnehmenden angaben, die AGBs auf Grund ihrer Länge und Komplexität nicht zu lesen und das Lesen dieser Texte für sie eine Einbuße bei der Installation einer Applikation darstellt. Auf der anderen Seite wird eine Betrachtung der Zusammenfassung der abzugebenden Daten und Rechte nur als kleine Einbuße wahrgenommen, welche jedoch zu einem datenschutzfreundlicheren Verhalten führen kann. Demnach kann eine intuitive und einfachere Methode die AGBs darzustellen eine höhere Lesebereitschaft mit sich bringen.

5.8.4 Zur Hypothese 4: Unterschied des Datenschutzes im gewerblichen und privaten Bereich

Hypothese 4:

Die Datensicherheit spielt in großen Konzernen eine sehr wichtige Rolle, wobei sie über mittelständische Unternehmen bis zu den Endnutzenden stetig abnimmt.

Bereits im Abschnitt 2.2.10 wurde herausgestellt, dass die Ausgaben für die IT-Sicherheit in Deutschland seit dem Jahr 2017 um 24,5 % auf 4,9 Milliarden Euro gestiegen sind. Für das Jahr 2021 wird eine weitere Steigung auf 5,7 Milliarden Euro erwartet. Weltweit liegen die Ausgaben für die IT-Sicherheit bei etwa 124 Milliarden US-Dollar im Jahr. Diese Ausgaben sind mit dem Anstieg von Cyber-Angriffen verbunden, welche eine hochgerechnete Gesamtschadenssumme von 43,4 Milliarden Euro deutschlandweit ergab. Demnach büßt jedes zweite geschädigte Unternehmen einen Schaden von bis zu 50.000 Euro ein. Die Marktgröße des Bereiches Serversicherheit wurde im Jahr 2016 auf 122 Milliarden US-Dollar geschätzt und es wird eine Steigerung von etwa 60 % im Jahr 2021 prognostiziert. Diese steigenden Ausgaben sind eine Reaktion auf die immer häufigeren und qualitativ steigenden Cyber-Angriffe. Bereits im Jahr 2014 wurde ein Fünftel der Unternehmen im Bereich der IT-Sicherheit täglich oder mehrmals pro Woche angegriffen. Bei mittelständischen Unternehmen ist die IT-Sicherheit eine der vier wichtigsten Herausforderungen und bereitet zwei Fünfteln der befragten Geschäftsführer Sorgen. Trotzdem wird für die IT-Sicherheit lediglich 10 % des IT-Budgets angewandt, wobei dies nur 3 % des Jahresumsatzes darstellt. In Konzernen berichten 76 % der Entscheidungstragenden über gestiegene Ausgaben im Bereich der IT-Sicherheit. So fühlt sich die Mehrheit der großen Unternehmen (56 %) so gut wie möglich geschützt und besitzt eine umfassende Strategie zum Umgang mit Cyber-Gefahren. Diese wenden etwa 15 % ihres gesamten IT-Budgets für die Sicherheit auf, wobei ein Fünftel der Unternehmen sogar 20 % des Budgets in die IT-Sicherheit investiert. Aus der durchgeführten Studie geht hervor, dass 86,3 % sich für die höchste finanzielle Gegenleistung innerhalb des Experimentes entschieden und somit ihre Daten an die höchste Anzahl von Universitäten und Unternehmen weitergeben würden. Lediglich zwei Teilnehmende haben sich gegen die Weitergabe ihrer persönlichen Daten an Dritte entschieden. Hierbei muss allerdings erwähnt werden, dass die meisten Teilnehmenden die Studie durchgeführt haben, um eine finanzielle Gegenleistung zu erhalten, sodass die Erwartungshaltung der Teilnehmenden dazu geführt haben könnte, die höchste finanzielle Aufwandsentschädigung zu wählen.

Somit kann die Hypothese bestätigt werden, weil große Unternehmen oder Konzerne etwa 15 % ihres gesamten IT-Budgets für die Sicherheit aufwenden, während mittelständische lediglich 10 % des Budgets im Bereich der IT für die Sicherheit investieren. Darüber hinaus zeigt die Auswahl der

finanziellen Gegenleistung der Teilnehmenden die geringe Bereitschaft, finanzielle Mittel für den Schutz ihrer Daten aufzuwenden.

5.8.5 Zur Hypothese 5: Gleichgültigkeit gegenüber der Abgabe von Informationen durch uneinsichtige Konsequenzen

Hypothese 5:

Die Gleichgültigkeit der Nutzenden bei der Abgabe von Informationen wird durch die uneinsichtigen Konsequenzen bedingt.

Die sozialen Repräsentationen, welche in der Studie von Plaut und Bartlett (2012) aufgezeigt werden, können weitestgehend bestätigt werden. Ferner gaben 45,4 % der Teilnehmenden als Grund für die Unterlassung des Lesens der AGB an, dass diese zu lang seien. Beim Darbieten der sozialen Repräsentation „AGBs zu lesen ist lang und zeitaufwendig“ stimmten 79,4 % der Teilnehmenden voll zu, während 14,4 % zustimmten und nur 4 % nicht zustimmten. Diese beiden Ergebnisse stimmen mit der ersten sozialen Repräsentation von Olson und Olson (2003) überein. Insgesamt 19,5 % der Teilnehmenden gaben als zweithäufigsten Grund an, dass die Sprache, in der der Text geschrieben wird, zu kompliziert sei. Beim Darbieten der sozialen Repräsentation „AGBs sind in einer schwer verständlichen Juristensprache formuliert“ stimmten 25,8 % der Teilnehmenden voll zu, während 38,1 % zustimmten und 19,6 % nicht zustimmten. Diese Ergebnisse stimmen mit der zweiten sozialen Repräsentation nach Hartley (2008) überein. Die Studie von Fuchs (2010), welche im Abschnitt 2.2.9 erläutert wurde, kommt ebenfalls zum Schluss, dass die Datenschutzbedingungen aufgrund der juristischen und komplexen Sprache von der Mehrheit der Nutzenden nicht gelesen und verstanden werden. Darüber hinaus sind die Einstellungen der Privatsphäre nur schwer verständlich und nicht sofort ersichtlich, sodass Nutzende kaum in der Lage seien, die Weitergabe von Informationen zu unterbinden. Den Mangel an Motivation gaben 16,5 % der Teilnehmenden als Grund an. Dieser Punkt stimmt mit keiner der sozialen Repräsentationen überein. Darüber hinaus gaben 11,3 % der Teilnehmenden an, dass die Texte von verschiedenen AGBs zu ähnlich seien, als dass sie sich erneut mit ihnen befassen müssten. Diese Ansicht stimmt mit der vierten sozialen Repräsentation überein, welche aussagt, dass alle CTAs den gleichen Inhalt haben (Epstein, 2006). Bei der Darbietung dieser Repräsentation stimmten 10,3 % der Teilnehmenden voll zu, 36,1 % stimmten zu, 26,8 % stimmten eher nicht zu und 9,3 % stimmten nicht zu. Zusätzlich nannten 5,2 % der Teilnehmenden als Begründung das Lesen der AGBs zu unterlassen, dass diesen zugestimmt werden muss. Dieses Ergebnis stimmt mit der dritten sozialen Repräsentation überein, welche aussagt, dass die Kunden die CTAs akzeptieren müssen, wenn sie das zugehörige Produkt erwerben wollen (Rakoff, 1983). Nur 3,1 % der

Teilnehmenden begründeten das Unterlassen des Lesens der AGBs mit dem Vertrauen in die Anbieter der Applikation. Diese Ansicht stimmt sowohl mit der siebten sozialen Repräsentation überein, welche besagt, dass Anbieter mit einem gewissen Ansehen keine ökonomischen Gründe haben, um faire Bedingungen anzubieten oder zu erzwingen, als auch mit der sechsten sozialen Repräsentation, welche besagt, dass die Bedingungen der Anbieter in den CTAs generell fair und vernünftig sind (Gillette, 2004). Die achte soziale Repräsentation „Niemand liest die AGBs“ wurde in den Freitextfeldern nicht genannt und fand im Fragebogen zum allgemeinen Umgang mit persönlichen Daten nur mäßige Zustimmung. Somit ist davon auszugehen, dass dieses Kriterium eher eine hintergründige Rolle bei dem Unterlassen des Lesens der AGB spielt.

Generell ist bei der Abfrage der Zustimmung der sozialen Repräsentationen aufgefallen, dass das höchste Maß an Zustimmung in den Aussagen „CTAs sind zu lang und zu zeitaufwendig“ und „Die Kunden müssen zustimmen, wenn sie das zugehörige Produkt erwerben wollen“, wiederzufinden ist. Hieraus könnte geschlossen werden, dass diese beiden Eigenschaften der CTAs bzw. AGBs hauptursächlich für das Unterlassen des vollständigen Lesens der zuzustimmenden Bedingungen sind. Die geringste Zustimmung ist bei den sozialen Repräsentationen „vor Gericht erdrückende Bedingungen werden im Nachhinein für ungültig erklärt“ und „Die Bedingungen der Anbieter in den CTAs sind generell fair und vernünftig“ zu sehen. Somit wäre es bedeutend notwendiger dem Problem des Nicht-Beachtens der AGBs entgegenzuwirken, indem eine Lösung gefunden wird, diese kürzer zu gestalten, um ein intuitives und unmittelbares Verständnis dieser zu schaffen. Hierzu sollte eine einfache schriftliche Darbietung der AGBs oder eine Alternative zu dieser gesucht werden.

Die sozialen Repräsentationen nach Olson und Olson (2003), Epstein (2006) und Hartley (2008) können bei der Frage, warum die Teilnehmenden die AGBs nur in Auszügen lesen, bestätigt werden, weil 28,57 % meinen, dass diese zu lang wären, 17,86 % verwiesen darauf, dass viele Standardformulierungen auftauchen würden, und 3,47 % empfanden den Text als zu unübersichtlich, um diesen komplett lesen zu wollen.

Es wird geprüft, ob die Gleichgültigkeit der Teilnehmenden, operationalisiert durch den angegebenen Stellenwert des Schutzes der persönlichen Daten, mit der Uneinsichtigkeit der Konsequenzen zusammenhängt. Dieser Zusammenhang kann nicht gezeigt werden. Es ist zu vermuten, dass das Ausmaß der Diskrepanz der beiden Gruppengrößen ($N1 = 15$, $N2 = 85$) einen signifikanten Unterschied finden zu können erschwert.

Um zu überprüfen, wie groß die Stichprobe hätte sein müssen, um ein signifikantes Ergebnis zu erzielen, wird eine Power-Analyse mit Hilfe des Programmes G*Power Version 3.1.9.2 von Axel Buchner, Edgar Erdfelder, Franz Faul und Albert-Georg Lang durchgeführt. Es resultiert eine

Effektstärke von *d* = 2,221, die zur Berechnung der Power verwendet wird. Die Power Analyse mit einem Alpha Fehler von 0,05 ergibt eine Power (1 – Beta-Fehler Wahrscheinlichkeit) von 0,189. Die anschließende Apriori-Analyse ergibt, dass bei oben genannter Effektstärke und einer Alpha-Fehler-Wahrscheinlichkeit von 0,05 eine Stichprobengröße von *N* = 532 nötig gewesen wäre, um eine Power von 0,8 zu erreichen.

Somit kann aufgrund der für diesen Signifikanztest nicht ausreichenden Stichprobengröße die fünfte Hypothese nicht aufrechterhalten werden.

5.8.6 Zur Hypothese 6: Aushändigen von persönlichen Daten für eine geringe Gegenleistung

Hypothese 6:

Die Nutzenden händigen für eine relativ geringe Gegenleistung ihre persönlichen Informationen aus.

In Abschnitt 2.2.7 wird ebenso angemerkt, dass die Verbraucher eine große Bereitschaft zeigen persönliche Daten freizugeben, um gewisse Gegenleistungen, beispielsweise digitale Dienstleistungen, zu erhalten (IFH Köln, 2015). Auch dieses Verhalten kann bestätigt werden. Obwohl die Teilnehmenden über zehn Minuten lang persönliche Meinungen und Favorisierungen innerhalb des Täuschungsexperiments preisgaben, wählte ein Großteil der Teilnehmenden die höchstmögliche Vergütung, welche mit der freizügigsten Weitergabe ihrer persönlichen Daten einherging. Die Teilnehmenden konnten in einem Fragebogen zur Weitergabe ihrer Daten entscheiden, welche regionalen, nationalen und internationalen Institutionen ihre Daten erhalten dürfen. Je mehr Institutionen und je größer die Reichweite dieser, desto höher war die finanzielle Gegenleistung. Die Teilnehmenden wählten eine durchschnittliche finanzielle Gegenleistung von 7,60 Euro (*SD* = 2,07) bei einer Spannweite von 2 bis 10 Euro. Während sich 23 Personen dafür entschieden, ihre persönlichen Daten für internationale Universitäten und Marktforschungsunternehmen freizugeben, entschieden sich lediglich zwei der Teilnehmenden dafür, dass ihre persönlichen Daten nur innerhalb der Studie beziehungsweise dieser Dissertation genutzt werden dürfen. Dabei kann kein Unterschied zwischen Geschlecht, Alter und Präsentationsform der Teilnahmevereinbarungen bei der gewählten Vergütung gefunden werden.

Während große Unternehmen einen stetig steigenden finanziellen Aufwand betreiben, um die Datensicherheit zu gewährleisten, scheint der Umgang mit den persönlichen Daten seitens der Endnutzenden sehr freizügig. Aus Abschnitt 2.2.10 wird ersichtlich, was für einen Stellenwert Datenschutz in der Wirtschaft hat, in dem sich die exponentiell steigenden Ausgaben von geschätzt

202 Milliarden US-Dollar vor Augen gehalten wird. Dieses Verhalten sollte den Endnutzenden als Vorbild dienen. Vor allem weil es den Endnutzenden möglich ist, Daten zu schützen, indem sie ihr Verhalten bzw. den Umgang entsprechend ändern und keine sonderlich hohen finanziellen Ausgaben zu leisten sind. Aus dieser Studie kann jedoch ein gegenteiliges Verhalten festgestellt werden. Anstatt die persönlichen Daten zu schützen, waren die Teilnehmenden bereit, für eine geringe finanzielle Gegenleistung all ihre Daten auszuhändigen.

Aus der Freizügigkeit der Teilnehmenden, persönliche Daten gegen einen geringen monetären Wert auszuhändigen, lässt sich darüber hinaus schließen, dass ein großer Anteil von Nutzenden mobiler Endgeräte eher abgeneigt ist, einen finanziellen Aufwand zu betreiben, um die Dienstleistungen einer Applikation nutzen zu können. Somit entfällt der App-Verkauf, der In-App-Verkauf sowie die Spende als Ertragserbringung, wie sie in Abschnitt 2.2.2 erläutert werden, für den Anbieter.

Verwunderlich ist hierbei, dass die Teilnehmenden ihren Daten einen hohen monetären Wert zuschreiben. Auf Grund der zahlreichen Ausreißer, welche teilweise in einem siebenstelligen Bereich liegen, wurde sich dazu entschieden, die Mediane zu vergleichen (Alter *Mdn* = 5 Euro, Geschlecht *Mdn* = 4 Euro, Adresse *Mdn* = 10 Euro, Standortdaten *Mdn* = 10 Euro, Kontaktdaten aus dem Adressbuch *Mdn* = 15 Euro, persönliche Bilder *Mdn* = 10 Euro, Browserchronik *Mdn* = 20 Euro). Dabei fällt auf, dass vor allem die Kontaktdaten sowie die Browserchronik als am wertvollsten bewertet werden. Eine Vermutung, weshalb ausgerechnet diese beiden Arten von Datensätzen mit dem höchsten monetären Wert beziffert wurden, sind die Möglichkeiten potenzielle Kunden über die Kontaktdaten zu gewinnen und diese mit personalisierter Werbung durch die Browserchronik zu konfrontieren. Die Ergebnisse der Studie von Staiano et al. (2014), welche ebenfalls im Abschnitt 2.2.7 vorgestellt wird, zeigen auf, dass die Positionsdaten von den Teilnehmenden am wertvollsten eingestuft werden und konnten somit nicht bestätigt werden.

Es sollte jedoch ebenfalls Rücksicht auf die Nutzenden genommen werden, welche die Weitergabe und Analyse ihrer persönlichen Daten als Eingriff in ihre Privatsphäre empfinden. Somit bleibt ihnen nur die Option, die Applikation nicht zu nutzen, um ihre Privatsphäre zu schützen. Eine alternative Option ist bereits im Bereich der In-App-Werbung, die in Abschnitt 2.2.3 beschrieben wird, zu betrachten. Einige kostenfreie Apps beinhalten Werbung, um sich zu finanzieren. Dabei haben die Nutzenden jedoch die Möglichkeit, eine Version finanziell zu erwerben, welche keine Werbung enthält. Dieses Modell ließe sich ebenfalls auf das Sammeln von Daten übertragen. Wichtig hierbei ist, dass die Nutzenden von vornherein umfassend über das Ausmaß der Datenweitergabe informiert werden. Sind diese damit nicht einverstanden, so sollten die Nutzenden die Möglichkeit haben, gegen einen

finanziellen Aufwand die Datenweitergabe unterbinden zu können, um weiterhin die Dienstleistung der Applikation zu nutzen.

Aufgrund der von der Mehrheit der Teilnehmenden gewählten Option, ihre Daten an die höchstmögliche Anzahl von Institutionen und Unternehmen für eine relativ geringe finanzielle Aufwandsentschädigung auszuhändigen, kann die sechste Hypothese aufrechterhalten werden.

5.8.7 Zur Hypothese 7: Unterschiede der Lesedauer zwischen den unterschiedlichen Präsentationsformen

Hypothese 7:

Zwischen den Nutzenden, welchen die Teilnahmebedingungen als CTA in digitaler Form und denen, welchen die Teilnahmebedingungen als Ausdruck in Papierform präsentiert wurden, besteht hinsichtlich der Lesezeit kein Unterschied.

Im Abschnitt 2.2.6 wurde bereits anhand einer Studie von Schwabe et al. (2020) dargelegt, dass bezüglich des Verständnisses und der Lesebereitschaft zwischen digitalen Texten und gedruckten Texten in Papierform keine Unterschiede aufzuweisen sind.

Beim Vergleich der Lesedauern zwischen den Präsentationsformen der Teilnahmevereinbarungen als Papierform und als digitales Dialogfenster kann, der Hypothese entsprechend, kein signifikanter Unterschied hinsichtlich der Lesedauer gefunden werden. Hieraus ließe sich schließen, dass die getesteten Personen einen schriftlichen Vertrag genauso bedenkenlos unterschreiben wie sie ein Dialogfeld mit einem einfachen Mausklick bestätigen.

Somit kann die siebte Hypothese aufrechterhalten werden.

Hierbei ist jedoch zu berücksichtigen, dass die Studie an einer Universität stattgefunden hat, welche von der Mehrheit als vertrauenswürdig und nicht gewinnorientiert angesehen wird (TUI Stiftung, 2018), sodass sich dieses Gefühl von Sicherheit in dem Unterlassen des Lesens der Teilnahmevereinbarungen widerspiegeln könnte.

Es wird eine Power-Analyse durchgeführt, um zu prüfen, wie groß die Stichprobe hätte sein müssen, um ein signifikantes Ergebnis zu erhalten. Es resultiert eine Effektstärke von d = 0,133, die zur Berechnung der Power verwendet wird. Die Power Analyse mit einem Alpha Fehler von 0,05 ergibt

eine Power von 0,074. Die anschließende Apriori-Analyse ergibt, dass bei oben genannter Effektstärke und einer Alpha-Fehler-Wahrscheinlichkeit von 0,05 eine Stichprobengröße von 1854 nötig gewesen wäre, um eine Power von 0,8 zu erreichen.

5.8.8 Diskussion der explorativen Ergebnisse

Um zu überprüfen, ob die Begründung für ein vollständiges Lesen, anteiliges Lesen oder Unterlassen des Lesens mit der Lesedauer zusammenhängen, wurden Korrelationen zwischen den Begründungen für die Häufigkeit der Befassung mit den Teilnahmevereinbarungen und der Lesedauer durchgeführt. Lediglich eine Korrelation lieferte ein signifikantes Ergebnis: Eine lange Lesedauer korreliert positiv mit der Angabe, die AGBs seien in zu komplizierter Sprache geschrieben, mit $r = 0{,}326$ und $p < .02$. Dies führt zu der Annahme, dass die Teilnehmenden bemüht waren, die AGBs zu lesen und zu verstehen, es ihnen jedoch aufgrund der komplizierten Sprache nicht gelungen ist.

In den folgenden Absätzen werden die explorativen Ergebnisse bezüglich der Lesedauer diskutiert.

5.8.8.1 Geschlechterunterschiede

Mit der anschließenden Testung soll überprüft werden, ob es einen Geschlechterunterschied gibt. Hierbei ist anzumerken, dass der Mittelwert der Lesedauer des männlichen Geschlechtes bei deskriptiver Betrachtung deutlich unter dem der Frauen liegt, explorativ jedoch kein signifikanter Unterschied zu finden ist. Dies ist der großen Standardabweichung der Datensätze zuzuschreiben.

Um zu überprüfen, wie groß die Stichprobe hätte sein müssen, um ein signifikantes Ergebnis zu erzielen, wird erneut eine Power-Analyse durchgeführt. Es resultiert eine Effektstärke von $d = 0{,}487$, die zur Berechnung der Power verwendet wird. Die Power Analyse mit einem Alpha Fehler von 0,05 ergibt eine Power von 0,369. Die anschließende Apriori-Analyse ergibt, dass bei oben genannter Effektstärke und einer Alpha-Fehler-Wahrscheinlichkeit von 0,05 eine Stichprobengröße von 142 nötig gewesen wäre, um eine Power von 0,8 zu erreichen. Alle weiteren Korrelationen mit dem Geschlecht ergeben keine signifikanten Unterschiede. Selbst bei der Vergütung, welche die Bereitschaft der Weitergabe persönlicher Daten repräsentiert, kann kein signifikanter Unterschied festgestellt werden. Somit können die Ergebnisse der Studie von Midha (2002), welche ergab, dass weibliche Nutzende größere Bedenken in Bezug auf das Einschreiten in ihre Privatsphäre haben als männliche Nutzende, nicht bestätigt werden.

5.8.8.2 Alter

Zunächst soll geprüft werden, ob ein Zusammenhang zwischen dem Alter und der Lesedauer vorliegt. Die Spearman-Korrelation zwischen Alter und Lesedauer ergibt einen negativen Zusammenhang, der jedoch nicht signifikant ist. Die Altersspanne liegt zwischen 18 und 68 Jahren und ist damit für altersbedingte physiologische Veränderungen, welche beispielsweise die Lesegeschwindigkeit beeinflussen, zu klein. Darüber hinaus sinkt die Lesegeschwindigkeit mit steigendem Alter (Rodríguez-Aranda, 2003), wobei in dieser Studie ein entgegengesetzter Verlauf zu beobachten ist. Eine mögliche Erklärung der geringen Auseinandersetzungszeit mit den Teilnahmevereinbarungen von älteren im Vergleich zu jüngeren Teilnehmenden ist, dass letztere häufiger mit AGBs konfrontiert werden, weil es bei diesen häufiger zu Installationen von Applikationen kommt und sie somit die Relevanz des Inhaltes der AGBs besser einschätzen können. Die Spearman-Korrelation zwischen dem Alter und der gewünschten Vergütung in Euro, welche die Teilnehmenden beim Dokument zur Weitergabe der Daten in Anhang G angaben, zeigt keine Signifikanz. Das bedeutet, dass auch ältere Menschen bereit sind, sämtliche persönliche Daten weiterzugeben, um den höchstmöglichen finanziellen Gegenwert zu erhalten. Dieses Ergebnis widerspricht der in Abschnitt 2.2.7 erwähnten Studie von Milne und Rohm (2000), welche einen negativen Zusammenhang zwischen der Bereitschaft zur Weitergabe der persönlichen Daten und dem Alter aufzeigt, sodass jüngere Menschen ein freizügigeres Verhalten aufweisen.

Die Spearman-Korrelation zwischen der gewählten Vergütung und der vorherrschenden Lesedauer ergibt kein signifikantes Ergebnis. Dieser Test wird mit dem Hintergrund durchgeführt, dass Personen, die eine geringere Vergütung wählen würden, vorsichtiger mit der Frei- bzw. Weitergabe ihrer Daten sind und somit auch die AGBs gründlicher lesen. Dies würde zu einer längeren Lesedauer führen. Die Nicht-Signifikanz des Ergebnisses ist mit der sehr einseitigen Auswahl der Vergütung seitens der Teilnehmenden sowie einer recht hohen Standardabweichung der Lesedauer zu begründen. Darüber hinaus wird eine Korrelation zwischen der Häufigkeit des Lesens der AGB und der Lesedauer, die für das Lesen der Teilnahmevereinbarungen notwendig ist, durchgeführt. Auch dieses statistische Verfahren erzielt keine Signifikanz im Ergebnis. Anlass für die Testung ist die Vermutung, dass Personen, die sich häufiger die AGBs durchlesen, mehr Zeit dafür investieren, weil sie die Relevanz besser einschätzen können. Dabei wird jedoch nicht berücksichtigt, dass nahezu keine Person den Aufwand aufbrachte, die Teilnahmevereinbarungen vollständig zu lesen. Somit besteht die Möglichkeit, dass die Personen die regelmäßig die AGBs lesen, in der gleichen Lesezeit einen Einblick in einen deutlich höheren Anteil der AGBs haben. Ferner korreliert das Alter signifikant negativ mit der Häufigkeit der Nutzung von Messenger Applikationen. Hieraus könnte abgeleitet werden, dass vor allem jüngere Personen einen intensiveren Umgang mit Applikationen im Bereich der sozialen

Netzwerke pflegen und somit deutlich mehr den Applikationen ausgesetzt sind, welche einen Großteil der persönlichen Daten weitergeben.

5.8.8.3 Unterschrift

Aufgrund der Tatsache, dass viele Teilnehmende vor dem Lesen der Teilnahmevereinbarungen bereits unterschrieben haben, wurde geprüft, ob es einen signifikanten Unterschied zwischen den Lesedauern der Gruppen gibt. Hierbei kommt die Vermutung auf, dass die Personen, die die Unterschrift schon im Vorhinein geleistet haben, sich deutlich kürzer mit den Teilnahmevereinbarungen befassten als die Personen, die die Unterschrift erst nach dem Lesen leisteten. Dieser Gedankengang ist damit zu begründen, dass bei geleisteter Unterschrift die Einwilligung bereits stattgefunden hat und der Inhalt der Teilnahmevereinbarungen nicht mehr für die Entscheidungsfindung relevant ist. Obwohl der Mittelwert der Gruppe der Personen, die nach dem Lesen der Teilnahmevereinbarungen unterschrieben haben, doppelt so hoch ist wie der jener der Gruppe der Personen, die davor unterschrieben haben, kann kein signifikantes Ergebnis gefunden werden.

Nur 7,8 % der Teilnehmenden gaben an, beim Unterschreiben der Einverständniserklärung gezögert zu haben. Hierbei ist davon auszugehen, dass der Rest der Stichprobe keinerlei Bedenken beim Unterschreiben der Teilnahmevereinbarung hatte. Weiterhin ist fraglich, ob dieses Verhalten mit der Nicht-Kenntnis der Konsequenzen oder der Inkaufnahme dieser verbunden ist.

5.9 Probleme und Ausblick

Eine der größten Bedenken war die Vertrauenswürdigkeit und der Ruf einer Universität. Dabei wird davon ausgegangen, dass die Teilnehmenden ein positives Bild von Universitäten und deren Forschungen haben. Die meisten Teilnehmenden halten die an einer Universität durchgeführten Experimente für gemeinnützig und wohlwollend. Dieses positive Bild der Universitäten könnte dazu geführt haben, dass die Teilnehmenden eine gewisse Sicherheit verspürt haben und somit nicht davon ausgehen, dass die Teilnahme an einer Studie negative Konsequenzen mit sich tragen könnte. Aus diesem Grund könnte die Vermutung aufgestellt werden, dass die Teilnehmenden somit weniger Zeit für das Lesen der Teilnahmevereinbarung aufgewandt haben als sie es unter anderen Umständen getan hätten. Allerdings belegen zahlreiche Studien (Bakos et al., 2014; Plaut & Bartlett, 2012) den geringen Aufwand des Lesens der AGBs, sodass davon auszugehen ist, dass die folgenden Ergebnisse dem alltäglichen Verhalten entsprechen. Ein weiterer Aspekt, der die Teilnehmenden dazu verleitet

haben könnte, freizügig mit ihren Daten umzugehen, ist die Formulierung in dem Dokument der Weitergabe der Daten, welche vermittelt, dass die Daten ausschließlich anonym an die entsprechenden Institutionen ausgehändigt werden. Diese Formulierung war ursprünglich nicht so vorgesehen, wurde jedoch von der Ethikkommission vorgeschrieben.

5.10 Fazit

In dieser Studie soll untersucht werden, ob und mit welcher Gründlichkeit die AGBs durchgelesen werden und wie freizügig die Teilnehmenden mit ihren persönlichen Daten umgehen. Darüber hinaus wird untersucht, ob die Präsentationsform der AGBs einerseits als Ausdruck in Papierform und andererseits als digitales Dialogfenster (Click-through-Agreement) Auswirkungen auf das Verhalten hat. Hierfür wurde ein Täuschungsexperiment entworfen, bei dem den Teilnehmenden zunächst vermittelt wurde, dass es sich um einen Persönlichkeitstest handle. Ziel dabei war es, die Teilnehmenden glauben zu lassen, dass viele persönliche Informationen über sie gesammelt wurden, um anschließend die Bereitwilligkeit der Weitergabe der Daten durch die Incentivierung in Form einer finanziellen Gegenleistung zu untersuchen.

Die wichtigsten Erkenntnisse aus den gesammelten Daten und der statistischen Analyse dieser Studie sind folgende:

a. Im Fragebogen gaben die meisten Teilnehmenden an, die AGBs allgemein nur in Auszügen zu lesen, während etwa ein Zehntel der Teilnehmenden angab, die AGBs komplett durchzulesen. Im direkten Interview, welches sich auf das Täuschungsexperiment bezog, gab über die Hälfte der Teilnehmenden an, die Teilnahmevereinbarungen vollständig und etwas weniger als die Hälfte der Teilnehmenden gaben an, die Teilnahmevereinbarungen teilweise gelesen zu haben. Nur 5,9 % der Teilnehmenden gaben an, die Teilnahmevereinbarungen nicht gelesen zu haben. Durchschnittlich wurden die Teilnahmevereinbarungen jedoch weniger als eine Minute betrachtet. Diese Zeit genügt nicht, um die dreieinhalb Volltextseiten gründlich durchlesen zu können.

b. Die Teilnehmenden schätzten die aufgewandte Lesedauer als deutlich länger ein als sie tatsächlich die Teilnahmevereinbarungen gelesen haben.

c. Die Mehrheit der Teilnehmenden ist nach dem Lesen der Teilnahmevereinbarung nicht bewusst gewesen, dass bei der Weitergabe ihrer Daten diese von Dritten genutzt werden können. Somit ist davon auszugehen, dass die Teilnehmenden die Teilnahmevereinbarung entweder nicht gründlich genug gelesen oder diese inhaltlich nicht richtig verstanden haben.

d. Aus der Theorie konnte eruiert werden, dass große Unternehmen und Konzerne mehr in die IT-Sicherheit investieren als mittelständische Unternehmen, während aus der durchgeführten Studie hervorgeht, dass Endnutzende nur einen sehr geringen Aufwand betreiben, um ihre persönlichen Daten zu schützen.

e. Die Teilnehmenden sind sich weniger über langfristige Konsequenzen bei der Weitergabe ihrer persönlichen Daten bewusst als über kurzfristige Konsequenzen, wie z.B. dem Erhalt von Spam-Mails.

f. Die Teilnehmenden haben ihren persönlichen Daten einen hohen Stellenwert zugeschrieben.

g. Die Teilnehmenden gaben an, dass sie die Click-through-Agreements allgemein als „zu lang und zu zeitaufwändig“ erachten und sie diesen sowieso zustimmen müssten, um das Produkt erwerben oder nutzen zu können.

h. Die Teilnehmenden werten das Lesen der AGBs als große Einbuße und sind nicht bereit, diese zum Schutz ihrer persönlichen Daten und Informationen hinzunehmen.

i. Die Teilnehmenden waren bereit, für eine geringe finanzielle Gegenleistung ihre Daten an sämtliche Unternehmen und Institutionen auszuhändigen.

j. Die Teilnehmenden schreiben ihren Daten einen hohen monetären Wert zu.

k. Zwischen den Präsentationsformen der Teilnahmevereinbarung als Papierform und als digitales Dialogfenster konnte kein signifikanter Unterschied hinsichtlich der Lesedauer gefunden werden.

l. Nur eine sehr geringe Anzahl der Teilnehmenden zögerte beim Unterschreiben der Einverständniserklärung.

Die Analyse des vorgestellten Experiments hat bereits gezeigt, dass die Teilnehmenden ein paradoxes Verhalten in Bezug auf den Wert ihrer Daten und den tatsächlichen Umgang mit ihnen zeigen.

Aus den eben aufgelisteten Erkenntnissen lässt sich schlussfolgern, dass die AGBs kürzer gestaltet werden müssen, um ein intuitives und unmittelbares Verständnis zu schaffen. Deshalb sollte eine Lösung gefunden werden, den Endnutzenden mit möglichst geringem kognitivem Aufwand die potenzielle Weitergabe ihrer persönlichen Daten durch den Erwerb oder das Herunterladen von Applikationen zu vermitteln.

6 Empirischer Versuch 2 – Einfluss einer Datenschutzskala auf das Auswahlverhalten im App-Markt

Das folgende Kapitel umfasst die zweite empirische Untersuchung, welche das Ziel hat, die Endnutzenden mobiler Endgeräte bei der Applikationsauswahl für Privatsphäre-Aspekte zu sensibilisieren und es den Endnutzenden somit zu ermöglichen, die Auswahl der Applikationen im Hinblick auf die Wahrung ihrer Privatsphäre bzw. den Schutz ihrer Daten zu optimieren.

Die folgenden Unterkapitel beinhalten die Forschungsfragen, Forschungshypothesen, die Untersuchungsvariablen sowie die Operationalisierung dieser. Abschließend erfolgt eine Beschreibung des durchgeführten Versuchs, der Methodik sowie der Ergebnisse.

6.1 Forschungsfragen

In dieser Studie soll evaluiert werden, ob Informationen über die Güte des Datenschutzes innerhalb eines App-Marktes die Kauf- bzw. Nutzungsentscheidung von Nutzenden beeinflussen. Ferner soll geprüft werden, ob die in Abschnitt 2.1.8 beschriebene Datenschutzgrundverordnung Auswirkungen auf das Applikationsverhalten bezüglich der Anzahl an Zugriffen auf die Daten der Endnutzenden mit sich bringt.

Wie schon in 2.2.11 beschrieben, zeigen die Ergebnisse der Studie von Tsai et al. (2011), dass Personen bei leichtverständlichen und auffällig dargestellten Informationen über den Eingriff in die Privatsphäre seitens der Applikation einen höheren finanziellen Aufwand betreiben würden, um ein gewisses Maß an Privatsphäre zu erhalten.

Darüber hinaus ist eine der Strategien zum Schutz der Privatsphäre, die in 2.2.12 beschrieben werden, dass Nutzende adäquat über die Verwendung und Verarbeitung ihrer Daten informiert werden sollen. Dies soll den Nutzenden in der aktuellen Studie ermöglicht werden, indem eine entsprechende Datenschutzskala dargestellt wird, die darüber Auskunft gibt, wie häufig die Applikation auf die Daten der Nutzenden zugreift. Ferner soll mit Hilfe einer Datenschutzskala das Kontiguitätsprinzip, welches in Abschnitt 2.2.5 erläutert wird, bei den Endnutzenden angewandt werden. Die Skala veranschaulicht den Nutzenden unmittelbar nach der Applikationssuche die Aggressivität der Applikation bezüglich des Einschreitens in die Privatsphäre. Somit wird das Problem der Datenweitergabe akut noch vor der Auswahl der Applikation den Nutzenden vor Augen gehalten, um diese abstrakte und mittelbare Gefahr zum Zeitpunkt der Entscheidung wahrzunehmen und in diese einfließen zu lassen.

Für das Experiment werden im Rahmen einer Vorstudie fünf verschiedene Skalen entworfen, um die Aggressivität der Applikation bei der Weitergabe persönlicher Daten zu illustrieren. Die adäquateste Skala wird anschließend in der Studie verwendet, mit der es die folgenden vier Forschungsfragen zu beantworten gilt:

a) Ist es möglich die Nutzenden durch eine Datenschutzskala für den Schutz ihrer persönlichen Daten zu sensibilisieren?

b) Führt die Darstellung einer Datenschutzskala in einem App-Markt zu einer einfacheren Entscheidung bezüglich der Applikationsauswahl?

c) Führt die Implementierung einer Datenschutzskala zu einer adäquateren Bewertung der Vertrauenswürdigkeit hinsichtlich der Aggressivität der Applikation?

d) Führt die Implementierung einer Datenschutzskala zu einem datenschutzfreundlichen Applikationsauswahlverhalten der Endnutzenden?

e) Führt die Implementierung einer Datenschutzskala zu einer schnelleren Entscheidungszeit bei der Applikationsauswahl.

f) Welchen Einfluss haben unterschiedliche Kenntnisse über die Datenschutzskala auf das Auswahlverhalten?

Ferner wird im Rahmen einer Vorstudie geprüft, ob die Einführung der EU-Datenschutzgrundverordnung eine Veränderung des Applikationsverhalten mit sich brachte.

6.2 Hypothesen

Im Abschnitt 2.2.13 wurde erörtert, dass gewisse Kontexthinweise, wie zum Beispiel Privatsphäresymbole wirksam eingesetzt werden können, um den nachfolgenden Umgang mit der Privatsphäre zu beeinflussen (Kelley et al., 2012). Dementsprechend ist davon auszugehen, dass die Nutzenden, die eine Datenschutzskala im App-Markt vorfinden, die Vertrauenswürdigkeit der Applikationen adäquater hinsichtlich deren Aggressivität einschätzen können als Nutzende, welche diese nicht vorfinden. Darüber hinaus wird angenommen, dass Nutzende mit einer detaillierten Beschreibung der Datenschutzskala die Vertrauenswürdigkeit der Applikationen adäquater hinsichtlich

deren Aggressivität einschätzen können als Nutzende, die die Datenschutzskala dargeboten bekommen, jedoch keine detaillierte Beschreibung erhalten, und als Nutzende, bei denen keine Datenschutzskala im App-Markt implementiert ist. Wie schon von Hoepman (2014) in den acht verschiedenen Strategien zum Schutz der Privatsphäre postuliert wurde, führt eine Darbietung einer adäquaten Information über den Nutzen und der Verwendung von persönlichen Daten zu einem besseren Schutz dieser. Von diesen Vermutungen lässt sich ableiten, dass Nutzende, welche eine Datenschutzskala mit einer detaillierten Beschreibung erhalten, weniger aggressive Applikationen wählen als Nutzende, die keine detaillierte Beschreibung zur Datenschutzskala erhalten und Nutzende, die keine Datenschutzskala erhalten. Ein weiterer Gedanke, der diese Vermutung verstärkt, ist die Tatsache, dass Nutzende, die eine detaillierte Beschreibung für die Datenschutzskala erhalten, schon mit dem Problem des Datenmissbrauches konfrontiert werden, indem sie die Funktion der Skala beschrieben bekommen haben. Hinsichtlich der Entscheidungszeit ist damit zu rechnen, dass die Verwendung der Datenschutzskala mit der Anzahl der Durchgänge abnimmt, weil die Skala als Entscheidungshilfe eine Heuristik ist und kognitiven Aufwand reduziert. Dass Entscheidungshilfen wie die Datenschutzskala den kognitiven Aufwand reduzieren, konnte in der Studie von Todd und Benbasat (1992) bewiesen werden. In der Studie führten die Entscheidungshilfen zu rationaleren und konsistenteren Antworten.

Weiterhin ist hinsichtlich der Entscheidungszeit mit einem Interaktionseffekt zu rechnen. Es wird angenommen, dass die Nutzenden, welche eine Datenschutzskala mit einer detaillierten Beschreibung erhalten einen höheren Abfall der Entscheidungszeit über mehrere Durchgänge haben als die Gruppe, die keine detaillierte Beschreibung erhält oder die Gruppe, für die keine Privatsphäreskala im App-Markt implementiert wird. Hierbei wird davon ausgegangen, dass die Nutzenden bei der ersten Konfrontation mit der Datenschutzskala eine gewisse Zeit aufwenden, um sich über die Funktion näher zu informieren. Nachdem die Nutzenden die Funktionsweise verstanden haben, ist mit einer deutlich kürzeren Entscheidungszeit zu rechnen, die sich im Laufe der Wiederholungen weiterhin verkürzt. Eine weitere Annahme besteht darin, dass die Nutzenden mit einer detaillierten Beschreibung der Datenschutzskala eine höhere Fixationsdauer auf diese aufweisen als die Nutzenden, die keine detaillierte Beschreibung zur Datenschutzskala erhalten. Somit lassen sich folgende Hypothesen formulieren, die zur besseren Überprüfung in Unterhypothesen aufgeteilt werden:

Hypothese 1:

Die Gruppen, welche eine Datenschutzskala zur Verfügung haben und mehr Informationsgehalt über diese erhalten, bewerten die Vertrauenswürdigkeit der Applikation adäquater hinsichtlich deren

Aggressivität als jene Gruppen ohne Datenschutzskala oder mit weniger Informationsgehalt über diese.

- Hypothese 1a: Die Gruppe (A) der Nutzenden, die eine Datenschutzskala mit einer detaillierten Beschreibung erhält, bewertet die Vertrauenswürdigkeit der Applikation adäquater hinsichtlich deren Aggressivität als die Gruppe (B), die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält. Außerdem wird angenommen, dass die Gruppe (A) die Vertrauenswürdigkeit auch exakter bewertet als die Gruppe (C), welche zur Datenschutzskala keine detaillierte Beschreibung erhält und die Gruppe (D), die keine Datenschutzskala erhält.

- Hypothese 1b: Die Gruppe (B) der Nutzenden, die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält, bewertet die Vertrauenswürdigkeit der Applikation adäquater hinsichtlich deren Aggressivität als die Gruppe (C) der Nutzenden, die eine Datenschutzskala ohne detaillierte Beschreibung erhalten und die Gruppe (D), die keine Datenschutzskala erhält.

- Hypothese 1c: Die Gruppe (C) der Nutzenden, die eine Datenschutzskala ohne detaillierte Beschreibung gezeigt bekommt, bewertet die Vertrauenswürdigkeit der Applikation adäquater hinsichtlich deren Aggressivität als die Gruppe (D), die keine Datenschutzskala erhält.

Hypothese 2:

Mit zunehmender Information über die Applikationen bezüglich des Datenschutzes werden weniger aggressive Applikationen gewählt.

- Hypothese 2a: Die Gruppe (A) der Nutzenden, die eine Datenschutzskala mit einer detaillierten Beschreibung erhält, wählt weniger aggressive Applikationen als die Gruppe (B), die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält, die Gruppe (C), die keine detaillierte Beschreibung erhält und die Gruppe (D), die keine Datenschutzskala erhält.

- Hypothese 2b: Die Gruppe (B) der Nutzenden, die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält, wählt weniger

aggressive Applikationen als die Gruppe (C), die eine Datenschutzskala ohne detaillierte Beschreibung gezeigt bekommt und die Gruppe (D), die keine Datenschutzskala erhält.

- Hypothese 2c: Die Gruppe (C) der Nutzenden, die eine Datenschutzskala ohne detaillierte Beschreibung erhält, wählt weniger aggressive Applikationen als die Gruppe (D), die keine Datenschutzskala erhält.

Hypothese 3:

Die Gruppen, welche eine Datenschutzskala zur Verfügung haben und mehr Informationsgehalt über diese erhalten, zeigen einen stärkeren Abfall der Entscheidungszeit über die Zeit als jene Gruppen ohne Datenschutzskala oder mit weniger Informationsgehalt über diese.

- Hypothese 3a: Die Gruppe (A) der Nutzenden, die eine Datenschutzskala mit einer detaillierten Beschreibung erhält, zeigt einen stärkeren Abfall der Entscheidungszeit (von Suche bis Installation der Applikation) über die Zeit als die Gruppe (B), die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält, die Gruppe (C), die eine Datenschutzskala ohne detaillierte Beschreibung erhält und die Gruppe (D), die keine Datenschutzskala erhält.

- Hypothese 3b: Die Gruppe (B) der Nutzenden, die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält, zeigt einen stärkeren Abfall der Entscheidungszeit (von Suche bis Installation) über die Zeit als die Gruppe (C), die eine Datenschutzskala ohne detaillierte Beschreibung erhält und die Gruppe (D), die keine Datenschutzskala erhält.

- Hypothese 3c: Die Gruppe (C) der Nutzenden, die eine Datenschutzskala ohne detaillierte Beschreibung erhält, zeigt einen stärkeren Abfall der Entscheidungszeit (von Suche bis Installation) über die Zeit als die Gruppe (D), die keine Datenschutzskala erhält.

Hypothese 4:

Die Fixationsdauer auf die Datenschutzskala steigt mit der Information über diese.

- Hypothese 4a: Die Fixationsdauer der Datenschutzskala ist höher bei der Gruppe (A) der Nutzenden, die eine Skala mit detaillierter Beschreibung bekommen als bei der Gruppe (B), die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält und der Gruppe (C), die eine Datenschutzskala ohne detaillierte Beschreibung erhält.

- Hypothese 4b: Die Fixationsdauer der Datenschutzskala ist höher bei der Gruppe (B) der Nutzenden, die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält als bei der Gruppe (C), die eine Datenschutzskala ohne detaillierte Beschreibung erhält.

6.3 Versuchsdesign

In der aktuellen Studie werden zunächst Daten über die Aggressivität von Applikationen gesammelt, welche über die Zugriffshäufigkeit auf Daten gemessen werden. Das Messen der Abrufe von privaten Daten wurde zunächst in Karlstad, Schweden, später auch in Berlin durchgeführt. Im nächsten Schritt wurde ein entsprechender App-Markt, angelehnt an den Google Playstore, eigens entwickelt. Dieser beinhaltet eine Sortierfunktion, mit der die Applikationen nach der Anzahl von Abrufen privater Daten und somit nach dem Grad der Berücksichtigung der Privatsphäre sortiert werden können. Darüber hinaus ist direkt im App-Markt neben jeder Applikation eine Datenschutzskala implementiert, welche Aufschluss über die Anzahl der angeforderten Rechte geben soll. Ferner haben die Teilnehmenden die Möglichkeit zwei Diagramme einzusehen, welche das Abfragen von Rechten der Applikationen im Stand-by-Modus illustrieren und das Risiko der Freigabe persönlicher Daten durch diese Abfrage präsentieren.

Anschließend wurde eine Studie durchgeführt, in der die Teilnehmenden verschiedene Aufgaben bewältigen sollten, welche auch im Alltag mit der Nutzung eines mobilen Endgerätes üblich sind. Die Aufgaben sollten jeweils mit selbst ausgewählten Applikationen ausgeführt werden, wobei mehrere für die Aufgabe passende Applikationen zur Verfügung standen, die jeweils unterschiedlich oft auf die Daten des Telefons zugriffen und somit divergent in die Privatsphäre der Nutzenden eindringen. Das Verhalten der Teilnehmenden wurde unter anderem mit einem Eye-Tracker aufgezeichnet, um zu verfolgen, welche Informationen des App-Marktes genauer betrachtet wurden. Eine Kontrollgruppe, die denselben App-Markt ohne die Datenschutzinformationen verwendete, wurde eingesetzt, um das Verhalten der Endnutzenden vergleichen zu können. Für das Experiment wurden im Rahmen einer

Vorstudie fünf verschiedene Skalen entworfen, um die Aggressivität der Applikation bei der Weitergabe persönlicher Daten zu illustrieren.

Die durchzuführende empirische Untersuchung besteht aus einem 6 x 1 between-subjects Design. Die Teilnehmenden werden randomisiert einer der folgenden vier Gruppen mit unterschiedlichen Versuchsbedingungen zugeteilt, die sich auf die unterschiedliche Verfügbarkeit von Informationen im App-Markt beziehen. Jede Gruppe durchläuft somit nur eine der vier Versuchsbedingungen:

- Gruppe A: Datenschutzskala mit einer detaillierten Beschreibung als Einleitung
- Gruppe B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf durch eigenständiges Klicken auf die Datenschutzskala
- Gruppe C: Datenschutzskala ohne eine detaillierte Beschreibung
- Gruppe D: Keine Datenschutzskala

Die Gruppe ohne Datenschutzskala stellt hierbei die Kontrollgruppe des Versuchs dar.

Zur Simulation des alltäglichen Gebrauchs eines mobilen Endgerätes, werden den Teilnehmenden acht Szenarien präsentiert, in welche sie sich hineinversetzen und eine dazu passende Applikation aus dem App-Markt auswählen, herunterladen und verwenden sollen, um alltagsübliche Aufgaben zu lösen. Dabei wird ihnen verschwiegen, dass das Experiment den Einfluss der Datenschutzskala auf das Auswahlverhalten eruieren soll. Ihnen wird lediglich vermittelt, dass das Experiment zur Erfassung der Benutzerfreundlichkeit durchgeführt wird. Die Szenarien beinhalten beispielsweise das Schreiben einer Nachricht (Messenger) oder die Führung einer Videokonferenz. Die Blickbewegung der Teilnehmenden wird während des Auswahlverfahrens aufgezeichnet, um dieses später zu analysieren und die Teilnehmenden bei der Beantwortung eines halbstrukturierten Interviews nach der Methode des lauten Denkens (Konrad, 2020; Sandmann, 2014) bzw. der Think-Aloud-Methode zu unterstützen (Guan et al., 2006; Ramey et al., 2006).

Nach der Erfüllung von acht verschiedenen Aufgaben werden die Teilnehmenden aufgeklärt und das eigentliche Ziel der Studie genannt.

Anschließend werden die Teilnehmenden gebeten einen Fragebogen auszufüllen, um die Bekanntheit der im Experiment verwendeten Applikationen zu erfassen (Abbildung 13 F1). Daraufhin wird eine Videokonfrontation mit dem bereits erwähnten Interview durchgeführt, bei dem die Teilnehmenden erläutern sollen, weshalb sie bestimmte Bereiche fixiert haben und worauf die meiste Aufmerksamkeit gerichtet wurde. In einem weiteren Fragebogen sollen die Teilnehmenden die Einfachheit der Auswahl und die Vertrauenswürdigkeit (Abbildung 13 F2) der Applikation bewerten.

Weiterhin werden sie gebeten in dem Fragebogen die Datenschutzskala bezüglich der Akzeptanz und der Benutzerfreundlichkeit zu beurteilen (Abbildung 13 F3). Abschließend werden sie aufgefordert, eine angepasste Version des MUIPC-Fragebogens (measuring mobile users' concerns for information privacy) auszufüllen (Abbildung 13 F4). In dem letzten Teil des Fragebogens sollen die demographischen Daten und favorisierten Bewertungssysteme festgehalten werden (Rezension, Sterne, Aufrufe, Downloads und Datenschutzskala) (Abbildung 13 F5).

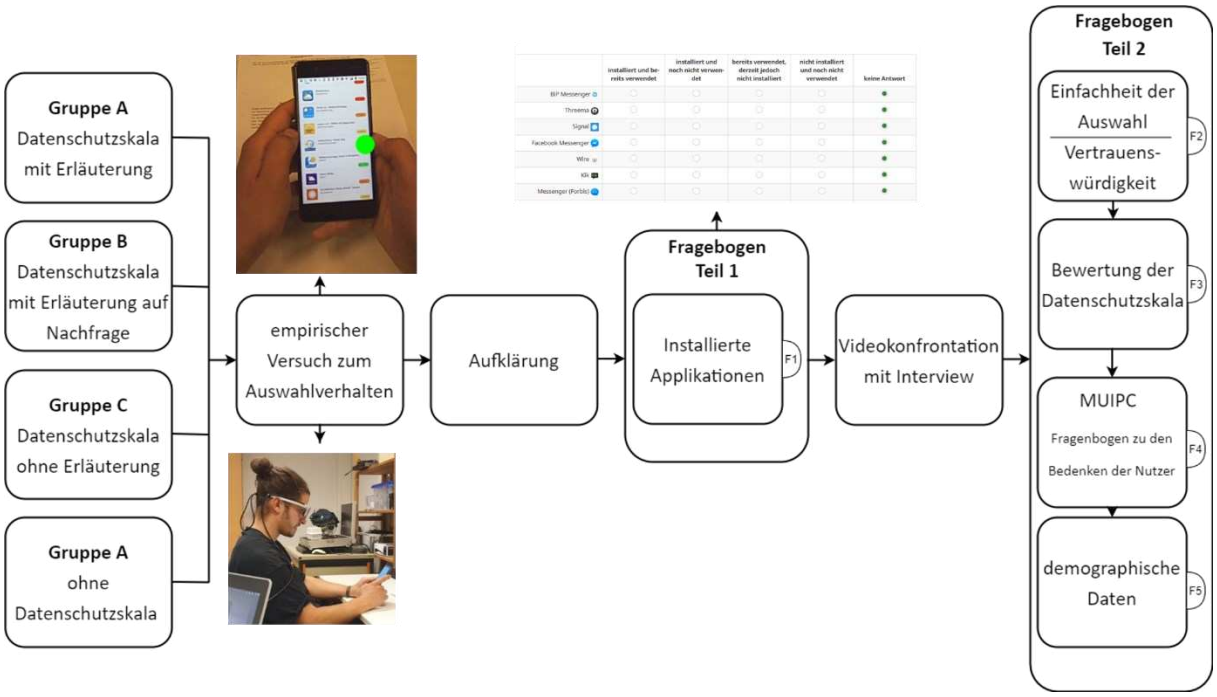


Abbildung 13. Flussdiagramm des zweiten empirischen Versuchs bezüglich der Datenschutzskala.

Dieses Flussdiagram veranschaulicht den Ablauf der zweiten Studie zur Erfassung des Einflusses einer Datenschutzskala auf das Auswahlverhalten in einem App-Markt.

6.4 Untersuchungsvariablen

Die zweite empirische Studie dieser These enthält ebenfalls eine unabhängige Variable und sechs abhängige Variablen, welche in den folgenden Abschnitten näher beschrieben werden.

Unabhängige Variable (UV)

Das Versuchsdesign beinhaltet eine unabhängige Variable, welche die Auswirkungen von der Information über das Eindringen der Applikation in die Privatsphäre erfassen soll.

- UV1: Die Information über das Eindringen der Applikation in die Privatsphäre

Die unabhängige Variable hat dabei vier Ausprägungen. Die Stichprobe wird dementsprechend in vier Gruppen aufgeteilt. Bei der ersten Gruppe wird die Datenschutzskala in den App-Markt implementiert, wobei die Nutzenden dieser Gruppe eine detaillierte Beschreibung über die Funktion der Skala erhalten. Die detaillierte Beschreibung zu der Datenschutzskala entspricht der Beschreibung, die beim Tippen auf die Schaltfläche der Datenschutzskala erscheint und im Anhang Q illustriert ist. Diese detaillierte Beschreibung wird den Teilnehmenden mit der Bitte vorgelegt, sich diese durchzulesen. Ziel ist es hier, eine bereits etablierte Datenschutzskala zu simulieren, wobei die Nutzenden bereits über Kenntnis der Funktionsweise und der Bedeutung der Datenschutzskala verfügen. Zusätzlich ist es den Teilnehmenden dieser Gruppe möglich, auf die Datenschutzskala zu tippen, um die Beschreibung erneut zu öffnen und zwei Diagramme einzusehen, welche das Abfragen von Rechten der Applikation in Stand-by-Modus illustrierte und das Risiko der Freigabe persönlicher Daten durch diese Abfrage präsentierte. Ein Bildschirmabzug der Benutzeroberfläche ist im Anhang Q zu finden.

Die zweite Gruppe und somit auch die zweite Ausprägung beinhaltet die Implementation der Datenschutzskala in den App-Markt, jedoch nur mit einer detaillierten Beschreibung, die beim eigenständigen Klicken auf die Datenschutzskala angezeigt wird. Diese Bedingung stellt die Situation dar, welche der Realität am nächsten kommt, weil bei der Einführung der Datenschutzskala die Endnutzenden mit der Datenschutzskala konfrontiert werden würden ohne eine detaillierte Beschreibung zu erhalten, diese jedoch jederzeit abrufbar wäre. Die dritte Gruppe erhält ebenfalls eine Datenschutzskala, hat jedoch nicht die Möglichkeit eine Beschreibung dieser zu erhalten. Hierbei soll in Erfahrung gebracht werden, ob es von Nöten ist, überhaupt eine Erläuterung zur Verfügung zu stellen oder die Skala intuitiv interpretiert wird. Somit variiert innerhalb der drei Gruppen der Informationsgehalt über die Datenschutzskala, dessen Auswirkungen auf das Auswahlverhalten überprüft werden soll. Die vierte Ausprägung stellt die Kontrollgruppe dar, welche keine Datenschutzskala vorfinden wird. Die Kontrollgruppe soll überprüfen, ob die Illustration einer Datenschutzskala überhaupt einen Einfluss auf die Applikationsauswahl erwirkt.

Abhängige Variablen (AV):

Der Versuch enthält sechs abhängige Variablen. Die erste abhängige Variable bezieht sich auf die Nutzererfahrung (User Experience) und umfasst die Bewertung der Datenschutzskala. Hierbei sollen die Nutzenden unter anderem bewerten, ob die Datenschutzskala vertrauenswürdig, benutzerfreundlich, leicht zu verstehen, intuitiv, gültig, zuverlässig, verwirrend, ausreichend oder komplex ist und ob die Nutzenden die Datenschutzskala überhaupt beachten.

Die zweite abhängige Variable soll darüber hinaus die aufgewandte Zeit zum Verstehen der Skala erheben. Hierbei wird die Fixationszeit auf die Skala durch Eye-Tracking gemessen.

Die dritte abhängige Variable soll ausfindig machen, ob die Datenschutzskala zu einem Auswahlverhalten führt, welches Applikationen bevorzugt, die weniger in die Privatsphäre eingreifen bzw. als weniger aggressiv gekennzeichnet worden.

Die vierte abhängige Variable soll die Informationsaufnahme beim Evaluieren der Entscheidung festhalten. Hierfür wird die Zeit von der Aufgabenstellung bis zur Installation der Applikation gemessen und unter den drei Gruppen verglichen.

Die fünfte abhängige Variable soll erfassen, ob die Datenschutzskala einen Einfluss auf die Fixationswechsel innerhalb der Oberfläche des App-Marktes mit sich bringt. Hierbei soll festgehalten werden, ob und wie sich die Aufmerksamkeit mit der Illustration einer Datenschutzskala verändert.

Die sechste abhängige Variable soll mit Hilfe einer Videokonfrontation erfassen, ob die Datenschutzskala zu einer einfacheren Applikationsauswahl führt und ob die Vertrauenswürdigkeit in die Applikation durch die Skala adäquater eingeschätzt wird. Darüber hinaus werden die Teilnehmenden befragt, weshalb sie bestimmte Bereiche fixiert haben und worauf sie die meiste Aufmerksamkeit gerichtet haben.

- AV1: Bewertung der Datenschutzskala
- AV2: Aufmerksamkeit auf die Datenschutzskala
- AV3: Applikationsauswahl
- AV4: Entscheidungszeiten
- AV5: Fixationswechsel
- AV6: Einfachheit der Applikationsauswahl und Vertrauenswürdigkeit in die ausgewählte Applikation

Kontrollvariablen:

Um mögliche Abweichungen der Ergebnisse erklären zu können werden über die unabhängigen und abhängigen Variablen hinaus sieben Kontrollvariablen erhoben. Die erste Kontrollvariable ist die Technikaffinität und die zweite Kontrollvariable ist die Häufigkeit der Nutzung des mobilen Endgerätes, die im Fragebogenteil im Anhang T erfasst werden.

Die dritte Kontrollvariable beinhaltet sechs Untervariablen, bestehend aus den demografischen Daten der Teilnehmenden wie dem Alter, dem Geschlecht und dem sozioökonomischen Status. Die Daten werden mit Hilfe eines Fragebogens, der sich im Anhang U Teil D befindet erfasst.

Die vierte Kontrollvariable soll die Bekanntheit bzw. die Vertrautheit mit den Applikationen erfassen. Der Grund der Abfrage besteht darin, dass bei einer bereits installierten Applikation, welche zu dem Zeitpunkt auch auf dem privaten Endgerät verwendet wurde, eine höhere Wahrscheinlichkeit gegeben ist, dass eben diese Applikation bei der Auswahl zur Erfüllung der Aufgabe favorisiert wird. Um sicherzustellen, dass die Auswahl nicht aufgrund von Vorerfahrung beeinflusst wird, wird überprüft, inwieweit sich die Teilnehmenden mit der Applikation auseinandergesetzt haben. Hierfür wurde ein Fragebogen erstellt, der nach dem Experiment an die Teilnehmenden verteilt wird. Der Fragebogen listet alle Applikationen auf, die im Rahmen des Experiments verwendet werden. Die Teilnehmenden werden gebeten anzugeben, ob sie die Applikation installiert haben und bereits verwenden, ob sie die Applikation bereits verwenden, jedoch derzeit nicht installiert haben, ob sie die Applikation nicht installiert und verwendet haben und ob sie die Applikation installiert und noch nicht verwendet haben. Der Fragebogen ist in Anhang U Teil A einzusehen.

Die fünfte Kontrollvariable erfasst, wie wichtig die Datensicherheit für die Teilnehmenden ist. Diese wird im Fragebogenteil D zu den demografischen Fragen unter D4 erhoben (s. Anhang U).

Die sechste Kontrollvariable soll erfassen, ob die Teilnehmenden schon einmal Opfer von Datenmissbrauch waren oder eine unerwünschte Konsequenz aus dem Akquirieren einer Applikation erleiden mussten. Diese Variable wird mit Hilfe der Dimension der vorherigen Datenschutzerfahrung aus dem MUIPC erfasst, die in Abschnitt 2.2.11 beschrieben ist.

- KV1: Technikaffinität der Teilnehmenden
- KV2: Häufigkeit der Nutzung des mobilen Endgerätes
- KV3: Demographische Daten (Alter, Geschlecht und sozioökonomischer Status)
- KV4: Bekanntheit der Applikation
- KV5: Stellenwert der Datensicherheit für die Teilnehmenden
- KV6: schlechte Erfahrungen bezüglich des Missbrauchs persönlicher Daten

6.5 Versuchsvorbereitung

In diesem Kapitel werden alle Schritte geschildert, die für die Durchführung dieses empirischen Versuches notwendig sind. Diese umfassen zwei Vorstudien, in denen zunächst die Anzahl der

Zugriffsberechtigungen sowie die Häufigkeit der Nutzung dieser erfasst werden. Anschließend werden geeignete Illustrationen einer Datenschutzskala entworfen, um diese mit Hilfe eines Fragebogens beurteilen zu lassen. Daraufhin wird die adäquateste Illustration der Datenschutzskala in einem App-Markt implementiert und die Stichprobengröße für das Resultieren eines signifikanten Ergebnisses berechnet.

6.5.1 Sammeln der Zugriffsdaten

Zunächst sollte untersucht werden, wie häufig Applikationen von den eingeforderten Rechten Gebrauch machen, um auf die Daten der Nutzenden auf dem mobilen Endgerät zuzugreifen. Hierbei wurde unterschieden, ob der Zugriff auf die Daten für die Primärfunktion, also der Funktion, für die die Applikation installiert wurde, benötigt wurden oder einer sekundären Funktion wie dem Abgreifen und Weiterleiten von Daten diente. Mit Hilfe dieser Daten sollte die bereits in den vorherigen Abschnitten erwähnte Datenschutzskala die Applikationen nach deren Aggressivität kategorisieren. Weiterhin sollte untersucht werden, ob das Verhalten der Applikationen sich durch die neue EU-Datenschutzverordnung, welche in Abschnitt 2.1.8 erläutert wurde, verändert hat. Zur Bestimmung der Aggressivität von Applikationen in Bezug auf die Zugriffshäufigkeit auf die Daten des Endgerätes wurden 80 verschiedene Applikationen installiert, zehn Applikationen zu jeder der folgenden Kategorien: Messenger, Videokonferenzen, Wetter, E-Mail, Musik, Fitness, Spiele und Nachrichten. Eine Tabelle mit den jeweiligen Applikationen, die nach den eben genannten Kategorien sortiert sind, befindet sich im Anhang Y (s. Tabelle 31). Die in der Tabelle 31 aufgeführten Applikationen wurden auf fünf Endgeräten der Marke Nokia des Modells TA-1053 installiert. Die Endgeräte wurden mit Betriebssystem Android 7.1.1 Nougat versehen, um ein „Rooten“ zu ermöglichen und somit die Möglichkeit zu schaffen, sämtliche Applikationen überwachen zu können. Beim „Rooten“ eines Gerätes werden Entwickleroptionen freigeschaltet, die es erlauben auf Einstellungen zurückzugreifen, die umfassenden Eingriff in das System haben können, wie zum Beispiel das Übertakten des Prozessors. Hierfür war es zunächst von Nöten, einen geeigneten „Bootloader“ auf die Geräte zu spielen. Für die gewählten Endgeräte kam zu der Zeit nur ein Anbieter in Frage. Somit wurde der Bootloader vom Team Win Recovery Project mit der Version 3.1.1-0 verwendet. Anschließend konnte das Betriebssystem aufgesetzt und die erforderlichen Applikationen installiert werden.

Personas für die Applikationen:

Um eine möglichst realitätsnahe Situation zu simulieren, wurden für die verschiedenen Applikationen vor der Versuchsdurchführung unterschiedliche Personas erstellt und deren fiktive Daten in die Applikation eingetragen. Diese beinhaltete E-Mail-Adresse, Name, Geburtsdatum, Gewicht und Größe,

abhängig von dem Aufbau und den Anforderungen der unterschiedlichen Applikation. Die genauen Daten der vier Personas sind dem Anhang L zu entnehmen und konnten somit nur bei einigen der installierten Applikationen angewendet werden, weil es mehrere der auf dem mobilen Endgerät installierten Applikationen gab, bei denen keine persönlichen Daten angegeben werden konnten, beispielsweise Wetterapplikation oder Spiele. Die Applikationen, bei denen keine Personalisierung möglich war, wurden in Tabelle 31 mit einem Asterisk markiert. Durch die hohe Anzahl an Applikationen wurden die Nutzenden mit relativ vielen Benachrichtigungen konfrontiert, was dazu führte, dass diesen eher weniger Beachtung geschenkt wurde. Darüber hinaus wurden die Applikationen so ausgewählt, dass sie möglichst unterschiedliche Zugriffe auf das Endgerät einfordern. Diese waren bei der Installation im App-Store nachzuvollziehen.

Um möglichst valide Daten zu sammeln, wurde für jede installierte Applikation, falls erforderlich, ein entsprechendes Konto erstellt und die Geräte an fünf verschiedene Teilnehmende ausgehändigt. Den Teilnehmenden wurde vermittelt, dass sie das mobile Endgerät so häufig wie möglich nutzen und es stets mit sich führen sollten. Es wurde auch in Betracht gezogen, dass die Teilnehmenden ihre eigenen Konten nutzen, beziehungsweise eigene Konten erstellen. Allerdings wurde dieses Vorhaben verworfen, um nicht zu sehr in die Privatsphäre der Teilnehmenden einzugreifen. Somit wurde zwar erfasst, wann, wo, wie häufig und auf welche internen Ressourcen zugegriffen wurde. Der Inhalt der Daten wurde allerdings nicht eingesehen. Zu den internen Ressourcen gehörten unter anderem der Zugriff auf die Kamera, die grobe und exakte Ortung, das Lesen des internen und externen Speichers sowie die Aufnahme von Tonaufnahmen. Zur Überwachung der Applikationen wurde eine in Kooperation mit der Universität Karlstad erstellte Software mit dem Namen A-Ware genutzt. Ein Bildschirmabzug der Oberfläche von der eben genannten Applikation ist dem Anhang X zu entnehmen. Diese beinhaltete die Funktion eines sogenannten Logging Services, ein Prototyp einer Überwachungs-Applikation, welche in der Lage war, die Zugriffe auf die internen Ressourcen festzuhalten. Hierfür wurde der Befehl AppOpsCommand genutzt, welcher nach einem Zeitintervall überprüfte, welcher Ressourcenzugriff bei der jeweils installierten Applikation zuletzt stattgefunden hat und diese in einem bestimmten vordefinierten Format festhielt. Der Inhalt wurde anschließend in eine JSON-Datei übertragen, welche aus drei Feldern bestand: der Name der Applikation, der Name der Ressource, auf die zugegriffen wurde und der Zeitstempel des Zugriffs. Die gesammelten Daten wurden anschließend automatisch und anonymisiert über eine verschlüsselte Verbindung an einen Server der Universität in Karlstad übertragen. Zusätzlich wurde noch eine Funktion eingebaut, die es den Nutzenden ermöglicht, die JSON-Datei manuell und lokal auf dem Gerät zu speichern, sodass bei einem möglichen Fehler der Übertragung die angeforderten Zugriffsberechtigungen direkt von dem Gerät heruntergeladen und begutachtet werden konnten. Der Server war für das Sammeln, Verarbeiten und Speichern der Daten

der Endgeräte verantwortlich, die kontinuierlich mit diesem synchronisiert wurden. Die Daten wurden zunächst lokal auf dem Endgerät gespeichert, um anschließend in einem vordefinierten Zeitintervall an den Server gesendet zu werden. Der Server erstellte für jedes registrierte Endgerät ein Profil. Darüber hinaus war er für die Analyse der Daten sowie die Pflege der Datenbank zuständig. Um die Aggressivität der Applikationen vor und nach der neuen EU-Datenschutzgrundverordnung, welche am 25. Mai 2018 in Kraft getreten ist, zu vergleichen, wurde die Messung an zwei verschiedenen Zeitpunkten getätigt.

Neben dem Sammeln der Zugriffsdaten für die Erstellung der Datenschutzskala stellen sich hierbei vier zentrale Fragen:

- Hat die neue EU-Datenschutzgrundverordnung einen Einfluss auf die Software der Endnutzenden?
- Hat die neue EU-Datenschutzgrundverordnung einen Einfluss auf die Art der Programmierung der Applikation?
- Hat die neue EU-Datenschutzgrundverordnung einen messbaren Effekt auf das Verhalten von Applikationen?

Die Messungen vor der Datenschutzgrundverordnung fanden von März bis November 2017 statt und wurden ausschließlich in Karlstad, Schweden, von Momen, Hatamian und Fritsch (2019) durchgeführt, während die zweite Erhebung in Berlin vom 08.11.2018 bis 23.05.2019 stattfand und unter der Leitung des Autors durchgeführt wurde. Hierbei ist zu erwähnen, dass die Ausgabe der Endgeräte an die Teilnehmenden ausschließlich in der zweiten Messung in Berlin stattfand. Die Datensammlung in Schweden fand lediglich unter Laborbedingungen statt, wobei die Endgeräte nicht aktiv bedient wurden. In dieser Studie wurde sich dafür entschieden, hauptsächlich die sogenannte gefährliche Berechtigung (Android dangerous permission privileges) (Documentation, 2019) als Indikator für die Aggressivität der Applikationen zu verwenden. Hierbei wurde ebenfalls darauf geachtet, ob die angeforderten Rechte mit den Funktionen der Applikationen und mit den Datenschutzerklärungen übereinstimmten. Darüber hinaus sollte die Zugriffsberechtigungen nur für den Zweck verwendet werden, für den sie auch erteilt wurde und somit das Prinzip der Zweckbindung (Artikel 5 - 1 (B)) eingehalten werden. Weiterhin sollte beobachtet werden, ob das Prinzip der Datenminimierung (Artikel 5 - 1 (C)) eingehalten wurde, indem der Gebrauch der Zugriffsberechtigungen so niedrig wie möglich gehalten werden sollte, während mit der Applikation interagiert wurde. Eines der wichtigsten Prinzipien dieser Arbeit ist das Prinzip der Transparenz (Artikel 5 - 1 (A)), welches besagt, dass „personenbezogene Daten […] auf rechtmäßige Weise, nach Treu und Glauben und in einer für die

betroffene Person nachvollziehbaren Weise verarbeitet werden“ (DSGVO, 2018). Derzeit kann jedoch mit einer einmaligen Zustimmung eine unbestimmte Anzahl an Zugriffsberechtigungen erteilt werden.

Um zu überprüfen, ob die genannten Prinzipien der Datenschutzgrundverordnung einen Einfluss auf das Verhalten der Applikationen haben, werden folgende Hypothesen aufgestellt:

- Hypothese 1: Nach dem Inkrafttreten der DSGVO wurde die Datenerfassung im Vergleich zum Zeitpunkt davor minimiert, sodass die Anzahl von gefährlichen Berechtigungen reduziert wurde.
- Hypothese 2: Nach dem Inkrafttreten der DSGVO ist die Häufigkeit der Verwendung von Berechtigungen geringer.

Beim Entwickeln einer Applikation ist es von Nöten Berechtigungen zu definieren, die für die Funktion der Applikation erforderlich sind. Basierend auf den Anfragen für die Berechtigungen (Momen et al., 2019) müssen die Nutzenden darüber entscheiden, ob sie sich damit einverstanden erklären. Aus diesem Grund vergleicht diese Studie die Berechtigungserklärungen der Entwickler vor und nach dem Inkrafttreten der DSGVO.

Vorherige Studien haben gezeigt, dass App-Entwickler normalerweise mehr Berechtigungen abverlangen als es für die primäre Funktion der Anwendungen erforderlich ist (Barrera et al., 2010; Hatamian et al., 2017; Kelley et al., 2012; Momen, 2018a).

Die Anzahl der deklarierten Berechtigungen ist im Laufe der Zeit stets gestiegen (Book et al., 2013).

6.5.1.1 Datenaufbereitung

Aus der JSON-Datei wurden anschließend der Name der Applikation, der Name der Ressource, auf die zugegriffen wurde, und der Zeitstempel des Zugriffs in eine MySQL Datenbank übertragen. Anschließend wurden die Datensätze nach der Art des Zugriffs in zehn Kategorien eingeordnet:

- Kalender (CALENDAR - Einsicht in vertrauliche Informationen und Kalendereinträge sowie Hinzufügen und Ändern dieser, Senden von E-Mails an Gäste ohne das Wissen des Veranstalters)

- Anrufprotokoll (CALL_LOG - Anruferliste auslesen und bearbeiten),

- Kamera (CAMERA – Aufnehmen von Fotos und Videos)

- Kontakte (CONTACTS - Einsicht in das Adressbuch und Änderung von Kontakten)

- Standort (LOCATION - Abrufen der ungefähren Position (Sendemasten basierend), der genauen Position (Sendemasten- und GPS-basierend), Zugriff auf den GPS-Sensor)

- Mikrofon (MICROPHONE – Verwenden des Mikrofons sowie Zugriff auf Audioaufnahmen)

- Telefon (PHONE - Tätigen von Anrufen, ausgehende Anrufe umleiten, Ändern des Telefonstatus, Anrufe ohne ihr Mitwirken tätigen)

- SMS (SMS - Erhalten, Lesen, Verändern, Senden von Nachrichten)

- Speicher (STORAGE – Inhalt des USB-Speichers z.B. SD-Karte lesen, löschen oder ändern und externen Speicher formatieren, bereitstellen oder trennen)

- weitere Sensoren (SENSORS – Zugriff auf Wearable-Sensoren wie z.B. Herzfrequenzmessgeräte und Abrufen von Updates über ihre physische Aktivität)

6.5.1.2 Ergebnisse

Bei näherer Betrachtung der gesammelten Berechtigungen von über 50 Applikationen wird bezüglich der gefährlichen Berechtigungen ein Rückgang in 44 Fällen ermittelt. Zur besseren Übersicht der einzelnen Applikationen und deren Zunahme und Abnahme der eingeforderten und benutzten Berechtigungen wurde von Momen et al. (2019) Abbildung 14 erstellt.

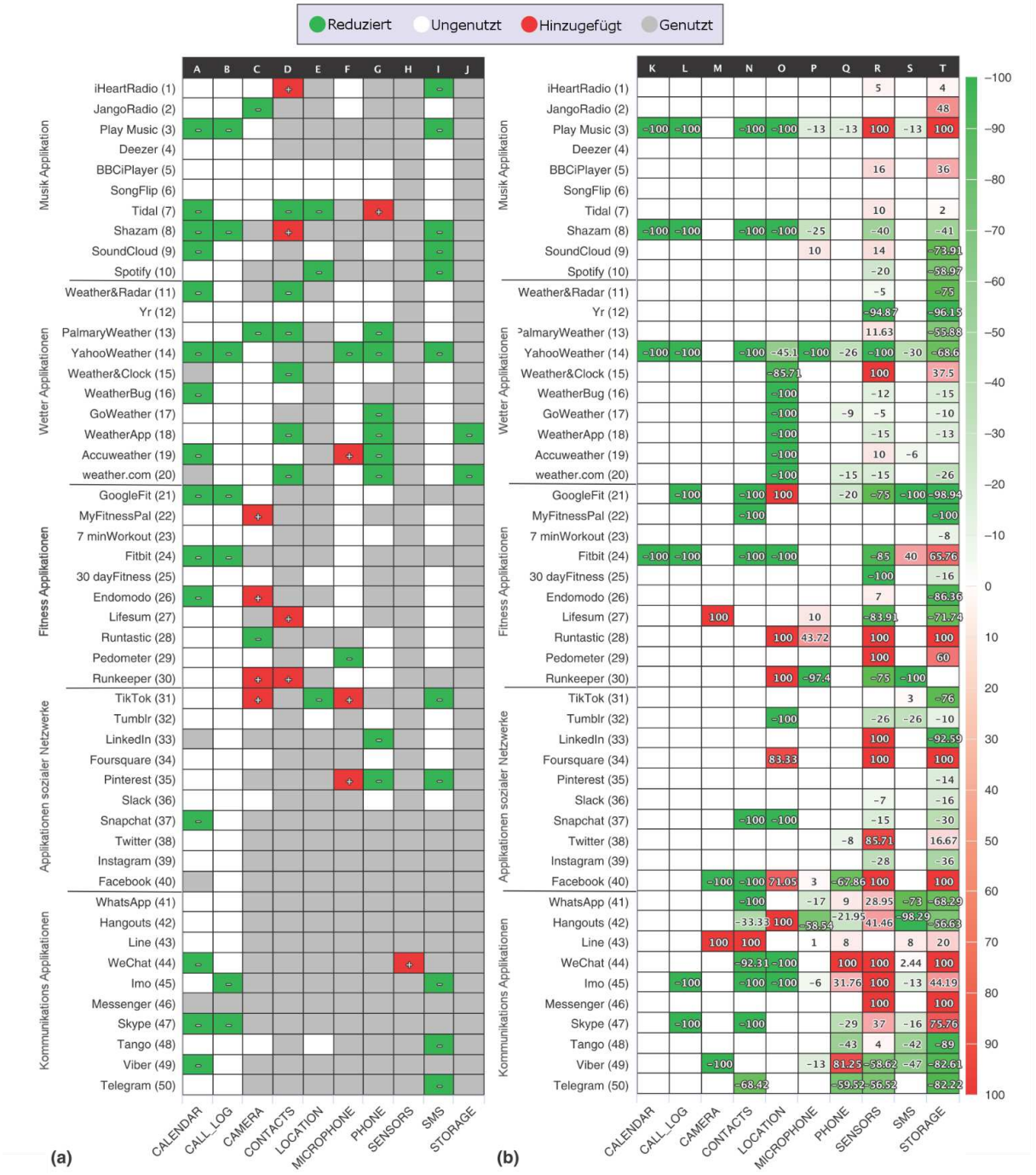


Abbildung 14. Änderung der Berechtigungsanfragen und der Berechtigungsnutzung vor und nach Inkrafttreten der DSGVO (Momen et al., 2019).

Diese Abbildung illustriert den Vergleich der Berechtigungsanfragen und der Nutzung der Berechtigung von den Applikationen vor und nach dem Inkrafttreten der DSGVO.

Der Rückgang der eingeforderten Berechtigungen ist ebenfalls anhand der blauen Balken in Abbildung 15 zu erkennen.

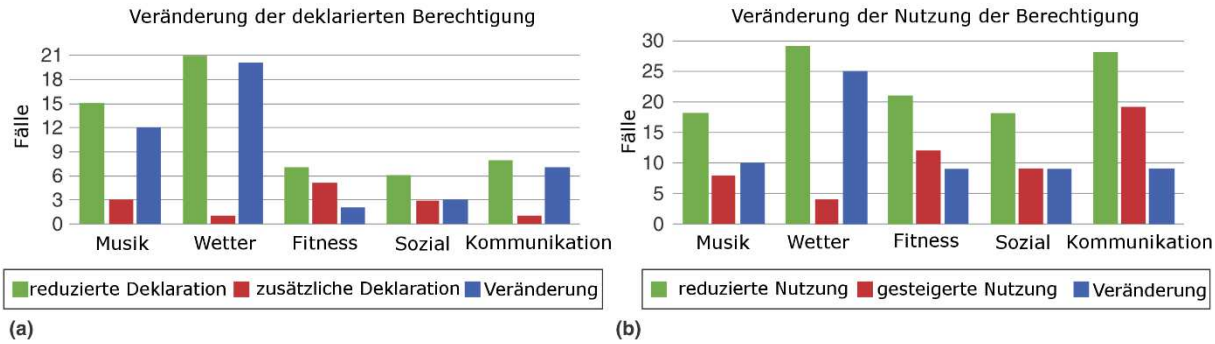


Abbildung 15. Vergleich zwischen den deklarierten und genutzten Berechtigungen vor und nach Inkrafttreten der DSGVO. (Momen et al., 2019).

Diese Abbildung zeigt den Vergleich zwischen den deklarierten und genutzten Berechtigungen vor und nach Inkrafttreten der DSGVO. Die blauen Balken illustrieren das Ausmaß der Reduzierung der (a) deklarierten Berechtigung und (b) der Nutzung der Berechtigung.

Dabei stellt der höchste Balken die größte Abnahme des potenziellen Datenzugriffs dar und kann somit als datenschutzfreundlich angesehen werden. Alle Applikationsgruppen zeigen einen Rückgang der erklärten Berechtigungen nach Implementierung der Datenschutzverordnung. In Abbildung 14 (a) werden die Veränderungen der erklärten Berechtigungen verdeutlicht. Die grünen Kästchen kennzeichnen eine Reduzierung der erklärten Berechtigungen, die roten Kästchen spiegeln eine Steigerung der erklärten Berechtigungen wider, die grauen Kästchen kennzeichnen erklärte Berechtigungen, die weiterhin bestehen, während die weißen Kästchen nicht erklärte Berechtigungen zeigen, bei denen keine Veränderung stattgefunden hat. Hierbei ist zu erkennen, dass besonders die Wetterapplikationen ein weniger aggressives Verhalten aufzeigen, vor allem bei den Berechtigungen PHONE in sechs Fällen, CONTACTS in fünf Fällen sowie CALENDAR in vier Fällen. Dies kann auch anhand der Abbildung 14 (b) bestätigt werden, die veranschaulicht, in welchem Ausmaß auf die Berechtigungen zugegriffen wird. In Abbildung 14 (b) stellen die grünen Schattierungen die Reduzierung der Zugriffe auf die Berechtigungen dar, während die roten Schattierungen die Steigerung der Zugriffe auf die Berechtigungen repräsentieren. Anhand der Stärke der Schattierung lässt sich das Ausmaß der Steigerung und der Reduzierung der Zugriffe erkennen. Zusätzlich wird das Ausmaß in Prozentzahlen je nach Ausprägung in den einzelnen Kästchen festgehalten. Sowohl in Abbildung 14 (a) als auch in Abbildung 14 (b) werden die einzelnen Applikationen nach Kategorie sortiert entlang der Zeilen aufgelistet, während den verschiedenen Berechtigungen jeweils eine Spalte zugeordnet wird. Darüber hinaus ist anhand Abbildung 15 zu erkennen, dass die Musikapplikationen nach den Wetterapplikationen die meisten Veränderungen bezüglich der Datenschutzfreundlichkeit aufzeigen. Auch die Fitnessapplikationen weisen eine höhere Datenschutzleistung als die Applikationen im

Bereich der Kommunikation oder der sozialen Netzwerke auf. Weiterhin zeigen die Ergebnisse der Studie, dass vor allem die Applikationen, welche die Berechtigung CALENDAR, SMS, PHONE, CONTACTS und LOCATION einfordern, ein weniger aggressives Verhalten aufweisen.

Zur Überprüfung der Hypothese 2 wurde die Nutzung der gefährlichen Berechtigung während der Ausführung einiger der meistgenutzten Applikationen in unterschiedlicher Kategorie bezüglich des Zugriffes auf Berechtigungen beobachtet. Dies fand ohne eine Interaktion mit dem Gerät statt. Die Applikationen wurden dabei auf vorkonfigurierte Endgeräte installiert. Eine detaillierte Beschreibung der Konfiguration ist bereits in Abschnitt 5.5.1 enthalten. Die Datensammlung fand dabei in Karlstad im März 2017 und somit vor der Verabschiedung der DSGVO statt. Die zweite Phase fand sowohl in Karlstad als auch in Berlin im Dezember 2018 statt, nachdem die DSGVO in Kraft getreten ist. Die beiden Datensätze werden im weiteren Verlauf dieses Abschnittes verglichen. Hierbei ist zu erwähnen, dass in Berlin zwei Datenerhebungen stattfanden. Eine ohne jegliche Interaktion mit den Geräten, um einen vergleichbaren Datensatz zu erhalten und eine, in der die Geräte an verschiedene Personen ausgehändigt wurden, wobei sie darum gebeten wurden, das Endgerät so alltagsüblich wie möglich zu nutzen.

Bei Betrachtung der Ergebnisse ist zunächst aufgefallen, dass die Applikationen vor dem Inkrafttreten der DSGVO häufig die gefährliche Berechtigung in Anspruch nimmt, während sie im Leerlauf (StandBy) sind, die Applikation also nicht aktiv genutzt wird.

Nach dem Analysieren der gesammelten Log-Dateien kann festgestellt werden, dass viele Applikationen die Nutzung der Zugriffsberechtigung nach der Verabschiedung der DSGVO deutlich reduziert haben, selbst wenn die Berechtigungen weiterhin eingefordert werden. Anhand der Spalten K11 bis T20 in Abbildung 14 ist zu erkennen, dass besonders in der Applikationskategorie des Wetters eine Reduzierung der Nutzung der Zugriffsberechtigung zu verzeichnen ist. Besonders die Applikation YahooWeather (14) zeigt ein deutlich datenschutzfreundlicheres Verhalten als vor dem Inkrafttreten der DSGVO. Ein ähnliches Verhalten ist bei den Wetterapplikationen Weather&Clock (15), WeatherBug (16), GoWeather (17), WeatherApp (18), Accuweather (19) und weather.com (20) zu sehen. Bei den Musikapplikationen kann ebenfalls eine Reduzierung der Nutzung der Zugriffberechtigung beobachtet werden. Hierbei stellt jedoch die Applikation GooglePlay-Music (3) in Spalte K3 bis T3 eine Ausnahme dar, wobei eine Steigerung des Zugriffs auf die Sensoren und den Speicher zu verzeichnen ist, während alle weiteren Zugriffsberechtigungen weniger genutzt werden. Insgesamt ist eine Steigerung der Anzahl der Nutzung der Zugriffsberechtigung in den Kategorien SENSORS, SMS und STORAGE zu verzeichnen, was hauptsächlich an den Applikationen Fitness, Kommunikation und Soziale Netzwerke liegt. In Spalte O ist eine Reduzierung der Anzahl der Nutzung der Zugriffsberechtigung im Bereich der

Positionsdaten (LOCATION) bei den Kategorien Wetter und Musik zu beobachten, während bei den Kategorien Fitness, Soziale Netzwerke und Kommunikation eine Steigerung der Zugriffe zu sehen ist. Die Applikationen Runtastic (28), Pedometer (29), Line (43), WeChat (44) und Imo (45) haben allesamt die Anzahl der Nutzung der Zugriffsberechtigung während des Leerlaufes gesteigert.

Beim Vergleichen der Abbildung 14 (a) mit der Abbildung 14 (b) kann eine Reduzierung der erklärten Berechtigungen als auch die Verwendung der verbleibenden Berechtigungen bezüglich der Applikation YahooWeather (14) verzeichnet werden. Die Applikationen Shazam (8) und GoogleFit (21) reduzierten die Verwendung gefährlicher Berechtigungen, entfernten jedoch nur wenige von ihnen aus den erklärten Berechtigungen. Bezüglich der Applikationen im Bereich der Sozialen Netzwerke und der Kommunikation (Zeile 31-50) ist in den Spalten K bis P eine reduzierte Anzahl der Nutzung der Zugriffsberechtigungen zu sehen, jedoch sind fast alle gefährlichen Berechtigungen weiterhin in den Erklärungen wiederzufinden und stehen somit jederzeit zur Verwendung bereit (Spalten C-J). Obwohl die Berechtigungen CAMERA und CONTACTS die am häufigsten hinzugefügten Berechtigungen nach dem Inkrafttreten der DSGVO sind (Spalten C und D), nahm ihre Verwendung im Leerlauf deutlich ab (Spalten M und N). Sowohl die Zugriffsberechtigungsanfragen als auch die Verwendung von PHONE (Spalten G und Q) und SMS (Spalten I und S) sind im Datensatz nach dem Inkrafttreten der DSGVO deutlich reduziert.

6.5.1.3 Diskussion

Hypothese 1: Nach dem Inkrafttreten der DSGVO wurde die Datenerfassung im Vergleich zum Zeitpunkt davor minimiert, sodass die Anzahl von gefährlichen Berechtigungen reduziert wurde.

Insgesamt kann eine Reduzierung der Berechtigungsnutzung in allen Datensätzen gesehen werden, die nach dem Inkrafttreten der DSGVO erstellt wurden. Darüber hinaus kann eine erheblich reduzierte Anzahl an erklärten Berechtigungen verzeichnet werden. Ferner werden deutlich weniger Berechtigungen während des Leerlaufes der Applikationen genutzt, allerdings ist der Zugriff auf die genutzten Berechtigungen deutlich gestiegen. Somit kann davon ausgegangen werden, dass die Applikationsentwickler dem Prinzip der Datenminimierung nachgekommen sind. Die Verbesserung im Bereich der Datenminimierung hat auch einen direkten Einfluss auf das Prinzip der Zweckbindung, wobei die Entwickler angeben müssen, für welche Funktionen sie die eingeforderten Berechtigungen benötigen. Eine weitere wichtige Beobachtung ist die Steigerung der angeforderten Zugriffberechtigung im Bereich der Sensordaten (CAMERA, MICROPHONE und SENSORS). Eine mögliche Erklärung ist, dass der Zugriff auf andere Berechtigungen (CONTACTS, LOCATION und

MICROPHONE) besonders von dem Status der Sensoren im mobilen Endgerät abhängt. So können beispielsweise Werbeanzeigen geschaltet werden, die sonst nicht erschienen wären, während die Nutzenden auf den Bildschirm schauen. Somit müssten die Applikationen Zugriff auf die Bewegungs- und Beschleunigungssensoren haben, um eine Werbung zu schalten.

Weiterhin fällt auf, dass eine hohe Anzahl von erklärten Berechtigungen, vor allem im Bereich der Kommunikation und Sozialen Netzwerke nicht genutzt werden kann. Dabei ist fraglich, ob diese ungenutzten erteilten Berechtigungen in Zukunft nicht dafür missbraucht werden, um größere Mengen von Daten zu sammeln und weiterzugeben, wie schon Fritsch (2017) gezeigt hat. Ein weiterer Grund für die Reduzierung der erklärten Berechtigungen im Bereich der Wetterapplikationen ist wahrscheinlich den Medien, wie z.B. The Times oder The Wallstreet Journal (Thurm & Kane, 2010), zu verdanken, die immer wieder über das aggressive Verhalten von Wetterapplikationen berichtet und auf die Sammlung und Weitergabe persönlicher Daten an Dritte aufmerksam gemacht haben. Um nicht weiterhin negativ aufzufallen, wurden viele dieser Applikationen verändert. Die Reduzierung der Berechtigungen PHONE (Telefonie) und SMS (Versenden von Textnachrichten) ist damit zu erklären, dass diese Dienste immer weniger Verwendung finden und durch Applikationen ersetzt werden, welche ähnliche Dienste anbieten.

Es kann eine Reduzierung der erklärten Berechtigungen nach dem Inkrafttreten der DSGVO verzeichnet werden, was Hypothese 1 somit bestätigt.

Hypothese 2: Nach dem Inkrafttreten der DSGVO ist die Häufigkeit der Verwendung von Berechtigungen geringer.

Die größte Reduzierung der Verwendung von Berechtigungen kann bei den Wetterapplikationen verzeichnet werden. Applikationen, die sich im Leerlauf befinden, nutzen deutlich weniger Berechtigungen als eingefordert, was Hypothese 2 bestätigt. Darüber hinaus kann ein großes Interesse an Sensordaten, Positionsdaten und Speicherzugriff beobachtet werden. Dennoch ist es vielen Applikationen möglich, auf gefährliche Berechtigungen zuzugreifen. Einige Applikationen wurden überarbeitet, um datenschutzfreundlicher zu werden, während andere nur auf gewisse Berechtigungen zugreifen, sobald mit dem Endgerät interagiert wird.

Das Inkrafttreten der DSGVO führt nicht zwangsweise zu einer Reduzierung der genutzten Berechtigungen, hat jedoch Einfluss auf die Art und Weise der Einholung der Berechtigungen. Der Datenschutz hat sich nach der Einführung der DSGVO somit nur leicht verbessert, sodass die Hypothese 2 nur teilweise bestätigt werden kann.

Die Analyse dieser Daten fand innerhalb der Karlstad Universität in Schweden statt und dauerte leider länger als erwartet, sodass zusammen mit dem Doktorvater Herr Prof. Dr. Rötting die Entscheidung getroffen wurde, die Datenschutzskala ohne das Einfließen dieser Daten in den App-Markt zu implementieren. Der Grund hierfür war die Ungewissheit, wann die entsprechenden Daten vorliegen werden. Darüber hinaus stand im Fokus dieser Studie, den Einfluss der Datenschutzskala auf das Auswahlverhalten im App-Markt zu eruieren. Hierbei wurde diskutiert, ob die Kategorisierung der Applikationen auf echten Daten basieren müsse oder diese fiktiv sein könnten. Nach Abwägen der Vorteile, die das Verwenden von echten Daten mit sich bringt und der Verzögerung, die den Fortschritt der Arbeit auf ungewisse Zeit stoppen würde, wurde sich dafür entschieden, die Kategorisierung der Applikationen randomisiert durchzuführen. Trotzdem wird in dem folgenden Kapitel erläutert, wie der Datenschutzwert errechnet werden würde, wenn die Daten mit einbezogen werden würden.

6.5.2 Berechnung des Privacy-Werts

Die Berechnung des Privacy-Werts wurde von Momen (2018b) erstellt und beruht auf der Häufigkeit der Anforderung der Applikationen auf bestimmte Daten oder Sensoren zuzugreifen. Die Formel, welche für die Berechnung verwendet wird, besteht aus den folgenden Komponenten:

$M = (\delta, \alpha, \rho, d\tau)$ wobei,

δ = begrenzte Menge von Geräten;

α = begrenzte Menge von installierten Applikationen auf dem Gerät;

ρ = begrenzt Menge von angefragten Zugriffsberechtigungen von Applikationen;

$d\tau$ = protokollierte Instanz (Zeitstempel)

Für ein bestimmtes Gerät δ1, eine bestimmte Applikation α1, einem bestimmten Zugriffsrecht ρ und einem bestimmten Zeitraum Δτ = (τ1 – τ2) wird die gesamte Ressourcennutzung einer einzelnen Zugriffsberechtigung (Rρ) berechnet: $R\rho = \int_{\tau=\tau 0}^{\tau=\tau t}(d\tau)$

Anschließend wird das Modell M genutzt, um Daten zu sammeln, die auf eine Anzahl von n Szenarien basieren mit S = s1, s2, … … … sn, wobei sich die Elemente auf boolesche Werte beziehen.

Dabei ist s1 die aktive oder passive Nutzung, welche davon abhängig ist, ob die Nutzenden mit der Applikation interagieren oder nicht. Es ist sehr unwahrscheinlich für die Nutzenden, eine Applikation den gesamten Tag über zu nutzen. Die Applikation verfügt jedoch über Zugriffsberechtigungen, um Daten ohne Einschränkungen dauerhaft abzurufen und zu sammeln.

Die Umgebung s2 ist davon abhängig, ob das mobile Endgerät sich an stark frequentierten Orten befindet oder nicht. Es ist davon auszugehen, dass Applikationen danach streben, bei großen Menschenmassen Gruppierungen zu bilden, um soziale Daten zu analysieren.

Die Bewegungs- und Netzwerkkonnektivität s3 beinhaltet die stationäre oder mobile Nutzung.

Weitere Szenarien können nach Bedarf definiert und festgelegt werden. Je nach Gebrauch der Zugriffsberechtigungen wird ein PIF-Wert errechnet, welcher es ermöglicht, die Priorisierung individuell zu gestallten. Der individuelle Priorisierungsfaktor wird wie folgt berechnet:

$$PIF = p_1 * s_1 + p_2 * s_2 \ldots + p_m * s_m$$

Wenn eine Anzahl m von PIFs vorliegt, die mit den entsprechenden Szenarien verbunden sind, wird für eine bestimmte Applikation α mit der Berechtigung ρ, die auf dem mobilen Endgerät δ für einen bestimmten Zeitraum Δτ = (τt −τ0) läuft, ein Risikowert (RSα) wie folgt definiert:

$$RS_{\alpha} = \sum_{i=0}^{m} R_{\rho i} \cdot PIF_{\rho i} \pm E = \sum_{i=0}^{m} R_{\rho i} \left(\sum_{j=0}^{n} p_j s_j \right) \pm E$$

6.5.3 Entwurf der Skalen

Um den Aufwand der Endnutzenden mobiler Endgeräte bei der Auswahl der adäquaten Applikation möglichst gering zu halten, sollten die Skalen eine hohe Intuitivität mit sich bringen. Darüber hinaus stellt die Farbe ein kritisches Attribut für eine akkurate Identifikation dar, während weitere Attribute wie zum Beispiel Größe, Helligkeit und Form dann variieren können, ohne die Identifikation zu beeinträchtigen (Born, 2001; Christ, 1975). Deshalb wurde sich dazu entschlossen, eine farbkodierte Skala zu verwenden. Nach Cimbalo et al. (1978), welche eine Studie mit Kindern und Studenten in Bezug auf emotional-gefärbte Bilder und Farbauswahl durchführten, werden grün stets fröhliche und somit positive Emotionen zugeschrieben, während rot eher mit traurigen und negativen Emotionen behaftet ist. Darüber hinaus haben Benbasat et al. (1986) eine Studie durchgeführt, in der Information als verständlicher und besser in Bezug auf Entscheidungsfindung eingeordnet wurde, sobald diese mehrfarbig dargestellt wurde, im Vergleich zur einfarbigen Darstellung. Dies führte zu einer Unterteilung der Skala in fünf verschiedene Farbabschnitte von dunkelgrün über hellgrün, gelb und orange bis rot. Es wurde zudem eine Skala gewählt, die einen geringen kognitiven Aufwand zum Verständnis bedarf, sodass die dargebotenen Informationen bei der Entscheidungsfindung besser

aufgenommen werden können. Dazu tragen die visuellen Hinweisreize, in diesem Fall die farbkodierten Symbole der einzelnen Skalen, bei (Hibbard & Peters, 2003).

6.5.4 Vorstudie zur Bestimmung einer adäquaten Illustrierung

Der Vortest diente dazu zu überprüfen, welches Skalen-Design am besten die Aggressivität und somit die Schwere des Eingriffs in die Privatsphäre illustriert. Darüber hinaus wurden noch weitere allgemeine Informationen wie beispielsweise Geschlecht und Alter erfasst. Weiterhin wurde der tägliche Gebrauch des mobilen Endgerätes in Stunden und die Art von Maßnahmen die persönlichen Daten zu schützen abgefragt. Die letzte Frage zu den demografischen Informationen bezog sich auf den höchsten Bildungsgrad der Teilnehmenden. Der Fragebogen zur Vorstudie ist im Anhang P zu finden. Im Applikationsraster des App-Marktes befand sich die Datenschutzskala stets in der unteren rechten Ecke in jedem Applikationsfenster.

Nachdem sich für eine farbkodierte Skala entschieden wurde, galt es, die richtige Form der Skala ausfindig zu machen. Eine ausgiebige Literaturrecherche ergab keine weiterführenden Hinweise zu einer optimierten Skala. Aus diesem Grund wurde in Absprache mit dem Doktorvater über Skalen diskutiert, die auch im Alltag wiederzufinden sind und die den Nutzenden bereits bekannt sind.

Zunächst wurde sich darauf geeinigt, eine fünfstufige Skala zu verwenden, um die kognitive Begrenzung der menschlichen Informationsverarbeitung bezüglich der Kanalkapazitäten zu berücksichtigen. In einer Studie von Miller (1956) kann belegt werden, dass das Kurzzeitgedächtnis eines Menschen 7 ± 2 Einheiten (Chunks) verfügbar halten kann. Diese Fähigkeit ist genetisch bedingt und kann mit einzelnen Ausnahmen nicht durch Übung (Training) gesteigert werden. Ferner wurde sich dafür entschieden, die untere Grenze der im Kurzzeitgedächtnis speicherbaren Einheiten zu wählen, sodass ein Großteil der Endnutzenden die Skala mit nur geringem kognitivem Aufwand verwenden kann. Zudem wurde eine ungeradzahlige Skala eingesetzt, um es zu ermöglichen, die Applikationen neben sicher und kritisch auch als moderat kennzeichnen zu können.

Die erste Skala (Bubble-Scale) bestand aus einem Kreis, der mit einem 3D-Effekt versehen wurde, um ein modernes Erscheinungsbild zu generieren und ähnelte den Leuchtsignalen einer Ampel. Je nach Aggressivität der Applikation änderte sich die Farbe des Kreises innerhalb der oben genannten Farbabschnitte (Abbildung 28 im Anhang O). Die zweite Skala (Smiley-Scale) entsprach der ersten Skala, war jedoch zusätzlich noch mit einem entsprechenden Gesichtsausdruck versehen. Diese Skala ist auch für die Bewertung der Kundenzufriedenheit im Einzelhandel wiederzufinden. Die Farbabstufungen blieben hierbei dieselben (Abbildung 29 im Anhang O). Die dritte Skala (Label-Scale) enthielt dieselbe

Farbkodierung wie die Vorherigen, wurde jedoch zusätzlich mit einem kategorisierenden Schriftzug versehen. Eine solche Kennzeichnung ist auch im Warentest wiederzufinden. Um den Schriftzug passend illustrieren zu können, wurde der Kreis durch einen Balken ersetzt (Abbildung 30 im Anhang O). Die vierte Skala (Arrow-Bar-Scale) ist eine vertikale Säule, deren Farbverlauf von Rot unten bis Grün oben die Aggressivität der Applikation widerspiegeln sollte. Die Skala ist einem Thermometer nachempfunden. Als Indikatoren dienen zwei Pfeile links und rechts der Säule (Abbildung 31 im Anhang O). Die fünfte Skala (Arrow-Speedometer-Scale) ähnelt einem Tachometer und stellt den Farbverlauf in einem horizontalen Halbkreis, von links grün bis rechts rot, dar. Die Stellung eines Pfeils in der Mitte zeigt die App-Aggressivität an (Abbildung 32 im Anhang O). Zusätzlich wurde in einer späteren Version des Fragebogens eine sechste und siebte Skala implementiert. Die sechste Skala besteht aus einem farblich kodierten Schild, auf dem ein schwarzes Bügelschloss abgebildet ist (s. Abbildung 33, Anhang O). Die siebte Skala besteht aus einem Kreis, auf dem eine schwarze Augenmaske abgebildet ist (s. Abbildung 34, Anhang O).

Die fünf bzw. sieben Skalen wurden in einem App-Markt implementiert und dieser als Bilddatei in einem Onlinefragebogen eingebettet (Abbildung 35 im Anhang O). Die Teilnehmenden wurden gebeten, die Ablesbarkeit der Information, die Unterscheidbarkeit der Farben, das Erscheinungsbild (Angemessenheit der Größe und Farbe), das Verstehen der dargebotenen Information und die Mehrdeutigkeit auf einer Likert-Skala von eins bis zehn zu bewerten. Die Ablesbarkeit ist nach Tekfi (1987) definiert als die Summe (Interaktionen inkludiert) aller Elemente eines gegebenen gedruckten Materials, welches den Erfolg beeinflusst, den die Leser mit diesem haben. Der Erfolg ist dabei bedingt durch das Verstehen, die optimale Geschwindigkeit des Lesens und das Interesse am Gelesenen.

6.5.4.1 Datenaufbereitung

Die Antworten des Fragebogens, welcher mit dem Portal LimeSurvey erstellt wurde, konnten anschließend in Form einer Excel-Tabelle heruntergeladen und zur statistischen Analyse in dem Programm SPSS importiert werden. Die meisten der Antworten wurden umcodiert, sodass eine statistische Analyse durchführbar war. Beispielsweise wurden bei dem Geschlecht „männlich“ und „weiblich“ durch eine „1“ und eine „2“ ersetzt. Dasselbe Prinzip wurde für die dritte Frage zur Erfassung der Zeit, welche die Teilnehmenden mit dem Nutzen des mobilen Endgerätes verbringen, und für die fünfte Frage, welche erfassen sollte, ob und was die Teilnehmenden unternommen haben, um ihre persönlichen Daten zu schützen, verwendet. Auch die sechste Frage, welche den höchsten Bildungsgrad erfassen sollte, wurde mit Zahlen kategorisiert. Problematisch wurde es bei der Auswertung der Bewertung der Datenschutzskalen, weil der Datensatz so aufgebaut war, dass jeweils

eine Zeile einer Versuchsperson entsprach und die Spalten die einzelnen Kategorien der Bewertungen (Größe, Ablesbarkeit, Verständnis, Farbe, Unterscheidbarkeit, Eindeutigkeit) der jeweils einzelnen Skalen (Bubble Scale, Arrow-Scale-Bar, Arrow-Scale-Meter, Label-Meter, Smiley-Meter, Bügelschloss, Augenmaske) aufzeigten. Problematisch bei dieser Anordnung der Ergebnisse war die fehlende Gruppenvariable, um die verschiedenen Bewertungen der fünf Datenschutzskalen untereinander auf signifikante Unterschiede zu vergleichen. Hierfür musste ein neues Excel-Dokument erstellt werden, indem die Bewertungen aller Skalen untereinander in einer Spalte aufgelistet wurden. Die Kategorien wurden gleich gewichtet und die Rohdaten somit für die statistische Auswertung zu einem Mittelwert der Bewertungen pro Skala zusammengefasst. Anschließend wurde die Tabelle wiederum in SPSS eingefügt, um explorative Analysen durchführen zu können.

6.5.4.2 Ergebnisse

Im Folgenden werden die Ergebnisse im Hinblick auf die Auswahl der adäquatesten Illustration der Skalen aufgezeigt. Dabei wird zunächst ein deskriptiver Überblick der Ergebnisse aufgezeigt, um diese anschließend auf ihre Signifikanz zu überprüfen.

Der erste Fragebogen war ab Ende August bis Ende Dezember freigeschaltet. Während dieser Zeit haben insgesamt 55 Personen an der Umfrage teilgenommen. Lediglich 28 Personen haben den Fragebogen mit den fünf Skalen vollständig ausgefüllt, sodass nur mit den entsprechenden Datensätzen gearbeitet werden kann. Aus 28 Personen, die Bewertungen in den sechs Kategorien abgegeben haben, ergeben sich N = 168 Bewertungen pro Skala.

Die deskriptive Auswertung ergibt bei einer Spannweite von eins bis zehn folgende Mittelwerte (SD) in absteigender Reihenfolge: Label-Meter M = 8,25 (2,28), Arrow-Scale-Meter M = 7,80 (2,50), Smiley-Meter M = 7,64 (2,51), Bubble-Scale M = 7,02 (2,68) und Arrow-Scale-Bar M = 6,64 (2,66).

Die Datensätze jeder Skala werden anschließend mit Hilfe des Kolmogorov-Smirnov-Tests (Lilliefors, 1967) auf Normalverteilung getestet. Dieser ist für alle Skalen signifikant (p < .000), sodass keine Normalverteilung vorzufinden ist. Darüber hinaus ist die Bewertung der verschiedenen Skalen von den gleichen Personen vorgenommen worden. Die Bewertungen aller Skalen sind daher als verbundene Stichprobe zu betrachten. Aus diesen Gründen wurde sich dazu entschlossen den nicht-parametrischen Friedman-Test (Conover & Iman, 1981) durchzuführen, welcher die Mediane der Bewertungen der Skalen untereinander auf signifikante Unterschiede testet. Dieser ergibt einen signifikanten Unterschied (χ^2 = 80,47; p < .000) (s. Tabelle 32, Anhang Y).

Die Datenerhebung der zweiten Umfrage mit sieben Skalen erstreckte sich über den Zeitraum von Ende Februar bis Ende Mai 2019. Diese Umfrage haben 22 Personen in den sechs Kategorien vollständig ausgefüllt, woraus sich $N = 132$ Bewertungen pro Skala zusammensetzen.

Die deskriptive Auswertung ergibt bei einer Spannweite von 1 bis 10 folgende Mittelwerte (SD) in absteigender Reihenfolge: Smiley-Meter $M = 7{,}70$ (2,70), Label-Meter $M = 7{,}58$ (2,81), Arrow-Scale-Meter $M = 7{,}27$ (2,70), Lock Emblem $M = 7{,}02$ (2,65), Bubble Scale $M = 6{,}97$ (2,94), Arrow-Scale-Bar $M = 6{,}39$ (2,30) und Mask Emblem $M = 6{,}05$ (3,00).

Die Mittelwerte der Bewertungen werden anschließend mit Hilfe des Kolmogorov-Smirnov-Tests auf Normalverteilung getestet. Dieser ist für alle Skalen signifikant ($p < .000$), sodass nicht von einer Normalverteilung ausgegangen werden kann. Aus denselben Gründen, die bereits bei der Auswertung der Umfrage mit fünf Skalen angeführt wurden, kommt der nicht-parametrische Friedman-Test ein weiteres Mal zur Anwendung. Dieser ergibt einen signifikanten Unterschied ($\chi^2 = 54{,}35$; $p < .000$) (s. Tabelle 33, Anhang Y).

6.5.4.3 Diskussion

Anhand der Mittelwerte der ersten Umfrage kann eine Favorisierung der Label Scale erkannt werden. In der zweiten Umfrage erzielt die Label Scale die zweithöchste Bewertung auf der Skala von 1 bis 10. Der Friedman-Test ergibt einen signifikanten Unterschied zwischen den Bewertungen der einzelnen Skalen, sodass eine Entscheidung zugunsten der Label Scale getroffen wird. Begründungen für die Bewertungen werden im Rahmen der Studie nicht erfasst. Es besteht jedoch Grund zur Annahme, dass die Label Skala mit geringerem kognitivem Aufwand interpretiert werden kann als die anderen Skalen und daher besser bewertet wird.

6.5.5 Erstellung des App-Marktes

Die aus den Ergebnissen der Vorstudie resultierende Skala, die Label-Scale (Schild), wurde mit Hilfe des Programms Axure RP Team Edition 8.0.0.3308 in eine App-Markt-ähnliche Umgebung implementiert. Das Design des App-Marktes wurde an den Playstore von Google angelehnt. Hierfür wurde ein Screenshot des Google Playstores erstellt und dieser mit dem Bildbearbeitungsprogramm GIMP Version 2.8.14 von Spencer Kimball, Peter Mattis und dem GIMP-Entwicklerteam so zusammengefügt, dass die Applikationen aus Tabelle 31 im Anhang Y entsprechend auf einer Seite mit einer entsprechenden Kategorie stehen. Somit wurden zunächst acht zusammengefügte Screenshots in den

Prototypen implementiert und als Hintergrund gesetzt. Dabei wurden allerdings alle Bewertungen und Preise entfernt, um die Anzahl an Störvariablen zu minimieren. Anschließend wurde über den aufgelisteten Applikationen ein unsichtbares Rechteck gelegt, welches mit dem Link der entsprechenden Applikation auf den Google Playstore versehen wurde. Der Startbildschirm wurde mit der gewohnten Eingabeleiste zur Suche von Applikationen versehen. Die Suchleiste wurde so programmiert, dass bei der Eingabe eines entsprechenden Begriffs, wie z.B. „Messenger“ oder der Name einer Applikation wie z.B. „WhatsApp“, eine Weiterleitung auf eine Seite mit den entsprechenden Applikationen erfolgte. Zusätzlich waren in der Suchleiste Vorschläge einprogrammiert, die bei entsprechender Eingabe von Buchstaben bzw. Buchstabenfolgen unter der Suchleiste erschienen. In der rechten unteren Ecke jedes Applikationsfensters wurde die zugehörige Label-Scale eingefügt. Die Labels wurden den Applikationen zufällig von rot (sehr unsicher) bis grün (sehr sicher) zugewiesen (Abbildung 16).

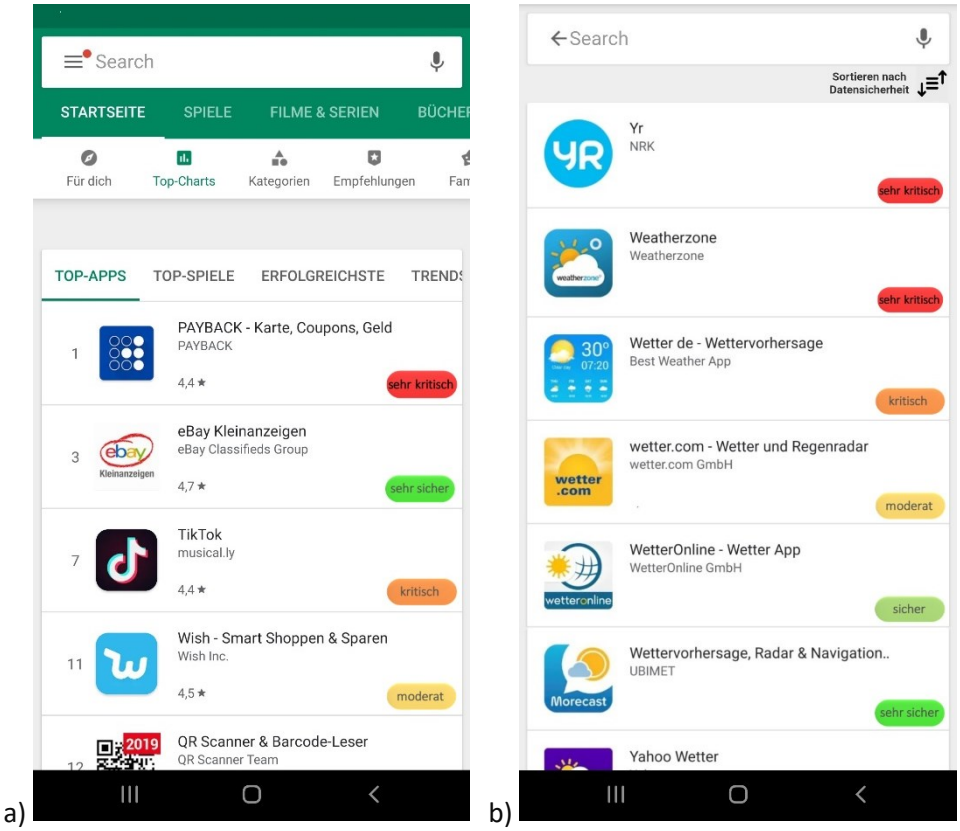


Abbildung 16. a) Startbildschirm des prototypisierten App-Marktes mit Datenschutzskala und b) Auflistung der Applikationen nach der Suche.

Diese Abbildung zeigt einen Bildschirmabzug des prototypisierten App-Marktes. Dabei wird in Abbildung 16 a) der Startbildschirm dargestellt, wie die Teilnehmenden das mobile Endgerät zu Beginn des Versuches vorgefunden haben, während Abbildung 16 b) die Auflistung nach der Suche von Applikationen des Szenarios Wetter abbildet.

Die entsprechenden Symbole der Lable-Scale wurden mit einer weiteren Seite verknüpft, welche genaue Informationen über ihre Funktionsweise enthielt. Je nach Stichprobe hatten die Nutzenden die Möglichkeit, sich durch das Tippen auf die Skala näher über diese zu informieren (s. Abbildung 36 Anhang Q).

Durch Tippen auf das Applikationsfenster selbst erfolgte eine Weiterleitung zur möglichen Installation der Applikation. Darüber hinaus befand sich direkt unter der Suchleiste eine Schaltfläche, die beim Betätigen dieser die Applikation nach der Datenschutzfreundlichkeit sortierte. Um diese Sortierung zu erlangen, musste der oben erwähnte Screenshot mittels des Bildbearbeitungsprogrammes erneut auseinandergeschnitten und in richtiger Reihenfolge zusammengesetzt werden.

6.5.6 Stichprobenumfangsberechnung

Zur Bestimmung des Stichprobenumfangs, der nötig wäre, um ein signifikantes Ergebnis zu erzielen, wird eine Power-Analyse mit Hilfe des Programmes G*Power Version 3.1.9.2 von Axel Buchner, Edgar Erdfelder, Franz Faul und Albert-Georg Lang durchgeführt. Eine Apriori-Analyse wird berechnet, eine Effektstärke von d = 0.8 annehmend, die zur Berechnung des Stichprobenumfangs verwendet wird. Die Analyse ergibt mit einem Alpha-Fehler von 0,05 und einer Power (1 – Beta-Fehler Wahrscheinlichkeit) von 0,8 einen notwendigen Stichprobenumfang von N = 21 pro Gruppe.

6.5.7 Auswahl der Teilnehmenden

In diesem Versuch wurden die Teilnehmenden für das Experiment ebenfalls über das Online-Probandenportal „Prometei“ der Technischen Universität Berlin akquiriert. Aufgrund der eben aufgeführten Stichprobenumfangsberechnung wurde eine Mindestteilnehmeranzahl von N = 84 festgelegt (21 Teilnehmende in jeweils vier Gruppen), um eine valide Aussage der Ergebnisse zu erreichen. Auch hier wurde versucht, eine möglichst heterogene Stichprobe für den Versuch zu akquirieren, sodass sich die demographischen Eigenschaften ausgleichen und in Summe keinen Effekt auf die Ergebnisse haben.

Den Teilnehmenden wurde im Online-Portal eine finanzielle Gegenleistung in einer Höhe von 10 Euro oder einer Versuchspersonenstunde für die Teilnahme angeboten. Sie konnten sich in dem Zeitraum vom 23.07.2019 bis 10.09.2019 für einen Termin werktags zwischen 10:00 und 17:00 Uhr eintragen.

6.6 Aufbau

Im folgenden Kapitel wird der Versuchsaufbau und -ablauf im Detail geschildert. Der Abschnitt ist in acht verschiedene Schritte unterteilt. Zunächst werden die Einleitung und die Einverständniserklärung beschrieben, welche in unterschiedlichen Formen an die verschiedenen Stichproben ausgehändigt wurde. Anschließend wird der Aufbau des Fragebogens zu den bereits auf den Endgeräten der Teilnehmenden installierten Applikationen geschildert und die Durchführung des Experiments beschrieben. Weiterhin wird veranschaulicht, wie die Aufklärung der Studie entworfen wurde und die Videokonfrontation mit dem Fragebogenteil zur Applikationsauswahl aufgebaut war. Ferner wird erläutert, wie die Teilnehmenden die Datenschutzskala bewerten konnten und auf welche Art und Weise der Fragebogen zu den Bedenken der Internetnutzenden im Bereich der mobilen Endgeräte (MUIPC) entworfen und aus dem Englischen übersetzt wurde.

6.6.1 Einleitung und Einverständniserklärung

Zu Beginn wurde den Teilnehmenden der Ablauf der Untersuchung nähergebracht. Darüber hinaus umfasste die Einleitung in die Studie auch die Einverständniserklärung in diese (s. Anhang R). Wie auch schon im vorherigen Versuch wurden die Teilnehmenden bezüglich des Ziels der Studie getäuscht. Ihnen wurde vermittelt, dass die Studie durchgeführt werde, um die Benutzerfreundlichkeit von und den Umgang mit einem App-Markt zu untersuchen. In der Einleitung wurde bei der Gruppe B (mit Datenschutzskala ohne Beschreibung) und der Gruppe C (ohne Datenschutzskala und ohne Beschreibung) nicht weiter auf die Datenschutzskala eingegangen. Lediglich der Stichprobe der Gruppe A (mit Datenschutzskala und Beschreibung) wurde die Funktion und der Hintergrund der Datenschutzskala im Detail erläutert. Hierbei sollen die drei Stichproben unterschiedliche Situationen im Alltag simulieren. Die Gruppe A sollte den Umgang der Datenschutzskala in einer Situation untersuchen, bei der sich die Skala schon etabliert hat und die Allgemeinheit über Funktion, Umgang und Hintergrund der Illustrierung informiert ist. Die Gruppe B simulierte die Situation der Einführung der Skala in einen App-Markt. Dabei wurden die Nutzenden mit der Datenschutzskala konfrontiert, ohne eine vorherige detaillierte Beschreibung dieser zu erhalten. Hierbei sollte besonders darauf geachtet werden, wie und in welchem Umfang die Nutzenden sich eigenständig über die Skala informieren, ob sie ein adäquates Verständnis über diese erlangen und ob sie dieses Verständnis bei der Auswahl der Applikation angemessen anwenden können. Die Gruppe C stellte die Kontrollgruppe dar und diente dazu, Veränderungen beim Auswahlverhalten bedingt durch die Datenschutzskala herauszustellen.

Zur Anonymisierung generierten die Teilnehmenden einen persönlichen Code nach einer standardisierten Anleitung (s. Anhang S), die von der Ethikkommission des Institutes für Psychologie und Arbeitswissenschaften vorgegeben wurde. Der Code setzt sich aus fünf Ziffern, dem ersten Buchstaben des Vornamens der Mutter, dem ersten Buchstaben des Vornamens des Vaters, des ersten Buchstaben des eigenen Geburtsortes, der letzten Ziffer des eigenen Geburtsjahres und der letzten Ziffer des eigenen Geburtstages, zusammen.

In der Einverständniserklärung wurden sie darüber hinaus gebeten, sich vorzustellen, dass das für die Studie bereitgestellte Endgerät ihr eigenes wäre und sowohl für private als auch für geschäftliche Zwecke verwendet werde. Den Teilnehmenden wurde darüber hinaus vermittelt, dass die Studie 60 Minuten lang dauere, diese mit 10 Euro vergütet werde und jederzeit ohne Nennung von Gründen abgebrochen werden könne. Weiterhin wurde darüber informiert, dass die gesammelten Daten für die Studie herangezogen werden und aus rechtlichen Gründen zehn Jahre aufbewahrt werden. Die Tonaufnahmen wurden nach erfolgreicher Transkription gelöscht. Darüber hinaus erfolgte eine separate Einwilligung zur Verarbeitung der Ton- und Videoaufnahmen, die von der Ethikkommission vorgegeben wurde (s. Anhang T). Ferner wurde darüber informiert, dass die Daten anonymisiert werden und in einem Zeitraum von zwei Wochen die Löschung beantragt werden könne. Eine Kopie der Einverständniserklärung mit enthaltener Einführung in das Experiment ist im Anhang R zu finden.

6.6.2 Bereits installierte Applikationen

Um der in Abschnitt 6.4 beschriebenen Störvariable bzw. Kontrollvariable der Voreingenommenheit entgegenzuwirken, bzw. diese in der Auswertung zu berücksichtigen, wurde den Teilnehmenden eine Liste von Applikationen vorgelegt, die in der Studie verwendet wurden. Dabei wurden sie gebeten anzugeben, ob sie die Applikation auf ihrem privaten mobilen Endgerät

- installiert und bereits verwendet,
- bereits verwendet, derzeit jedoch nicht installiert,
- nicht installiert und noch nicht verwendet oder
- installiert und noch nicht verwendet haben.

Der Fragebogen wurde mit Hilfe des LimeSurvey-Portals erstellt und von den Teilnehmenden auf einem zur Verfügung gestellten internetfähigen Endgerät beantwortet. Ein druckbares Exemplar des Fragebogens befindet sich im Anhang U Teil B.

6.6.3 Experiment zur Auswahl geeigneter Applikationen mit Eye-Tracking

Nachdem die Teilnehmenden Teil B des Fragebogens im Anhang U am Endgerät erfolgreich ausgefüllt haben, wurden sie mit Hilfe des *Head-mounted*- Eye-Trackers – Eye tracking glasses von SensoMotoric Instruments (SMI) ausgestattet. Dieser verfügte über eine maximale Abtastrate von 120 HZ, wobei in diesem Experiment eine Abtastrate von 60 Hz gewählt wurde, weil die Teilnehmenden die Aufgaben in einer sitzenden Position absolviert haben. Höhere Herzraten sind bei schnellen Bewegungen zu empfehlen, die jedoch in diesem Experiment nicht enthalten waren. Der Eye-Tracker musste zunächst kalibriert werden, indem die Teilnehmenden drei verschiedene vorgegebene Punkte fokussierten und diese im Eye-Tracking Computer bestätigt wurden. Zur Simulation des alltäglichen Gebrauchs eines mobilen Endgerätes, in diesem Fall eines Smartphones, wurden den Teilnehmenden acht Szenarien präsentiert, in welche sie sich hineinversetzen und eine dazu passende Applikation aus dem App-Markt auswählen, herunterladen und verwenden sollten. Die acht Szenarien sollten alltagsübliche Aufgaben simulieren, welche die Teilnehmenden mit Hilfe des Herunterladens und der Installation der entsprechenden Applikation bewältigen sollten. Die Szenarien beinhalteten das Schreiben einer Nachricht (Messenger), das Führen einer Videokonferenz, das Einsehen einer Wettervorhersage, das Verfassen einer E-Mail, das Abspielen eines Liedes, das Aufzeichnen der körperlichen Aktivitäten, das Lösen eines Logikrätsels und das Einsehen von Nachrichten (News). Die genaue Formulierung der Szenarien befindet sich im Anhang V. Um einen Reihenfolgeneffekt zu vermeiden, wurden bei jeder Gruppe jeweils zwei unterschiedliche Reihenfolgen der Szenarien verwendet. Die erste Reihenfolge wurde wie folgt gewählt: 1. Messenger, 2. Videokonferenz, 3. Wetter, 4. E-Mail, 5. Musik, 6. Fitness, 7. Spiele und 8. Nachrichten, wie sie auch im Anhang V wiederzufinden ist. Die zweite Reihenfolge lautet wie folgt: 1. Wetter, 2. Nachrichten, 3. Spiele, 4. Messenger, 5. Fitness, 6. E-Mail, 7. Musik und 8. Videokonferenz.

Für die acht dargebotenen Szenarien standen den Teilnehmenden jeweils zehn Applikationen zur Verfügung, welche in Tabelle 31 im Anhang Y, nach Kategorien sortiert, aufgelistet sind. Während der Bearbeitung der acht Aufgaben, wurden die Blickbewegungen der Teilnehmenden aufgezeichnet, um diese unter anderem als Hilfe zur Ergründung des Auswahlverhaltens nutzen zu können. Die Teilnehmenden wurden zu einem späteren Zeitpunkt gebeten, ihre eigene Blickbewegung auf dem Eye-Tracking-Video zu begutachten und ihre Gedanken zu dem entsprechenden Zeitpunkt laut wiederzugeben.

6.6.4 Aufklärung über das Ziel der Studie

Nachdem die Teilnehmenden die acht Aufgaben erfolgreich durchgeführt haben, wurde ihnen der Eye-Tracker abgenommen und sie wurden über die drei Stichproben und den damit zusammenhängenden unterschiedlichen Versuchsbedingungen aufgeklärt. Weiterhin wurden sie darüber informiert, dass das Ziel der Studie die Untersuchung der zugrundeliegenden Prozesse bei der Auswahl von Applikationen war und weiterhin geprüft werden sollte, ob diese Prozesse durch die Illustrierung weiterer Informationen zu sensibilisieren sind, um den Nutzenden eine adäquate Entscheidung zu ermöglichen, welche den Schutz der Privatsphäre miteinbezieht. Die Aufklärung erfolgte mündlich. Der genaue Wortlaut ist im Anhang W ersichtlich.

6.6.5 Videokonfrontation mit Fragebogenteil zur Applikationsauswahl

Nachdem die Teilnehmenden über das eigentliche Ziel der Studie aufgeklärt worden waren, wurde eine Videokonfrontation mit den einzelnen Teilnehmenden durchgeführt, um ein tiefergehendes Verständnis über die Grundlage der jeweiligen Auswahlentscheidung zu erlangen. Die Videokonfrontation mit jeweils anschließender Befragung nach Vertrauenswürdigkeit der gewählten Applikation und Einfachheit der Auswahlentscheidung erfolgte im Anschluss an die Bearbeitung aller Szenarien, um Unterbrechungen während der Durchführung zu vermeiden. Zu Beginn der Videokonfrontation erfolgte eine kurze Aufklärung, welche die Teilnehmenden darüber informierte, dass lediglich der Auswahlprozess der Applikationen für die Untersuchung relevant war. Den Teilnehmenden wurde zu jeder Auswahlentscheidung ihr Video vorgespielt, welches vorher mit Hilfe des Eye-Trackers bei der Entscheidungsfindung aufgenommen worden war. Dies sollte den Teilnehmenden den nachträglichen Zugang zu ihren Entscheidungsgründen vereinfachen. Bei der Konfrontation in Form eines Interviews wurden die Teilnehmenden nach den Beweggründen ihrer Entscheidung befragt. Sie wurden dazu aufgefordert, ihre Gedankengänge beim Auswahlprozess während des Abspielens des Eye-Tracking-Videos laut zu wiederholen und diese zu begründen. Das Gespräch wurde mit Hilfe eines Diktiergerätes aufgenommen. Zu jedem Szenario sollten die Teilnehmenden Teil C des Fragebogens im Anhang U ausfüllen. Hierbei wurden sie gebeten, zu zwei Aussagen, das Ausmaß an Zustimmung betreffend, Vertrauenswürdigkeit in die entsprechende Applikation und die Einfachheit der Auswahlentscheidung auf einer 7-stufigen Likert-Skala mit den Polen „trifft zu“ bis „trifft überhaupt nicht zu“ anzugeben.

6.6.6 Bewertung der Datenschutzskala

Im Anschluss an die Videokonfrontation wurden die Teilnehmenden der Gruppe (A) und der Gruppe (B) gebeten, den Teil D des Fragebogens im Anhang U zur Bewertung der Datenschutzskala auszufüllen. Hierbei wurden die Teilnehmenden gebeten, die Datenschutzskala in Hinblick auf ihre Intuitivität, Gültigkeit, Zuverlässigkeit, Auswirkungen, Verworrenheit, Komplexität, Vertrauenswürdigkeit und Informativität auf einer siebenstufigen Likert-Skala mit den in Abschnitt 6.6.5 genannten Polen zu bewerten. Ferner sollten sie mit derselben Skala evaluieren, ob die bereit gestellten Informationen der Datenschutzskala für die Nutzenden ausreichend sind, ob die Datenschutzskala das Gefühl des Schutzes der Privatsphäre erhöht und ob sie sich selbst eine Datenschutzskala im App-Markt wünschen würden. Darüber hinaus sollten sie angeben, ob sie bei der Option der Anzeige einer Datenschutzskala diese aktivieren würden. Die letzte Frage beinhaltete ein Textfeld, in dem die Teilnehmenden Verbesserungsvorschläge bezüglich der Datenschutzskala niederschreiben konnten.

6.6.7 Bedenken der Nutzenden im Bereich der mobilen Endgeräte (MUIPC)

Die Teilnehmenden wurden gebeten einen Fragebogen zu den Bedenken im Bereich der mobilen Endgeräte (siehe Abschnitt 2.2.11) auszufüllen. Der Fragebogen ist angelehnt an den MUIPC Fragebogen von Xu et al., welcher auf Englisch verfasst ist, jedoch für diese Studie in die deutsche Sprache übersetzt wurde. Darüber hinaus wurden Fragen abgeändert und entfernt, um den Fragebogen an diese Studie anzupassen. Folgende Fragen wurden aufgrund ihrer Trivialität in der heutigen Zeit entfernt: „I predict I would use mobile apps in the next 12 months.“ und „I intend to use mobile apps in the next 12 months.”. Es kann davon ausgegangen werden, dass die große Mehrheit der Deutschen sowie der gesamten Bevölkerung ein Smartphone besitzt und dieses meist täglich verwendet. Laut Bitkom besaßen im April 2018 81 % der deutschen Bevölkerung ein Smartphone. Eine Verwendung ohne Nutzung von Applikationen ist im Bereich der Smartphones nicht mehr denkbar. Aus diesem Grund wurde der Entschluss gefasst, die oben genannten Fragen nicht im Fragebogen aufzuführen.

Der Fragebogen wurde den Teilnehmenden bewusst erst am Ende der Studie ausgehändigt, um ein eventuelles Priming zu vermeiden und ist in fünf Dimensionen mit je drei Items unterteilt. Die erste Dimension bezieht sich auf die von den Nutzenden wahrgenommene Überwachung und erfasst die Besorgnis über die Sammlung von Informationen, die wahrgenommene Überwachung des Standorts ihres mobilen Endgerätes sowie die Besorgnis über die Aufzeichnung von Aktivitäten durch Applikationen. Die zweite Dimension fokussiert den von den Nutzenden wahrgenommenen Eingriff in die Privatsphäre und beinhaltet die Erfassung des Gefühls, dass andere durch die Verwendung von

Applikationen mehr über die Nutzenden wissen als es ihnen angenehm ist. Ferner wurde erfasst, ob die Nutzenden glauben, dass die Verwendung von Applikationen dazu führt, dass andere mehr über sie als Nutzende wissen als ihnen angenehm ist und ob die Steigerung an verfügbarer Information genutzt werden kann, um in die Privatsphäre einzudringen. Die dritte Dimension bezieht sich auf die Besorgnis über personenbezogene Daten durch sekundären Gebrauch und umfasst die Erhebung der Besorgnis, dass Applikationen persönliche Daten für andere Zwecke verwenden dürfen ohne die Nutzenden zu benachrichtigen oder ihre Berechtigung einzuholen. Darüber hinaus werden die Bedenken, dass Informationen der Nutzenden für andere Zwecke verwendet werden, beurteilt sowie die Besorgnis erhoben, dass persönliche Daten ohne Berechtigung mit anderen Instanzen geteilt werden könnten. Die vierte Dimension betrifft die vorherige Datenschutzerfahrung und erhebt die Häufigkeiten vorheriger Vorfälle binnen zwei Jahren, bei denen die persönlichen Daten der Nutzenden von Unternehmen der E-Commerce-Webseiten ohne Genehmigung dieser verwendet wurden und wie oft die Nutzenden im letzten Jahr über potenziellen Missbrauch des Sammelns von Informationen gehört oder gelesen haben. Im ursprünglichen Fragebogen von Xu et al. war bei dieser Frage kein zeitliches Fenster angegeben. Aufgrund der Tatsache, dass jene Vorfälle im Laufe der Zeit immer häufiger vorgekommen sind und um auf die Dringlichkeit der Problematik aufzuweisen, wurde nur nach Vorfällen innerhalb der letzten zwei Jahre gefragt. Zudem wurde die Anzahl der persönlichen negativen Erfahrungen erfragt, bei denen die Nutzenden unangemessene Eingriffe in ihre Privatsphäre erlebt haben. Die letzte Dimension betrachtet die Verhaltensabsicht seitens der Nutzenden in Bezug auf die Offenlegung von persönlichen Daten zur Nutzung von Applikationen. Dabei wird die Voraussage und die vorsätzliche Absicht Applikationen zu verwenden festgehalten.

Die übersetzte Version des MUIPCs befindet sich im Anhang U Teil E. Die dort angegebenen Aussagen wurden mit einer 7-stufigen Likert-Skala mit den Polen „trifft überhaupt nicht zu“ und „trifft voll zu“ von den Teilnehmenden bewertet beziehungsweise bei den Items der Dimension der vorherigen Datenschutzerfahrung mit folgenden vorgegebenen Single Choice Antwortmöglichkeiten erfragt: „kein Mal“, „1 – 2 mal“, „3 – 4 mal“ und „mehr als 5 mal“. Die 7-stufige Likert-Skala wurde von Xu et al. übernommen, während es jedoch nicht möglich war aus ihrem Artikel herauszulesen, mit welcher Skala die Häufigkeit der vorherigen Datenschutzerfahrung abgefragt wurde. Nach einem gescheiterten Versuch der Kontaktaufnahme mit den Autoren wurde entschieden eine möglichst teilnehmerfreundliche Variante zu wählen, welche aus den oben beschriebenen Single Choice Antwortmöglichkeiten bestand.

6.6.8 Demographische Daten

Zum Zweck der Beschreibung der Stichprobe sowie der Erfassung möglicher Einflussvariablen wurde unter anderem das Geschlecht, das Alter, der höchste Bildungsabschluss, die Technikaffinität auf einer 7-stufigen Likert-Skala (1 = „trifft überhaupt nicht zu“, 7 = „trifft voll zu“), die Häufigkeit der Smartphone-Nutzung in fünf Abstufungen, ob Maßnahmen zum Schutz der privaten Daten ergriffen werden und wie hoch die Wichtigkeit des Schutzes dieser ist, abgefragt. Der Fragebogen befindet sich im Anhang U Teil F.

6.7 Datenaufbereitung

Im folgenden Kapitel wird ähnlich wie im ersten empirischen Versuch die Aufbereitung der Rohdaten sowie das weitere Vorgehen zur Analyse der Daten erläutert. Die Datensätze wurden dafür in eine große Tabelle zusammengeführt. Vor allem die Aufbereitung der Eye-Tracking Videos erforderte einen außergewöhnlichen Arbeitsaufwand, weshalb diese etwas detaillierter beschrieben wird. Sämtliche Datensätze wurden wiederum in eine Tabelle bestehend aus 997 Variablen zusammengeführt und in SPSS importiert.

6.7.1 Demographische Daten der Stichprobe

Bezüglich der demographischen Daten wurde das Geschlecht kodiert, indem den männlichen Teilnehmern eine „1“ und den weiblichen Teilnehmern eine „2“ zugeordnet wurde. Das Alter bedurfte keiner weiteren Aufbereitung. Die Antworten zur Frage des höchsten Bildungsabschlusses wurden umkodiert, indem der Antwort „kein Abschluss“ eine „1“, „Hauptschule/ mittlere Reife“ eine „2“, „Abitur/ Allgemeine Hochschulreife“ eine „3“, „Berufsausbildung“ eine „4“ und „akademischer Abschluss“ eine „5“ zugeordnet wurden. Die Antworten bezüglich der Technikaffinität und der Wichtigkeit der Privatsphäre wurden auf einer siebenstufigen Likert-Skala mit den Polen „trifft überhaupt nicht zu“ und „trifft völlig zu“ beantwortet. Den Antworten wurden entsprechende Werte von eins bis sieben zugeordnet, um es zu ermöglichen die Mittelwerte der verschiedenen Gruppen zu ermitteln. Bezüglich der Frage zur täglichen Handynutzung wurden die Antworten „weniger als eine halbe Stunde“ mit einer „1“, „mehr als eine halbe Stunde, aber weniger als eine Stunde“ mit einer „2“, „mehr als eine Stunde, aber weniger als zwei Stunden“ mit einer „3“, „mehr als zwei Stunden, aber weniger als vier Stunden“ mit einer „4“ und „mehr als vier Stunden“ mit einer „5“ kodiert.

Betreffend der Frage nach dem aktiven Schutz der Privatsphäre wurden die Antwortmöglichkeiten dieser Frage jeweils einer Variable zugeteilt, weil bei dieser Frage Mehrfachantworten möglich waren. Mit den Antworten der Frage bezüglich der Relevanz der Punkte bei der Auswahl einer Applikation wurde wie bei dem vorherigen die Likert-Skala umgangen. Die entsprechenden Variablen sind im Anhang AA unter Nr. 207 – 212 wiederzufinden.

6.7.2 Fragebogen

Ähnlich wie beim ersten Versuch wurde auch dieser Fragebogen über das Portal LimeSurvey der Technischen Universität Berlin ausgefüllt. Dies ermöglichte den Import sämtlicher Daten in SPSS. Die folgenden Abschnitte erläutern die Aufbereitung der einzelnen Teile des Fragebogens.

6.7.2.1 Fragebogenteil über bisher verwendete Applikationen

Die Daten für den Fragebogenteil von den bisher verwendeten Applikationen wurden zunächst in eine Excel-Tabelle eingefügt. Anschließend wurden die Antworten aus dem ersten Teil des Fragebogens entnommen (6.6.2). Die Antworten „installiert und bereits verwendet“ wurden mit einer 1, „installiert und noch nicht verwendet“ mit 2, „bereits verwendet, derzeit jedoch nicht installiert“ mit 3, „nicht installiert und noch nicht verwendet“ mit 4 und „keine Antwort“ mit 5 kodiert. Daraufhin wurde wiederum überprüft, welche Applikation von den Teilnehmenden für das entsprechende Szenario gewählt wurde. Für jede einzelne Applikation wurde dabei eine Variable (VAPP_XX) erstellt und mit der entsprechenden Antwort in SPSS eingefügt. Somit sollte erfasst werden, ob die gewählte Applikation den Teilnehmenden bereits bekannt war oder sie sich für eine neue ihnen unbekannte Applikation entschieden haben. Eine Liste mit den Variablen befindet sich im Anhang AA Variablennummern 29 bis 106.

6.7.2.2 Fragebogenteil zu einzelnen Szenarien

Die Antworten des Fragebogen Teil C im Anhang U bezüglich der Vertrauenswürdigkeit und der Einfachheit der Auswahl wurden, ähnlich wie bei der Technikaffinität im Abschnitt 6.7.1, auf einer siebenstufigen Likert-Skala mit den Polen „trifft überhaupt nicht zu“ und „trifft völlig zu“ beantwortet. Den Antworten wurden entsprechende Werte von eins bis sieben gegeben, um es zu ermöglichen Mittelwerte der verschiedenen Gruppen zu ermitteln. Dies wurde bewerkstelligt, indem die Antworten von dem Lime-Survey Portal in eine Excel-Tabelle importiert wurden. Anschließend wurde mit Hilfe der

Funktion „Ersetzen“ nach den jeweiligen Antworten gesucht (z.B. „trifft zu“) und durch den zu vergebenen Wert ersetzt (in diesem Fall „6“). Wurden alle Antworten erfolgreich durch die entsprechende Zahl ersetzt, so erfolgte der Import der Daten in SPSS (Anhang Z Nr. 107 - 122).

Die Ergebnisse zur Relevanz der verschiedenen Bewertungsmethoden für die Auswahl einer Applikation wurden ebenfalls mit Hilfe einer Likert-Skala erfasst, wobei die gleiche Methode, die auch bei der Technikaffinität und dem Fragebogenteil zu den einzelnen Szenarien verwendet wurde, Anwendung fand. Die Variablen sind im Anhang AA von 220 bis 224 zu finden.

6.7.2.3 Fragebogenteil über die Bewertung der Datenschutzskala und des MUIPCs

Die Antworten zur Bewertung der Datenschutzskala waren genauso aufgebaut wie die zu den einzelnen Szenarien. So wurde hier die eben beschriebene Prozedur erneut angewandt (Anhang Z Nr. 179 – 193). Auch beim Fragebogenteil über die Bedenken der Internetnutzenden im Bereich der mobilen Endgeräte (MUIPC) wurde mit dem ersten Abschnitt genauso verfahren. Bei der Abfrage von Häufigkeiten wurde eine Single Choice Skala verwendet. Hierbei hatten die Teilnehmenden folgende Antwortmöglichkeiten zur Auswahl: „Kein Mal“, „1 bis 2-mal“, „3 bis 4-mal“ und „mehr als 5-mal“.

Auch hier wurden den Antworten in einer Excel-Tabelle die entsprechenden Werte von „1“ bis „4“ vergeben und anschließend in SPSS importiert (s. Anhang AA Nr. 194 – 206).

6.7.3 Eye-Tracking-Video

Mit Hilfe des Eye-Tracking-Videos konnte festgehalten werden, welche Applikation die Teilnehmenden in einem bestimmten Szenario ausgewählt haben. Hierfür wurden in einer ersten Runde alle Eye-Tracking-Videos gesichtet und in einer Excel-Tabelle festgehalten, welche Applikationen in den acht Szenarien gewählt wurden. Anschließend wurden die Applikationen von 1 bis 61 codiert. Dabei standen über 80 Applikationen zur Auswahl, wobei einige Applikationen nicht einmal gewählt wurden und somit keiner Codierung bedurften. Um zu ermitteln, ob die Teilnehmenden eine sichere oder kritische Applikation gewählt haben, wurde den Applikationen je nach Label und Farbe ein Score zugeteilt. Die „sehr kritischen“ Applikationen erhielten den niedrigsten Score mit 1, die „kritischen“ Applikationen einen Score mit 2, die „moderaten“ Applikationen einen Score mit 3, die „sicheren“ Applikationen einen Score mit 4 und die „sehr sicheren“ Applikationen einen Score mit 5. Darüber hinaus soll im weiteren Verlauf der Arbeit ebenfalls untersucht werden, ob der Rang der Applikation in der Listung einen Einfluss auf das Verhalten hat. Aus diesem Grund wurde den Applikationen je nach

Position auf den angezeigten Bildschirmen eine Zahl zugeordnet. Stand die Applikation ganz oben, so erhielt sie die Nummer 1, stand die Applikation ganz unten, so erhielt sie die Nummer 10 bzw. die Anzahl der Applikationen, die angeboten wurden. Die 24 Variablen sind in Anhang AA (Variablennummern 4 - 11; 21 – 28; 953 – 960) aufgelistet und wurden anschließend in SPSS eingefügt.

Weiterhin wurde festgehalten, ob die ausgewählten Applikationen bereits bekannt sind bzw. auf dem privaten Endgerät installiert oder benutzt wurden. Hierfür wurde geprüft, welche Applikation für ein bestimmtes Szenario genommen wurde (Variable CH_XX - in Anhang AA Variablennummern 4 - 11). Anschließend wurde anhand der Variablen, welche beinhalten, ob die Teilnehmenden die Applikationen bereits installiert oder verwendet haben (Variable VAPP_ XX - Anhang AA Variablennummern 29-106) geprüft, ob die Applikationen den Endnutzenden bekannt waren. Anschließend wurde in der Variable CH_VAPP_XX (Anhang AA Variablennummern 12- 20) festgehalten, ob die ausgewählten Applikationen bereits installiert oder verwendet wurden.

6.7.3.1 Anpassung der geschätzten Vertrauenswürdigkeit durch die Likert-Skala an die Datenschutzskala

Weiterhin war es für Hypothese 1, welche eine höhere Adäquatheit der Bewertung der Applikation bezüglich der Vertrauenswürdigkeit bei steigender Information über das Verhalten der Applikation betreffend des Datenschutzes postuliert, von Nöten, die Bewertungen der Applikation bezüglich der Vertrauenswürdigkeit mit dem eben erläuterten Score in Relation zu bringen.

Aufgrund der Tatsache, dass die Datenschutzskala fünfstufig war, die Bewertung der Vertrauenswürdigkeit jedoch mit Hilfe einer siebenstufigen Likert-Skala erfolgte, war es notwendig, diese beiden Skalen zunächst zu vereinheitlichen. In Absprache mit Prof. Dr. Rötting wurden drei Methoden für die Reskalierung beider Skalen diskutiert, die jedoch allesamt unterschiedliche Vor- und Nachteile mit sich bringen.

In der ersten Methode wurde die Likert-Skala gestaucht, indem die ersten beiden Kategorien („trifft überhaupt nicht zu“ und „trifft nicht zu“) und die letzten beiden Kategorien („trifft zu“ und „trifft völlig zu“) bezüglich der Aussage „Ich halte die Applikation für vertrauenswürdig im Hinblick auf den Schutz meiner Daten“ jeweils zusammengefasst wurden. Problematisch bei dieser Methode war, dass es zwischen den Teilnehmenden, welche die Vertrauenswürdigkeit der Applikation mit „trifft überhaupt nicht zu“ und „trifft nicht zu“ bzw. „trifft zu“ und „trifft völlig zu“ keinen Unterschied in der berechneten Differenz ergab und somit ein gewisser Detaillierungsgrad der Ergebnisse verloren ging.

Bei der zweiten Methode wurden beide Skalen auf eine prozentbasierte Skala umgewandelt. Aus der Datenschutzskala ergab sich somit eine prozentbasierte Aufteilung in 25er-Schritten: (0 (1 = sehr kritisch) / 25 (2 = kritisch) / 50 (3 = moderat) / 75 (4 = sicher) / 100 (5 = sehr sicher)), während sich bei der Likert-Skala eine Aufteilung in 100/6 Schritten (0 (1 = trifft überhaupt nicht zu) / 16,67 (2 = trifft nicht zu) / 33,34 (3 = trifft eher nicht zu) / 50 (4 = weder noch) / 66,67 (5 = trifft eher zu) / 83,34 (6 = trifft zu) / 100 (7 = trifft völlig zu)) ergab.

Problematisch bei dieser Methode war jedoch, dass bei einer Applikation, die als „kritisch“ (25 %) und als „sicher“ (75 %) eingestuft wurde, die Teilnehmenden keine Möglichkeit hatten, die Applikation angemessen zu bewerten. Mit der eben erwähnten Aufteilung der Likert-Skala wichen die Teilnehmenden jedoch mindestens 8,33 % ab, indem sie die Aussage, die Applikation als vertrauenswürdig zu empfinden, entweder als „nichtzutreffend“ oder „eher nicht zutreffend“ bewerteten.

Dabei musste der Betrag der Differenzen genommen werden, um einen Mittelwert zu errechnen, weil sich die Differenzen ansonsten gegenseitig aufheben würden und der Mittelwert den Anschein erwecken könnte, dass alle Teilnehmenden die Applikation adäquat bewertet haben.

Bei der dritten Methode wurde die fünfstufige Skala durch sieben dividiert, sodass folgende Aufteilung resultiert: 0,71 (1 = trifft überhaupt nicht zu) / 1,42 (2 = trifft nicht zu) / 2,14 (3 = trifft eher nicht zu) / 2,86 (4 = weder noch) / 3,57 (5 = trifft eher zu) / 4,28 (6 = trifft zu) / 5 (7 = trifft völlig zu). Hierbei ergab sich ein ähnliches Problem wie bei der zweiten Methode, welches sich jedoch intensiviert. Bei der vorliegenden Aufteilung stimmt lediglich der höchste Pol beider Skalen miteinander überein. Bei allen anderen Zahlen würde eine Differenz resultieren, sogar wenn es sich um eine sehr kritische Applikation handelt und die Teilnehmenden bezüglich der Vertrauenswürdigkeit die Antwort „trifft überhaupt nicht zu“ gewählt haben. Darüber hinaus war bei dieser Methode problematisch, dass wenn nicht der höchste Pol gewählt wurde, die Differenz teilweise größer ausfallen konnte, selbst wenn die Kategorien in etwa übereinstimmten. Hier ein kurzes Beispiel: Wenn die Teilnehmenden bei einer als „kritisch“ (2) eingestuften Applikation auf die Aussage der Vertrauenswürdigkeit mit „trifft nicht zu“ (1,42) antworteten, so resultierte eine Differenz von 0,58, während bei der Auswahl der Antwort „trifft eher nicht zu“ (2,14) eine Differenz von 0,14 resultierte.

Weil jede dieser Methoden Vor- und Nachteile mit sich bringt, wurde sich dazu entschlossen, alle drei Vorgehensweisen durchzuführen, um anschließend die Ergebnisse zu vergleichen.

Für die Umsetzung der ersten Methode (gestauchte Skala) wurden die ersten beiden Kategorien der Skala („trifft überhaupt nicht zu“ und „trifft nicht zu“) bezüglich der Aussage „Ich halte die Applikation

für vertrauenswürdig im Hinblick auf den Schutz meiner Daten“ mit einer 1 versehen. Der Kategorie „trifft eher nicht zu“ wurde die Zahl 2 zugeordnet, während für die Kategorie „weder noch“ die Zahl 3 eingefügt wurde. Die vierte Stufe entsprach somit der Kategorie „trifft eher zu“, während die beiden Kategorien „trifft zu“ und „trifft völlig zu“ wiederum zusammengeführt wurden und somit die fünfte Stufe der zusammengeführten Skala ausmachen. Das Ersetzen der Zahlen wurde bei Excel vorgenommen, indem folgende Formel verwendet wurde:

=WENN(V7=1;1;WENN(V7=2;1;WENN(V7=3;2;WENN(V7=4;3;WENN(V7=5;4;WENN(V7=6;5;WENN(V7=7;5;"#NULL")))))).

Anschließend wurden die Zahlen der acht Variablen (Anhang AA Nr. 123 – 130) in SPSS eingefügt. Darüber hinaus wurde die Differenz zwischen dieser neuen Skala (APP_5S_Vertrauenswürdigkeit_XX) und dem Score der ausgewählten Applikation (CH_XX_Score) berechnet, indem die neue Skala von dem Score subtrahiert wurde.

Die acht resultierenden Variablen (Anhang AA Nr. 131 – 138) wurden ebenfalls in SPSS eingefügt. Mit Hilfe dieser Variablen konnte jedoch nur die Häufigkeit der Teilnehmenden erfasst werden, welche die Vertrauenswürdigkeit der Applikation überschätzt, unterschätzt oder adäquat eingeschätzt haben. Ein Vergleich der Mittelwerte ist weiterhin nicht möglich, weil bei der Berechnung der Differenz bei einer Person, welche die Applikation als vertrauenswürdiger einschätzt als sie auf der Datenschutzskala eingestuft wurde, ein positives Ergebnis resultiert, während bei den Teilnehmenden, die die Applikation als weniger vertrauenswürdig einschätzen, ein negatives Ergebnis resultiert. Wird anschließend der Mittelwert aus diesen beiden Ergebnissen gebildet, so könnte sich eine Differenz von 0 ergeben, welche darauf schließen lässt, dass die Stichprobe insgesamt die Applikationen angemessen eingeschätzt hat, was jedoch nicht der Fall war. Aus diesem Grund wurde sich dazu entschieden, den Betrag der Differenz als neue Variable in SPSS einzupflegen (Anhang AA Nr. 139 – 146).

Die Umsetzung der zweiten Methode ähnelt dem bereits für die erste Methode erklärten Vorgehen. Hierbei wurden die entsprechenden Zahlen in Prozent umgerechnet. Um die beiden Skalen vergleichen zu können, musste dies jedoch anders als bei der ersten Methode bei der Likert-Skala und bei der Datenschutzskala durchgeführt werden. So wurden die Zahlen bei der Datenschutzskala durch die entsprechenden Prozentangaben ersetzt, indem folgende Formel in Excel verwendet wurde: =WENN(D4=1;0;WENN(D4=2;25;WENN(D4=3;50;WENN(D4=4;75;WENN(D4=5;100;))))).

Die Prozentangaben der Likert-Skala wurden mit folgender Formel berechnet: =WENN(B4=1;0;WENN(B4=2;16,67;WENN(B4=3;33,34;WENN(B4=4;50;WENN(B4=5;66,67;WENN(B4=6;83,34;WENN(B4=7;100;"")))))))

Anschließend wurde die Differenz zwischen der prozentualen Skala der Einschätzung der Vertrauenswürdigkeit und der prozentuellen Datenschutzskala berechnet, indem die erstere von zweiterer subtrahiert wurde. Hieraus resultierten folgende Variablen Nr. 147 – 154 (DIF_APP_Prozentual_Vertrauenswürdigkeit_XX), welche ebenfalls im Anhang AA zu finden sind. Weiterhin wurde hier ebenfalls der Betrag der Differenzen berechnet, um die Mittelwerte vergleichen zu können (Anhang AA Nr. 155 – 162).

Für die Umsetzung der dritten Methode musste lediglich die Likert-Skala der Vertrauenswürdigkeit mit $5/7$ multipliziert werden. Eine Umwandlung der Datenschutzskala war nicht nötig. Auch hier wurden die Differenzen berechnet, indem der Wert der Datenschutzskala von der umgewandelten Likert-Skala subtrahiert wurde. Hierbei wurde ebenfalls der Betrag berechnet, sodass insgesamt 16 Variablen in SPSS implementiert wurden (Anhang AA Nr. 163 – 170; 171 - 178).

6.7.3.2 Aufteilung der Areas of Interest und Erfassung der Blickfixation

Das Eye-Tracking-Video sollte ferner die Teilnehmenden unterstützen, sich während des Interviews in die vorherige Situation wieder hineinversetzen zu können. Dabei konnten sie das eigene Blickverhalten während der Applikationsauswahl in dem Video nachvollziehen, indem der Blickfixationspunkt als grüner Kreis im Video zu sehen war. Problematisch war in diesem Fall die Berechnungszeit, die benötigt worden wäre, um die Blickdaten im Video anzeigen zu lassen. Um den Ablauf des Experimentes zu beschleunigen, wurde deshalb eine Alternative gewählt, die das Programm Direct Gaze von SMI BeGaze™ anbietet. Diese ermöglichte die Blickbewegungsdaten während der Aufnahme als grüner Punkt direkt in die .avi-Videodatei zu implementieren. Nachteil an dieser Option war jedoch der Wegfall der Datei der Blickdaten, mit Hilfe derer es möglich gewesen wäre, Areas of Interest (AOI) zu bestimmen und eine Auswertung weitestgehend zu automatisieren. Aufgrund der Nichtverfügbarkeit dieser Datei war eine manuelle Auswertung von Nöten.

Hierfür wurde der Videoabschnitt jedes Szenarios in Teilabschnitte unterteilt, die verschiedene Tätigkeiten beinhalteten, welche für die Erfüllung der jeweiligen Aufgabe durchgeführt werden mussten. Manche dieser Tätigkeiten waren zwar für die Aufgabenerfüllung nötig, sind aber für die spätere Auswertung der Blickdaten mit dem Ziel der Identifikation der für die Entscheidungsfindung wichtigen Oberflächenelemente nicht relevant. Die für die Auswertung relevanten Teilabschnitte wurden mit einer Zahl zwischen „1“ und „14“ kodiert. Teilabschnitte, die nicht relevante Tätigkeiten beinhalteten, wurden mit der Zahl „99“ kodiert.

Vom Beginn des Videos bis zur Eingabe des ersten Buchstabens in die Suchzeile erfolgte die „Anweisung für die Aufgabe“. In dieser Zeitspanne wurde die Aufgabenstellung für das aktuelle Szenario vorgelesen und bei Bedarf aufkommende Fragen und Missverständnisse geklärt. Dieser Teilabschnitt ist für die Auswertung irrelevant und wurde deshalb mit „99“ kodiert.

Ab der Eingabe des ersten Buchstabens bis zur Aktivierung der Suche, welche durch das Ausblenden der Tastatur gekennzeichnet war, wurde der Abschnitt mit einer „1“ als „Eingabe des Stichworts“ gekennzeichnet. Hierbei ist zu erwähnen, dass nur der erste Buchstabe der letzten und somit erfolgreichen Suche als Anfangspunkt dieser Tätigkeit gewertet wurde, weil manche Teilnehmende mehrere Anläufe für die Auswahl der richtigen Applikation benötigt haben.

Darauf folgte der Abschnitt der „Entscheidungsfindung“, welcher aufgrund der Relevanz für die Fragestellung tiefergehend ausgewertet wurde. Ab diesem Moment wurden die Videos zusätzlich bezüglich des Blickverhaltens analysiert. Hierbei wurde bei jedem Frame des Videos festgehalten, welches Element die Teilnehmenden zu diesem Zeitpunkt betrachteten, also wo sich der Fixationspunkt befand. Dabei wurden zehn verschiedene Fixationsbereiche bzw. Blickbewegungen unterschieden und kodiert: Symbole der Applikationen (2), Namen der Applikationen (3), Datenschutzskala der Applikationen (4), Bewegung des Blicks (5), Suchzeile (6), Zurücktaste (7), Apptaste (8), Hometaste (9), Tastatur (10) und die zur Datenschutzskala zugehörigen Datenschutzdiagramme (11). Die Betrachtung eines Datenschutzdiagramms begann erst nachdem auf die Datenschutzskala geklickt wurde und sich das entsprechende Diagramm für die jeweilige Applikation öffnete.

Sobald die Teilnehmenden eine Applikation auswählten, begann der Abschnitt der „Applikationsauswahl“ (12). In diesem Abschnitt befanden sich die Teilnehmenden nun im originalen Google Play Store und konnten weitere Details über die ausgewählte Applikation einsehen. Hierbei wurde wie bei der Entscheidungsfindung ebenfalls das Blickverhalten der Teilnehmenden ausgewertet. Dabei war es relevant, ob und wie lange die Teilnehmenden die Vorschaubilder der Applikation (13) sowie Rezensionen bzw. Bewertungen (14) betrachteten (vgl. Abbildung 17). Sobald der Blick nicht auf den Bildern oder den Rezensionen lag, wurde wiederum der Abschnitt der Applikationsauswahl (12) eingetragen. Der Abschnitt endete mit dem Erscheinen des Installationsbalkens. Während der Studie wurde der Google Play Store leicht modifiziert, sodass statt dem Ladebalken ein Ladekreis um das Symbol der Applikation erschien. Es wurde sich dafür entschieden den Ladekreis statt des Ladebalkens als Zeichen für das Ende des Abschnittes der „Applikationsauswahl“ bzw. den Anfang des irrelevanten Abschnittes (99) zu verwenden.

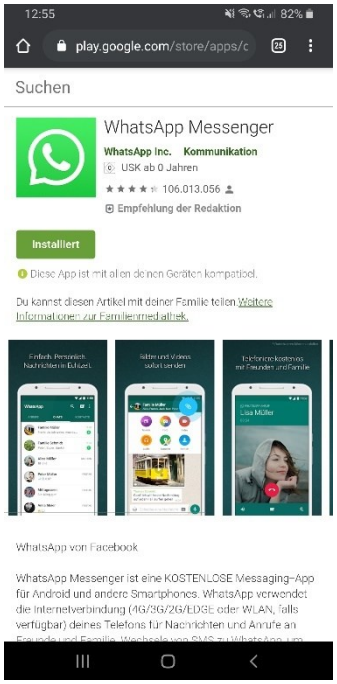


Abbildung 17. Applikation nach Auswahl vor der Installation.

Alle restlichen Tätigkeiten, einschließlich der Installation der Applikation, des Öffnens und des Einrichtens der Applikation, der Ausführung der Aufgabe, der Rückkehr in den App-Markt sowie der Aufgabenanweisung für das nächste Szenario, sind für die Auswertung irrelevant und wurden mit der Ziffer „99“ kodiert. Die irrelevanten Zeitabschnitte endeten somit, sobald der erste Buchstabe für das Suchwort des nächsten Szenarios in die Suchzeile eingetragen wurde. Ab diesem Moment erfolgt der nächste Durchlauf beginnend mit Tätigkeit „1“.

Die Zeitabschnitte, in denen für kurze Zeit kein Fixationspunkt im Video ersichtlich war, wurden mit der Ziffer 0 kodiert.

Es wurde sich für die Zusammenfassung der Tätigkeiten ab der Installation der Applikation bis zur Eingabe des neuen Stichwortes entschieden, weil diese Tätigkeiten (u.a. die Rückkehr in den App-Markt) wie oben erwähnt für die Beantwortung der Fragestellung bzw. die Überprüfung der Hypothesen keine Relevanz hatten. Die Zusammenfassung der Tätigkeiten geschah erst nachdem die ersten Videos ausgewertet wurden und der Zeitaufwand sowie die Ersparnis durch die Zusammenfassung abschätzbar waren.

Für die Berechnung der gesamten Bearbeitungszeit der einzelnen Aufgaben wurde den Frames, welche für die Aufgabenbearbeitung relevante Tätigkeiten beinhalteten, zusätzlich zur Ziffer für die Kodierung der Tätigkeit auch eine Kodierungsziffer des entsprechenden Szenarios zwischen 1 und 8 zugewiesen.

Aus diesem Grund wurden die für die Fragestellung als irrelevanten Tätigkeiten bzw. Abschnitte ebenfalls genau definiert:

Spezifische Beschreibung der irrelevanten Abschnitte

Die Tätigkeit, „Installation der Applikation“ (16), beginnt mit dem Erscheinen des Installationsbalkens nach Anklicken der Installationsschaltflächen und endet mit dem Anklicken der „Öffnen“-Schaltfläche. Die 17. Tätigkeit umfasste die Einrichtung der Applikation und begann direkt nach der 16. Tätigkeit, dem Anklicken der „Öffnen“-Schaltfläche. In dieser Zeit richtete die Person die Applikation ein, indem er/sie fiktive, persönliche Daten eingab oder sich bei der Applikation anmeldete. Die Tätigkeit endete mit dem Drücken der letzten Schaltfläche zur erfolgreichen Einrichtung. Ab diesem Zeitpunkt begann die Tätigkeit der „Aufgabenausführung“ (18), die bis zum Drücken der letzten Schaltfläche zur Erfüllung der Aufgabe, z.B. „abschicken“ oder „suchen“, andauerte. Nachdem die Aufgabe abgeschlossen wurde, begann die Person mit der Rückkehr in den App-Markt (19). Diese Tätigkeit beschreibt den Übergang nach der Erfüllung der Aufgabe bis zur Rückkehr in den App-Markt, um die nächste Aufgabenstellung zu erhalten. Dieser Zeitabschnitt endete dementsprechend, sobald der App-Markt wieder vollständig sichtbar war. Ab diesem Moment erfolgte der nächste Durchlauf der Tätigkeiten beginnend mit Tätigkeit 1.

Die Auswertung wurde mit Hilfe des SMPlayers Version 19.10.0 von Ricardo Villalba durchgeführt. Dieses Programm wurde gewählt, weil es zum einen die Möglichkeit bietet durch Tastenkürzel Bild für Bild zu betrachten, in diesem Fall konnte mit „ , “ ein Frame zurück und mit „ . “ ein Frame vorgesprungen werden. Darüber hinaus war es möglich, sich mit diesem Programm die verstrichene Zeit in Millisekunden anzeigen zu lassen. Die Eye-Tracking-Videos verfügten über eine Bildfrequenz von 24 Bildern pro Sekunde.

6.7.3.3 Beschreibung der Auswertungstabelle

Um die Auswertung der Videos so einfach wie möglich zu gestalten, wurde eine Excel-Tabelle mit sechs Spalten angelegt, in der jede Zeile einen Frame repräsentierte. Für jede Person wurde eine separate Datei erstellt.

In Spalte A wurde, wie oben beschrieben, festgehalten, in welchem Szenario (1: Messenger; 2: Videokonferenz; 3: Wetter; 4: E-Mail; 5: Musik; 6: Fitness; 7: Spiele; 8: Nachrichten) sich die Person zum Zeitpunkt des jeweiligen Frames befand, sowie in Spalte B, welche der eben genannten Tätigkeiten bzw. Blickfixationen zutreffend waren (0 - 14 bzw. 99).

Ferner wurde eine Spalte (F) angelegt, welche die verstrichene Zeit zum Zeitpunkt des jeweiligen Frames enthielt und dies als Summe der verstrichenen Sekunden angab. Die Spalte wurde berechnet, indem aufgrund der Bildfrequenz von 24 Frames pro Sekunde 1/24 Sekunden, also 41,67 Millisekunden zum vorherigen Wert addiert wurden. Zwischen den Frames liegen somit jeweils ca. 42 Millisekunden. Aufgrund der Tatsache, dass 1/24 als Dezimalzahl periodisch und somit unendlich ist, wurde die Zahl auf neun Nachkommastellen gerundet, weil die Zahl ein Ausgangswert für weitere Berechnungen ist und durch das Runden einige Probleme vermieden wurden. Folgende Formel wurde in die jeweilige Zeile der Excel-Tabelle eingetragen, wobei (x) die aktuelle Zeile repräsentiert: =RUNDEN(SUMME(F(x)+1/24);9).

Die verstrichene Zeit wird im Videoplayer mit dem Format hh:mm:ss,000 angegeben, wobei „hh“ für Stunden, „mm“ für Minuten, „ss“ für Sekunden und „000“ für Millisekunden steht. Nach 1000 Millisekunden wird der Sekundenwert hochgezählt. Beispielsweise folgt auf den Frame zum Zeitpunkt 00:10:09,958 der nächste Frame zum Zeitpunkt 00:10:10,000. Dieser zweite Wert wird in Spalte F als 610.000 Millisekunden angegeben. Zur Vermeidung der ständigen Umrechnung wurden in Spalte E die Millisekunden in das Zeitformat des Players umgewandelt. Dies wurde erreicht, indem der Wert aus Spalte F durch die Anzahl der Sekunden eines Tages (86400 s) dividiert wurde und in Excel das Zeitformat hh:mm:ss,000 für die Spalte E gewählt. Folgende Formel wurde in die jeweilige Zeile der Excel-Tabelle eingetragen, wobei (x) die aktuelle Zeile repräsentiert: =F(x)/86400.

Um das Ablesen der einzelnen Frames zu erleichtern, wurde die Anzeige der Stunden, Minuten und Sekunden auf Spalte C und die Anzeige der Millisekunden auf Spalte D verteilt. In Spalte C wird die verstrichene Zeit des Video bis zu dem entsprechenden Frame somit im Format hh:mm:ss angegeben (bspw.:0:00:01). Dies wurde berechnet, indem der entsprechende Werte aus Spalte F auf die nächstkleinere ganze Zahl abgerundet und anschließend durch die Anzahl der Sekunden eines Tages geteilt wird. Folgende Formel wurde in die jeweilige Zeile der Excel-Tabelle eingetragen, wobei (x) die aktuelle Zeile repräsentiert: =ABRUNDEN(F(x);0)/86400.

In Spalte D wurde wie oben erwähnt die Anzahl der verstrichenen Millisekunden der jeweiligen Sekunde des aktuellen Frames angezeigt. Der Wert entspricht dem gerundeten Vielfachen von 41,667 Millisekunden, welcher berechnet wurde, indem eine Sekunde (1000 Millisekunden) durch die 25 Frames pro Sekunde dividiert wurde. Um die Millisekunden jeder Sekunde von eben dieser zu trennen, wurde zunächst der Wert aus Spalte F auf drei Kommastellen gerundet (bspw.: 1,234). Anschließend wurde dieser Wert auf die nächste natürliche Zahl, also auf die nächste volle Sekunde abgerundet (bspw.:1). Hierzu zählte auch die Zahl 0. Dieser Wert wurde anschließend von dem ursprünglichen Wert aus Spalte F subtrahiert und mit 1000 multipliziert (bspw.: 1,234 – 1 = 0,234 * 1000 = 234). Somit

wurden die Minuten und die Sekunden von dem Wert der verstrichenen Zeit abgezogen und es verblieben allein die Millisekunden jeder Sekunde. Folgende Formel wurde in die jeweilige Zeile der Excel-Tabelle eingetragen, wobei (x) die aktuelle Zeile repräsentiert: =RUNDEN((F(x)-GANZZAHL(RUNDEN(F(x);3)))*1000;0).

Darüber hinaus wurde in Spalte G für jede Zeile geprüft, ob sich die aktuelle Tätigkeit dieser Zeile von der vorherigen Tätigkeit in der vorangegangenen Zeile unterscheidet. Wenn dem so war, wurde in Spalte G der Wert der aktuellen Tätigkeit eingetragen. War keine Veränderung der Tätigkeit vorhanden, so wurde in Spalte G „NA“ eingetragen. Folgende Formel wurde in die jeweilige Zeile der Excel-Tabelle eingetragen, wobei (x) die aktuelle Zeile und somit (x-1) die vorherige Zeile repräsentierten: =WENN(B(x-1)<>B(x);B(x);"NA").

Um die oben beschriebenen Werte der einzelnen Tätigkeiten jedes Szenarios näher zu betrachten, wurden anschließend acht separate, untereinander angeordnete Tabellen in Spalte I bis N in die Excel-Mappe eingefügt. Für jedes Szenario erfolgte somit eine separate Auswertung. Eine neunte Tabelle fasste alle Szenarien der einzelnen Teilnehmenden zusammen und berechnete die insgesamten Werte. In den neun Tabellen wurden die insgesamte Häufigkeit und das Andauern der jeweiligen Tätigkeit pro Szenario errechnet. Dabei umfasst die Tabelle jedes Szenarios jeweils 20 Zeilen, da unter anderem alle Tätigkeiten (0 - 14 und 99) einzeln betrachtet wurden und in den letzten beiden Zeilen die Zeiten für die insgesamte Bewältigung des Szenarios und für die Entscheidungsfindung zusammengefasst wurden. Im weiteren Verlauf wurden die neun Tabellen als Szenario-Tabellen bezeichnet und die einzelnen Funktionen der Spalten erläutert.

In der zweiten Zeile der Spalte I jeder Szenario-Tabelle wurde jeweils das zu betrachtende Szenario von 1 – 8 angegeben. Spalte J enthielt jeweils die Tätigkeiten von 0 – 14 sowie den für diesen Versuch nicht relevanten Abschnitt, der mit 99 beziffert wurde. Dieser wurde trotzdem in die Zusammenfassung einberechnet, um zu erfassen wie viel Zeit die Teilnehmenden insgesamt für die Aufgabenbewältigung benötigten.

Die Spalte K zählte mit Hilfe der Spalte G, wie häufig eine Tätigkeit in dem Szenario durchgeführt wurde. Es wurde für alle Zeilen geprüft, wie oft die spezifischen Kombinationen von Szenario (Spalte A) und der Wechsel auf eine Tätigkeit (Spalte G) vorkamen. Diese Häufigkeit wurde anschließend in Spalte K (Anzahl der Wechsel) eingetragen. Folgende Formel wurde in die jeweilige Zeile der Excel-Tabelle eingetragen, wobei (x) die aktuelle Zeile repräsentiert: =ZÄHLENWENNS(A:A;I(x);G:G;J(x)).

In Spalte L wurde die Anzahl der Frames berechnet, die für die Erfüllung einer Tätigkeit in dem spezifischen Szenario benötigt wurde. Ähnlich wie in Spalte K wurde in Spalte L betrachtet, wie häufig

der Szenariowert aus Spalte I mit dem Szenariowert aus Spalte A übereinstimmte und der Tätigkeitswert aus Spalte J mit dem Tätigkeitswert der Spalte B übereinstimmte. Folgende Formel wurde in die jeweilige Zeile der Excel-Tabelle eingetragen, wobei (x) die aktuelle Zeile repräsentiert: =ZÄHLENWENNS(A:A;I$(x);B:B;J(x)). Das Ergebnis ist die gesamte Anzahl der Frames dieser Tätigkeit in diesem Szenario, die in Spalte M in Sekunden umgerechnet wurden, indem die Anzahl der Frames durch 24 geteilt wird. Folgende Formel wurde in die jeweilige Zeile der Excel-Tabelle eingetragen, wobei (x) die aktuelle Zeile repräsentiert: =L(x)*1/24.

In der 19. und 20. Zeile der Spalte M wurde für jedes Szenario jeweils die Summe der Zeit für die Entscheidungsfindung sowie die Summe der gesamten Zeit, die für die Bearbeitung des Szenarios aufgewandt wurde, berechnet. Die Zeit der Entscheidungsfindung besteht aus den Tätigkeiten 2 – 11 und 13 – 14. Alle anderen Tätigkeiten wurden bei der Berechnung der Summe der Entscheidungsfindungszeit nicht berücksichtigt, weil sie für die Entscheidungsfindung als nicht relevant angesehen wurden. Darunter zählten die Eingabe des Stichwortes (1), die Anweisungen in die Aufgabe (99), die Installation und die Einrichtung der Applikation (99) sowie die Ausführung der Aufgabe als auch die Rückkehr in den Apps-Markt (99).

Um die insgesamt aufgewandte Zeit für die Tätigkeitserfüllung in dem Szenario zu berechnen, wurden anschließend die Zeiten aller Tätigkeiten aufsummiert, wobei die Zeit für die Entscheidungsfindung zusätzlich einzeln betrachtet wurde und hierfür die Zeiten der für die Entscheidungsfindung wichtigen Tätigkeiten separat aufsummiert wurde. Dies passierte in der 19. und 20. Zeile der Spalte M.

Weiterhin wurde in Spalte N angegeben, wie groß der zeitliche Anteil der spezifischen Tätigkeiten an der Entscheidungsfindung in diesem Szenario war. Dies wurde erreicht, indem die Zeit der einzelnen Tätigkeit durch die zeitliche Summe der für die Entscheidungsfindung wichtigen Tätigkeiten geteilt wurde. Dasselbe Verfahren wurde angewandt, um den Prozentsatz der Tätigkeit innerhalb des ganzen Szenarios zu erfassen. Diese Werte standen in Spalte O.

6.7.3.4 Zusammenführung der Auswertungstabellen

Um eine erste deskriptive Auswertung über alle vier Gruppen zu ermöglichen, wurde eine neue Excel-Tabelle angelegt, welche vier Mappen entsprechend der Gruppen von A bis D enthielt. In diesen Mappen wurden die Tabellen der einzelnen Versuchspersonen nebeneinandergestellt, welche aus acht untereinanderstehenden Tabellen entsprechend der Szenarien bestehen. Die neunte Tabelle fasst alle Szenarien pro Person zusammen. Eine weitere zusammenfassende Tabelle enthält alle

Teilnehmenden einer Gruppe, sodass es möglich war, diese vier resümierenden Tabellen nebeneinanderzustellen und zu vergleichen.

Zur Einspeisung der Daten in das Statistikprogramm SPSS war es von Nöten, alle Daten einer Versuchsperson in einer Zeile anzugeben. Um sicherzustellen, dass bei dieser Transponierung keine Fehler beim Kopiervorgang unterlaufen, wurde eine Excel-Tabelle erstellt. Bei dieser musste lediglich die Anzahl der Wechsel und die Anzahl der Frames für jede Tätigkeit (0 bis 14 und 99) pro Szenario bei jeder VP eingefügt werden. Die Zeit in Sekunden, der zeitliche Anteil der Entscheidungsfindung, der zeitliche Anteil insgesamt, die Summe der Entscheidungsfindung sowie deren prozentueller Anteil als auch die Summe der Zeit insgesamt in Sekunden wurden durch die entsprechenden Formeln, die bereits im Unterpunkt 6.7.3.3 beschrieben wurden, berechnet. Die zusammenfassende Tabelle jeder Testperson über alle acht Szenarien wurde ebenfalls in dieser Tabelle zur Einspeisung in SPSS berechnet. Dies ermöglichte beim Abgleich der Ergebnisse eine schnelle Verifizierung der korrekten Datenübertragung in ebendiese Tabelle.

Insgesamt ergibt sich eine Anzahl von 711 Variablen, die aus jeweils der Anzahl der Wechsel (Spalte K der Auswertungstabelle), der Anzahl der Frames (Spalte L), der Zeit für die Tätigkeiten in Sekunden (Spalte M), dem zeitlichen Anteil der Tätigkeit bezüglich der Entscheidungsfindung (Spalte N) und dem zeitlichen Anteil der Tätigkeit insgesamt (Spalte O) bestehen. Darüber hinaus enthält die Tabelle zur Einspeisung in SPSS die Summe der Zeit in Sekunden insgesamt sowie die Summe der Zeit für die Entscheidungsfindung und den prozentualen Anteil dieser. Ferner wurden die eben genannten Variablen zusammenfassend für eine Person über alle Szenarien resümiert. In einem weiteren Schritt werden diese zusammenfassenden Tabellen aller Teilnehmenden einer Gruppe wiederum in einer übergeordneten Tabelle aufgeführt. In einer Tabelle für ein Szenario sind insgesamt 16 Tätigkeiten enthalten. Für diese 16 Tätigkeiten wird für die Anzahl der Wechsel, Anzahl der Frames, Zeit für die Tätigkeit in Sekunden sowie den zeitlichen Anteil insgesamt jeweils eine einzelne Variable erstellt (4 x 16 = 64 Variablen). Weitere 12 Variablen kommen durch die Berechnung der Anteile für die Entscheidungsfindung relevanter Tätigkeiten hinzu (64 + 12 = 76 Variablen). Des Weiteren werden die Summe der Zeit, die für das Szenario benötigt wurde, sowie die Summe der Zeit, die für die Entscheidungsfindung aufgewandt wurde, als Variable dargestellt (76 + 2 = 78 Variablen). Die letzte Variable beinhaltet den prozentuellen Anteil der Zeit der Entscheidungsfindung von der Summe der Zeit insgesamt (78 + 1 = 79 Variablen). Für jede Testperson wurden dementsprechend acht Tabellen, für jedes Szenario eine, erstellt. Eine weitere Tabelle fasst die Zeiten über alle Szenarien für eine Versuchsperson zusammen. Dies ergibt eine Zahl von 9 x 79 = 711 Variablen. Die Beschriftung der Variablen erfolgte nach dem folgenden Prinzip:

Alle 711 Variablen beginnen mit dem Kürzel „EV_“ für Eye-Tracking-Video. Anschließend wird das Szenario nummeriert benannt „EV_1Messenger“. Im nächsten Schritt wird angegeben, was die angegebene Zahl beinhaltet (Anzahl der Wechsel, Anzahl der Frames, Zeit für die Tätigkeit in Sekunden, etc.): „EV_1Messenger_AnzahlWechsel“. Im letzten Teil wird angegeben, um welche Tätigkeit es sich bei der Variablen handelt: „EV_1Messenger_AnzahlWechsel_kein_Signal“ (Anhang Z Nr. 225 – 952). Eine Liste aller Variablen ist im Anhang AA wiederzufinden.

Zur Prüfung der vierten Hypothese war es darüber hinaus von Nöten, 16 weitere Variablen einzufügen. Dies war notwendig, weil die Stichprobe die auszuführenden Aufgaben in zwei verschiedenen Reihenfolgen absolvierte.

Zunächst wurden acht Variablen (Anhang AA Nr. 938 – 945) eingefügt, welche die Entscheidungszeiten in Sekunden der jeweils 1. – 8. Applikation in chronologischer Reihenfolge enthalten. So enthielt die erste Variable bei den Teilnehmenden, welche die erste Reihenfolge beginnend mit der „Messenger“-Applikation hatten, die Entscheidungszeit in Sekunden für eben diese Applikationskategorie. Bei den Teilnehmenden, welche die Aufgaben der Studie in der zweiten Reihenfolge absolvierten, enthielt die erste Variable die Entscheidungszeit in Sekunden der „Wetter“-Applikation. Dementsprechend wurde die Entscheidungszeit für alle acht Szenarien bzw. Aufgaben chronologisch in die entsprechende Variable eingefügt. Damit die Variable nicht manuell eingetragen werden musste, wurde in Excel eine Formel verwendet, die prüft, in welcher Reihenfolge die Testperson, die die Aufgaben absolvierte, um dann die entsprechende Entscheidungszeit der dazugehörigen Aufgabe einzutragen. Hierfür wurde eine weitere Variable eingefügt, welche die Reihenfolge angibt, in der die Teilnehmenden die Szenarien absolviert haben (EV_Reihenfolge). Anschließend wurde mit Hilfe einer Gleichung (Beispiel für die erste Applikation =WENN(EV_Reihenfolge =1; Messenger;WENN(EV_Reihenfolge =2;IB2;"NA"))) geprüft, ob in dieser Variable eine „1“ für die erste oder eine „2“ für die zweite Reihenfolge stand. Anschließend wurde die entsprechende Entscheidungszeit in Sekunden des dazugehörenden Szenarios ausgelesen und in die Variable kopiert. Weiterhin wurden 7 weitere Variablen (Anhang AA Nr. 946 – 952) erstellt, welche den Unterschied der Entscheidungszeit zwischen der vorangegangenen und der nachfolgenden Applikation berechnen. Beide Reihenfolgen sind in 6.6.3 wiederzufinden.

Um zu erfassen, welche Applikationen in den jeweiligen Szenarien von den Teilnehmenden ausgewählt wurden, mussten zunächst alle Videos gesichtet werden. Die entsprechenden Applikationen des jeweiligen Szenarios wurden anschließend bei der dazugehörigen Versuchsperson eingetragen. Nachdem alle Videos vollständig ausgewertet wurden, ergab sich eine Tabelle mit 82 Versuchspersonen bei der jeweils in acht Szenarien die ausgewählte Applikation ausgelesen werden

konnte. Um diese Tabelle in die SPSS implementieren zu können, wurde den einzelnen Applikationen eine Kennziffer (Code) von 1 bis 61 zugeordnet. Die geringe Anzahl der zu kodierenden Applikationen ist durch das Auswahlverhalten der Teilnehmenden bedingt. Den Teilnehmenden standen im selbstentwickelten App-Markt über 80 Applikationen zu Verfügung, unter anderem wurden jedoch Applikationen während des gesamten Experimentes nicht gewählt, sodass diese auch nicht kodiert wurden. Im Verlauf der Studie wurden insgesamt lediglich 61 Applikationen gewählt und somit später auch kodiert.

Anschließend wurde in einer weiteren Variablen (CH_xx_Score) festgehalten welche Kategorisierung die von den Teilnehmenden ausgewählten Applikationen in Bezug auf den Datenschutz hatten. Hierfür wurde zunächst überprüft, welche Applikationen die Testperson in dem entsprechenden Szenario gewählt hat. Um zu evaluieren, ob ein Unterschied zwischen den Gruppen bezüglich der Applikationsuaswahl und deren Datenschutzfreundlichkeit zu finden ist, wurde betrachtet, welcher Kategorisierung die entsprechende Applikation zugeordnet war (von sehr unsicher = 1 bis sehr sicher = 5). Dementsprechend wurde in der Variablen die Kategorisierung der ausgewählten Applikation eingetragen (Anhang AA Nr. 21 – 28).

Ferner wurde die Variable in SPSS aufgeteilt nach den Versuchspersonen eingetragen. Weiterhin wurde eine zusätzliche Variable hinzugefügt, welche festhält an welcher Stelle die von der Testperson ausgewählte Applikation in der Liste steht (RA_). Hierfür wurde wiederum manuell überprüft, an welcher Stelle die von der Testperson ausgewählte Applikation in der Liste stand und entsprechend in eine Excel-Tabelle eingetragen, um diese anschließend in SPSS zu übertragen (Anhang AA Nr. 953 – 960).

In der späteren Auswertung soll unter anderem überprüft werden, ob es einen Zusammenhang zwischen der Platzierung der Applikation im App-Markt und der Häufigkeit der Auswahl dieser Applikation gibt. Hierfür musste eine neue SPSS erstellt werden, weil diese Häufigkeiten nicht nach Personen, sondern nach Rang getrennt werden müssen (s. Tabelle 34, Anhang Y). Diese Tabelle gibt an, wie häufig die Applikation eines Szenarios auf einem bestimmten Rang installiert wurde.

6.7.4 Interview

Das Interview, welches direkt nach dem Experiment zur Auswahl der Applikationen stattgefunden hat, wurde mit Hilfe eines Diktiergerätes der Marke *Youthink* aufgezeichnet. Anschließend wurde das Gespräch mit Hilfe einer Word-Vorlage transkribiert. Die Vorlage enthielt die entsprechenden Fragen,

die vom Studienleiter gestellt wurden, sodass nur noch die Antworten der Teilnehmenden unter den entsprechenden Fragen eingefügt werden mussten. Für das Abspielen der Audiodateien wurde der VLC media player der Version 3.0.7 *Vetinari* genutzt.

Die Datenaufbereitung und die Auswertung der Ergebnisse der Interviews wurden im Rahmen einer Bachelorarbeit „Einfluss einer Datenschutzskala auf das Auswahlverhalten in einem App-Markt“ von Herrn Stefan Wichmann durchgeführt.

Die Transkription der Interviews wurde nach den Regeln von Dresing und Pehl (2020) und Krüger und Riemeier (2014) mit Hilfe der Software MAXQDA 2020 von VERBI durchgeführt.

Dabei wurden die Teilnehmenden hinsichtlich ihrer Motive für die Auswahl der Applikation in drei Gruppen unterteilt:

- Gruppe 1: Teilnehmende, welche die Datenschutzskala als das wichtigste Auswahlmotiv erachteten
- Gruppe 2: Teilnehmende, welche die Datenschutzskala als zweit- oder drittwichtigstes Merkmal erachteten
- Gruppe 3: Teilnehmende, bei denen die Datenschutzskala keinen Einfluss auf die Auswahl ihrer Entscheidung hatte

Anschließend wurden die Transkripte einer qualitativen Inhaltsanalyse nach Mayring (2015) durchgeführt. Dabei wurden die Interviews der 82 Teilnehmenden auf die Entscheidungsmotive untersucht. Ferner wurden die ersten drei wichtigsten Faktoren zur Auswahl der Applikation erfasst, wobei die Teilnehmenden meist nur einen Grund nannten. Ferner wurde eine verkürzte Form der Transkriptionen erstellt, welche nur wesentliche inhaltstragende Passagen enthielt. Dabei wurden irrelevante Aussagen und Wiederholungen gestrichen. Die verbliebenen Aussagen wurden anschließend durch einen induktiven als auch iterativen Prozess generalisiert und kodiert. Dabei wurde davon ausgegangen, dass gleiche Entscheidungsmotive von verschiedenen Teilnehmenden unterschiedlich verbalisiert wurden.

Von der Erhebung wurden einzelne Datensätze ausgeschlossen. Bei der Versuchsperson 4 wurde versehentlich das Szenario der Fitness übersprungen. Bei der Versuchsperson 6 war die Aufnahmedatei beschädigt. Die Versuchsperson 13 nannte trotz der mehrfachen Nachfrage keine Motive. In der Aufnahmedatei der Versuchsperson 41 war die Datei des Szenarios der Spiele nicht erhalten. Bei der Versuchsperson 69 stimmte die angegebene Applikation mit der genannten nicht überein.

In der Auswertung der Szenarien Messenger, Videokonferenz, E-Mail und Musik wurden somit Auswahlgründe von 82 Personen miteinbezogen, während in den Szenarien Wetter, Fitness und Spiele Auswahlgründe von 81 Personen und in dem Szenario der Nachrichten von 80 Personen der insgesamt 82 Teilnehmenden eingeflossen sind.

6.8 Ergebnisse

In dem folgenden Kapitel werden die Ergebnisse der durchgeführten Studie zum Einfluss der Datenschutzskala auf das Auswahlverhalten im App-Markt aufgezeigt. Das erste Unterkapitel beinhaltet die demografischen Daten der Teilnehmenden, während das zweite Unterkapitel die Ergebnisse beinhaltet, welche aus dem Eye-Tracking-Video entnommen werden können. Darunter fallen unter anderem der Vergleich der Entscheidungszeiten zwischen den Szenarien, sowie der Vergleich der Fixationszeiten zwischen den Gruppen. In dem dritten Unterkapitel wird die Häufigkeit der ausgewählten Applikationen, die den Teilnehmenden zur Verfügung standen, aufgeführt. Die Angemessenheit der Applikationsauswahl wird in dem vierten Unterkapitel zwischen den Gruppen verglichen. Hierbei wird darauf geachtet, ob die Teilnehmenden unterschiedlicher Gruppen bedingt durch den Informationsgehalt bezüglich des Datenschutzes unterschiedliche Applikationen gewählt haben. Im fünften Unterkapitel werden die Aussagen, die innerhalb des Interviews während der Videokonfrontation getätigt wurden, dargestellt und die Häufigkeiten der kategorisierten Aussagen aufgezeigt. Anschließend werden im sechsten Unterkapitel die Ergebnisse des Fragebogens vorgestellt. Dabei umfassen die Ergebnisse die Häufigkeiten der Bekanntheit der Applikationen, die Bewertung der Datenschutzskala, die Einfachheit der Auswahl, die Vertrauenswürdigkeit der Applikationen, die alltäglichen Bedenken der Nutzenden mobiler Endgeräte im Bereich der Privatsphäre sowie den Vergleich der Relevanz verschiedener Applikationsbewertungsmethoden. Schließlich wird der Zusammenhang zwischen der Auswahl der Applikation und den Bedenken über den Datenschutz geprüft. Bei der Inferenzstatistik wurde erneut von einem Signifikanzniveau kleiner .05 ausgegangen, sofern kein anderes Signifikanzniveau angegeben wurde.

6.8.1 Demographie der Teilnehmenden

Insgesamt nahmen 82 deutschsprachige Personen an der Laborstudie teil. Die Alterspanne liegt bei der Stichprobe zwischen 18 und 68 Jahren mit einem Durchschnitt von $M = 32{,}15$ und einer Standardabweichung von $SD = 11{,}37$. Darüber hinaus sind 43 Teilnehmer männlich und 38 Teilnehmerinnen weiblich. Eine Person identifiziert sich dabei als weder männlich noch weiblich (s.

Tabelle 35, Anhang Y). Der Bildungshintergrund variiert von der Mittelschule bis zu höheren akademischen Graden: Sechs haben die Mittelstufe erreicht, 28 haben ein Abitur, sieben weitere haben eine Berufsausbildung abgeschlossen, während 41 einen höheren akademischen Abschluss von Universitäten besitzen (s. Tabelle 36, Anhang Y). Dabei verbringen sechs Personen mehr als 30 Minuten, 25 Personen mehr als 1 Stunde, 37 Personen mehr als 2 Stunden und 13 Personen mehr als 5 Stunden mit ihrem Smartphone (s. Tabelle 37, Anhang Y).

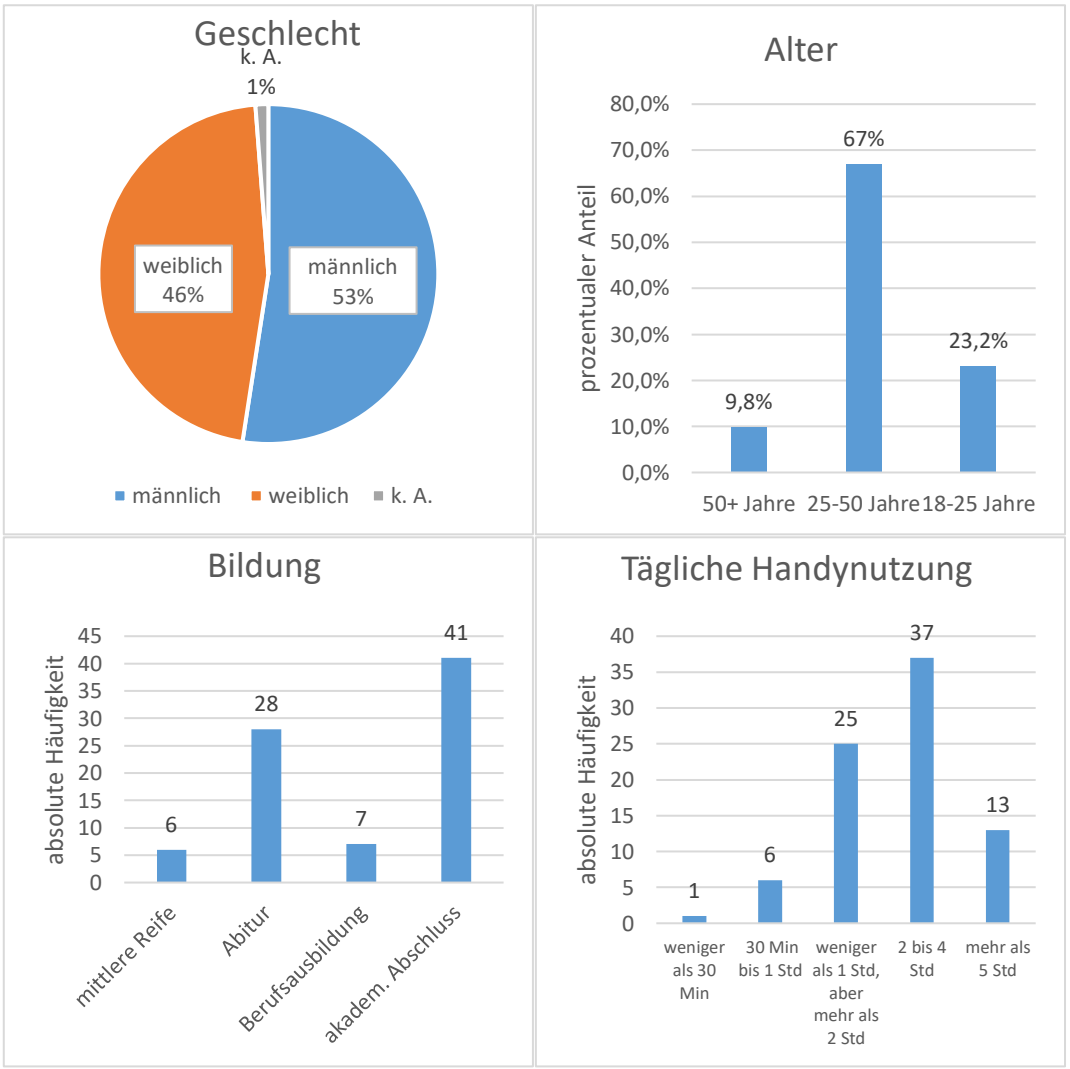


Abbildung 18. Verteilung des Geschlechtes, des Alters, der Bildung und der Handynutzung der Stichprobe.

Die Verteilungen der Daten sind zur besseren Veranschaulichung in Abbildung 18 illustriert. Die Aussage „Ich habe eine große Affinität zur Technik“ beantwortete lediglich eine teilnehmende Person als überhaupt nichtzutreffend. Zwei Personen geben an, dass die Aussage nichtzutreffend ist, während 34 Personen und somit die Mehrheit angibt, dass diese Aussage eher nicht zutreffe. Elf Personen gaben eine neutrale Antwort „weder noch“ an. Bei 24 Personen trifft die Aussage zu, während diese bei zehn

Personen völlig zutrifft. Keiner der Teilnehmenden gab an, dass die Aussage eher zutrifft (s. Tabelle 38, Anhang Y).

Bezüglich der Aussage „Mir ist der Schutz meiner Privatsphäre wichtig“ gab eine Person (1,2 %) an, dass diese Aussage nicht zutrifft, während 32 Teilnehmende (39,5 %) angaben, dass diese Aussage eher nicht zutrifft. Drei Teilnehmende (3,7 %) gaben eine neutrale Antwort („weder noch“). Insgesamt 23 Teilnehmende (28,4 %) gaben an, dass diese Aussage zutrifft, währen 22 Teilnehmende (27,2 %) angaben, dass diese Aussage völlig zutrifft (s. Tabelle 39, Anhang Y).

Bei der Frage, ob die Teilnehmenden aktiv sind, um ihre Daten zu schützen, haben insgesamt 25 Teilnehmende (30,9 %) angegeben dies zu tun, während 23 Teilnehmende (28,4 %) angaben, den aktiven Schutz der Daten zu unterlassen. Acht Teilnehmende (9,9 %) gaben an, eine Applikation zum Schutz ihrer Daten installiert zu haben, während 49 Teilnehmende (60,5 %) angaben, so wenige Daten wie möglich von ihrer Person preiszugeben. Die AGBs zu lesen, bevor eine Applikation installiert wird, gaben 17 Teilnehmende (21,0 %) an (s. Tabelle 39, Anhang Y).

Darüber hinaus wurde im Freitextfeld von einer Versuchsperson angegeben, dass das Gefühl existiere, aus Nachlässigkeit mehr preiszugeben, als man sollte. Eine weitere Person gab an, sich Rezensionen zum Datenschutz bezüglich bestimmter Applikationen von fachkündigen Personen durchzulesen. Ein Teilnehmer gab an, ausschließlich Applegeräte zu nutzen, um seine Daten zu schützen. Eine weitere Methode zum Schutz der Daten, die angegeben wurde, ist die Überprüfung der geforderten Zugriffsberechtigungen vor der Installation.

6.8.2 Eye-Tracking-Video

In den folgenden Kapiteln werden die Ergebnisse aus den Eye-Tracking-Videos vorgestellt. Aufgrund der Tatsache, dass einige Teilnehmende Sehhilfen benötigten, konnten bei diesen keine Eye-Tracking-Videos erstellt werden, welche genügend Qualität für eine Auswertung hatten. Somit wurden diese Teilnehmenden in den Ergebnissen für das Eye-Tracking-Video nicht weiter berücksichtigt. Aus diesem Grund erfolgt zunächst eine erneute Präsentation der demographischen Daten der Teilnehmenden mit auswertbarem Video. Anschließend werden die Entscheidungszeiten zwischen den Szenarien sowie zwischen den Gruppen verglichen. Darüber hinaus werden die Differenzen der Entscheidungszeiten der Applikationen in chronologischer Reihenfolge verglichen. Abschließend erfolgt ein Vergleich der Fixationszeiten und der Fixationswechsel unter den Gruppen.

6.8.2.1 Demographie der Teilnehmenden im Eye-Tracking-Video

Von den insgesamt 82 Teilnehmenden können 72 Eye-Tracking-Videos ausgewertet werden. In acht Fällen ist eine Auswertung der Videos nicht möglich, weil die teilnehmenden Personen eine Sehhilfe benötigten, um die gestellten Aufgaben adäquat absolvieren zu können. Bei einer Person kann die Videodatei nicht aufgefunden werden.

Das Alter der Stichprobe, bei der eine Videoauswertung durchgeführt werden konnte, hat eine Spanne von 18 bis 62 Jahren sowie einen Mittelwert von 30,5 Jahren (*SD* = 9,403). Unter den 72 Teilnehmenden befinden sich 35 männliche und 36 weibliche sowie eine Person, die sich weder als weiblich noch als männlich identifiziert. Nach der Auswertung ist die Verteilung der Stichprobe auf die einzelnen Gruppen wie folgt: Gruppe A umfasst 18 Teilnehmende, davon sind acht männlich und zehn weiblich. Der Mittelwert des Alters beträgt 27,78 Jahre (*SD* = 4,532). Die Gruppe B umfasst 16 Teilnehmende, davon sind fünf männlich und elf weiblich, wobei der Mittelwert des Alters 35,25 Jahre ist (*SD* = 13,051). Gruppe C umfasst 20 Teilnehmende, davon sind zwölf männlich und sieben weiblich zzgl. der Person, die sich als weder männlich noch weiblich identifiziert. Der Mittelwert des Alters liegt bei dieser Gruppe bei 30 Jahren (*SD* = 10,488). Gruppe D umfasst 18 Teilnehmende, davon sind zehn männlich und acht weiblich und der Mittelwert des Alters beträgt 29,56 Jahre (*SD* = 6,723) (s. Tabelle 40, Anhang Y).

6.8.2.2 Vergleich der Entscheidungszeiten zwischen den Szenarien

Werden die Entscheidungszeiten der einzelnen Szenarien untereinander verglichen, so fällt auf, dass für die Wahl der geeigneten Applikation im Szenario der Musik durchschnittlich am wenigsten Zeit mit *M* = 11,25 Sekunden (SD = 26,81) von den Teilnehmenden in Anspruch genommen wird. Mit nur einem geringen Unterschied ist die zweitgeringste Entscheidungszeit im Szenario der Videokonferenz mit *M* = 11,7 Sekunden (*SD* = 28,16) wiederzufinden. Am drittschnellsten kann sich im Szenario des Messengers mit *M* = 13,43 Sekunden (*SD* = 18,04) entschieden werden, wobei der Mittelwert der Entscheidungszeit des Szenarios des Wetters mit 17,01 Sekunden (*SD* = 18,12) knapp vier Sekunden über dem des Messengers liegt. Die Entscheidungszeit im Szenario der Nachrichten unterscheidet sich mit *M* = 17,54 Sekunden (*SD* = 20,73) nur wenig von der des Wetters. Im Szenario der Spiele beträgt die Entscheidungszeit *M* = 19,71 Sekunden (*SD* = 31,6), während die zweitlängste Zeit im Szenario der Fitnessapplikation mit *M* = 25,53 Sekunden (*SD* = 41,22) wiederzufinden ist. Die meiste Zeit benötigen die Teilnehmenden für die Auswahl der E-Mail-Applikation mit *M* = 28,24 Sekunden (*SD* = 47,2). Eine genaue Übersicht der Entscheidungszeiten ist in Tabelle 41 im Anhang Y wiederzufinden.

Um zu überprüfen, ob die Mittelwerte der Entscheidungszeiten für die Applikation in den jeweiligen Szenarien einen signifikanten Unterschied aufweisen, wird aufgrund der Abwesenheit einer Normalverteilung bei allen Datensätzen der nicht-parametrische Friedman-Test für gepaarte Stichproben mit Messwiederholung (s. Tabelle 42, Anhang Y) angewandt. Dieser ergibt einen signifikanten Unterschied mit $\chi^2 = 105{,}79$; $p < .00$.

Ferner wird, um zu überprüfen, welche Szenarien sich signifikant voneinander unterscheiden, ein paarweiser Vergleich mit Hilfe des Wilcoxon-Tests für nicht-parametrische gepaarte Stichproben zwischen allen Szenarien durchgeführt.

Nach dem Durchführen von 28 Signifikanztestes kann bei 23 ein signifikanter Unterschied festgestellt werden (s. Tabelle 43, Anhang Y). Die Entscheidungszeit des Messengers unterscheidet sich dabei signifikant von allen anderen Szenarien (Videokonferenz ($z = -3{,}4$; $p < .000$; $r = 0{,}4$), Wetter ($z = -2{,}24$; $p < .025$; $r = 0{,}26$), E-Mail ($z = -3{,}628$; $p < .000$; $r = 0{,}42$), Musik ($z = -3{,}2$; $p < .001$; $r = 0{,}37$), Fitness ($z = -3{,}44$; $p < .001$; $r = 0{,}40$), Spiele ($z = -1{,}84$; $p < .065$; $r = 0{,}22$) und Nachrichten ($z = -2{,}12$; $p < .034$; $r = 0{,}25$)). Bei näherer Betrachtung der Ergebnisse bezüglich des Szenarios der Videokonferenz sind signifikante Unterschiede zwischen allen anderen Szenarien außer dem der Musik wiederzufinden (Wetter ($z = -4{,}16$; $p < .000$; $r = 0{,}49$), E-Mail ($z = -5{,}47$; $p < .000$; $r = 0{,}64$), Fitness ($z = -5{,}81$; $p < .000$; $r = 0{,}68$), Spiele ($z = -4{,}324$; $p < .000$; $r = 0{,}51$) und Nachrichten ($z = -4{,}01$; $p < .000$; $r = 0{,}47$)). Hinsichtlich des Szenarios des Wetters konnten signifikante Unterschiede in drei von fünf Szenarien identifiziert werden (E-Mail ($z = -2{,}21$; $p < .027$; $r = 0{,}26$), Musik ($z = -4{,}48$; $p < .000$; $r = 0{,}52$), Fitness ($z = -2{,}33$; $p < .002$; $r = 0{,}27$)). Betreffend das Szenario der E-Mail konnten drei signifikante Unterschiede in vier Vergleichen festgestellt werden (Musik ($z = -5{,}17$; $p < .000$; $r = 0{,}61$), Spiele ($z = -2{,}82$; $p < .005$; $r = 0{,}33$), Nachrichten ($z = -2{,}73$; $p < .006$; $r = 0{,}32$)). Bezüglich der Fitness-Applikation bleiben lediglich zwei Vergleiche offen, die sich beide als signifikant erwiesen (Spiele ($z = -3{,}19$; $p < .001$; $r = 0{,}37$), Nachrichten ($z = -3{,}02$; $p < .003$; $r = 0{,}35$)). Beim Vergleichen der Datensätze des Szenario Spiele mit dem der Nachrichten ergab sich keine Signifikanz.

6.8.2.3 Vergleich der Entscheidungszeiten zwischen den Gruppen

Bei näherer Betrachtung der gesamten Entscheidungszeiten aufgeteilt nach Gruppen ist zu erkennen, dass die Gruppe A mit $M = 18{,}08$ Sekunden ($SD = 24{,}58$) durchschnittlich am längsten benötigt, um sich für eine Applikation zur Bewältigung der vorgegebenen Aufgabe zu entscheiden. Gruppe C benötigt durchschnittlich $M = 17{,}87$ Sekunden ($SD = 24{,}61$), während die Gruppe D $M = 15{,}39$ Sekunden ($SD = 17{,}59$) benötigt. Bei Gruppe B ist die kürzeste Entscheidungszeit mit $M = 13{,}50$ Sekunden ($SD = 13{,}66$)

wiederzufinden (s Tabelle 44, Anhang Y). Weder der Kruskal-Wallis-Test (Kruskal & Wallis, 1952) (s. Tabelle 45, Anhang Y) für mehr als zwei ungepaarte Vergleiche noch der Mann-Whitney-U-Test (s. Tabelle 46, Anhang Y) für paarweise Vergleiche der Gruppen untereinander, können signifikante Unterschiede feststellen. Darüber hinaus wird ein paarweiser Vergleich der einzelnen Szenarien zwischen den Gruppen durchgeführt (s. Tabelle 47, Tabelle 48, Tabelle 49, Tabelle 50, Tabelle 51, Tabelle 52, Anhang Y). Hierbei können lediglich signifikante Unterschiede mit einem mittleren Effekt bezüglich des Szenarios Messenger zwischen den Gruppen A und D (U = 79; z = -2,626; p < .009; r = 0,4), bezüglich des Szenarios Fitness zwischen den Gruppen B und C (U = 98; z = -2,037; p < .04; r = 0,3) sowie zwischen den Gruppen C und D bezüglich der Szenarios Videokonferenz (U = 112,5; z = -1,974; p < .04; r = 0,3) und Musik (U = 110,5; z = -2032; p < .04; r = 0,3) festgestellt werden.

6.8.2.4 Vergleich der Differenzen der Entscheidungszeiten der Applikation in chronologischer Reihenfolge

Hinsichtlich der Differenzen der Entscheidungszeiten ist zu sehen, dass insgesamt zwischen den Entscheidungszeiten der ersten und der zweiten Applikation eine Differenz von 3,13 Sekunden (SD = 23,34) vorzufinden ist. Somit benötigen die Teilnehmenden durchschnittlich ca. 3 Sekunden weniger, um eine Entscheidung hinsichtlich der Applikationsauswahl zu treffen. Zwischen der zweiten und dritten Applikation (-0,34 Sekunden, SD = 18,25), der dritten und vierten Applikation (-1,58 Sekunden, SD = 17,50), der vierten und fünften Applikation (-1,78 Sekunden, SD = 27,71) und der fünften und sechsten Applikation (-5,31 Sekunden, SD = 22,99) konnte betrachtet werden, dass die Teilnehmenden stetig langsamer ihre Entscheidung bezüglich der Applikationsauswahl getroffen haben. Die Differenz der Entscheidungszeiten zwischen der sechsten und siebten Applikation (8,36 Sekunden, SD = 41,52) sowie der siebten und achten Applikation (3,81 Sekunden, SD = 31,20) zeigen einen deutlichen Anstieg der Differenz. Somit könnte die Vermutung aufgestellt werden, dass die Teilnehmenden weniger Zeit benötigt haben, um eine Auswahl zu treffen. Eine Übersicht der Mittelwerte der Differenzen der Entscheidungszeiten von allen Gruppen zusammen ist in Tabelle 53 im Anhang Y zu finden. Werden die Mittelwerte der Differenzen der Entscheidungszeiten zwischen den Gruppen verglichen, so fällt lediglich auf, dass zwischen der ersten und der zweiten Applikation in Gruppe A (M = 1,86; SD = 11,59), B (M = 17,21; SD = 26,47) und C (M = 5,10; SD = 12,06) jeweils ein positiver Wert zu finden ist, während in der Kontrollgruppe D (M = 10,3; SD = 31,3) ein negativer Wert zu sehen ist. Alle anderen Werte scheinen bei der ersten Betrachtung keine auffällige Struktur aufzuweisen und werden deshalb hier nicht einzeln genannt. Eine Übersicht der Mittelwerte, Standardabweichung und Normalverteilung ist aus der Tabelle 54 im Anhang Y zu entnehmen. Um zu überprüfen, ob der Unterschied dieser Mittelwerte zwischen den Gruppen signifikant ist, wurde zunächst ein Kruskal-Wallis-Test für nicht-

parametrische Datensätze angewandt. Der Kruskal-Wallis-Test zeigte lediglich ein signifikantes Ergebnis bei der Entscheidungszeit zwischen der ersten und zweiten Applikation mit $\chi^2 = 8{,}292$, $p < .04$. Nach der Bonferroni-Korrektur (Sedgwick, 2012), welche durchgeführt wird, um die Alphafehler-Kumulierung, die durch multiples Testen entsteht, zu neutralisieren, müsste allerdings ein *p*-Wert von .007 (das Signifikanzniveau von .05 wird durch die Anzahl von den Tests geteilt) unterschritten werden, was hier nicht der Fall ist (s. Tabelle 54, Anhang Y). Bei den paarweisen Vergleichen mit Hilfe des Mann-Whitney-U-Tests ergibt sich lediglich ein signifikanter Unterschied zwischen der Gruppe B und D ($U = 71$; $z = -2{,}52$; $p < .012$; $r = 0{,}43$) hinsichtlich der Differenz der Entscheidungszeit zwischen der ersten und der zweiten Applikation. Alle weiteren paarweise Vergleiche zeigen keine weiteren Signifikanzen auf und sind aus Tabelle 56, Tabelle 57, Tabelle 58, Tabelle 60 und Tabelle 61 im Anhang Y zu entnehmen.

Aufgrund der Robustheit des t-Tests, die in mehreren Studien bestätigt wird (Pagano, 2010; Salkind, 2010; Wilcox, 2011), wird ein weiterer paarweiser Vergleich zwischen allen Differenzen der Entscheidungszeiten über alle Gruppen durchgeführt. Auch hier lassen sich drei signifikante Unterschiede mit einem starken Effekt zwischen der Differenz der Entscheidungszeit der ersten und zweiten Applikation beim Vergleich der Gruppen A und B ($t(32) = -2{,}15$; $p < .044$; $r = 0{,}35$), B und D ($t(32) = 2{,}75$; $p < .01$; $r = 0{,}44$) sowie Gruppe C und D ($t(32) = 2{,}04$; $p < .049$; $r = 0{,}32$) feststellen. Alle weiteren paarweise Vergleiche zeigen keine weiteren Signifikanzen auf und sind aus Tabelle 62, Tabelle 63, Tabelle 64, Tabelle 65, Tabelle 66, Tabelle 67 im Anhang Y zu entnehmen.

6.8.2.5 Vergleich der Fixationszeiten

Durchschnittlich haben die Teilnehmenden 12,44 Sekunden (*SD* = 10,29) auf die Skala, 44,16 Sekunden auf den Text (*SD* = 26,71) und 18,22 Sekunden (*SD* = 19,29) auf das Symbol der Applikation geschaut.

Bezüglich der Skala ist beim Vergleich zwischen den Gruppen A (*M* = 12,46 Sekunden; *SD* = 12,06), B (*M* = 12,41; *SD* = 10,28) und C (*M* = 12,44; *SD* = 8,49) auf den ersten Blick kein nennenswerter Unterschied bezüglich der Zeit der Fixationen auf die Skala zu erkennen.

Bei näherer Betrachtung der Mittelwerte der Fixationszeiten auf das Symbol der Applikation im App-Markt ist die längste Fixationsdauer bei Gruppe A mit 22,1 (*SD* = 16,55) wiederzufinden, während Gruppe B mit 16,25 Sekunden (*SD* = 12,04) und Gruppe C mit 14,89 Sekunden (*SD* = 20,32) die niedrigsten Werte aufweisen. Die Teilnehmenden der Gruppe D haben durchschnittlich 19,78 Sekunden (*SD* = 25,6) investiert, um das Symbol zu betrachten und liegen somit zwischen den Mittelwerten von Gruppe A und B. Beim Betrachten der Fixationszeiten des Textes ist ein inverses

Verhalten zu beobachten. Gruppe A zeigt mit 35,54 Sekunden (*SD* = 25,27) die geringste Fixationszeit auf, während bei Gruppe B mit 44,47 Sekunden (*SD* = 26,97) und Gruppe C mit 50,48 (*SD* = 23,87) die längsten Fixationszeiten zu finden sind (s. Tabelle 68, Anhang Y).

Anschließend wird mit Hilfe des Kruskal-Wallis-Tests auf Signifikanz geprüft, wobei lediglich die Skala mit χ^2 = 39,415; p <.00 einen signifikanten Unterschied aufzeigt (s. Tabelle 69, Anhang Y). Nach der Prüfung auf Signifikanz mit Hilfe des Mann-Whitney-U-Tests kann jedoch lediglich ein signifikanter Unterschied mittleren Effektes beim Vergleich der Fixationszeiten zwischen Gruppe A und C bezüglich des Textes (*U* = 96,5; *z* = -2,441; *p* < .015; *r* = 0,4) identifiziert werden. Darüber hinaus ergeben sich signifikante Unterschiede beim Vergleich der Gruppen A, B und C mit der Gruppe D. Dies ist nicht weiter verwunderlich, weil bei Gruppe D keine Datenschutzskala im App Markt implementiert war und die Fixationszeiten in dieser Gruppe auf die Skala nicht existent sind (s. Tabelle 70, Tabelle 71, Tabelle 71, Tabelle 72, Tabelle 73, Tabelle 74, Tabelle 75, Anhang Y).

Ferner kann erfasst werden, dass der Eye-Tracker durchschnittlich *M* = 4,71 Sekunden (*SD* = 11,11) keine Blickbewegung aufnehmen konnte, weil es in diesem Moment nicht möglich war, die Pupillen zu erkennen. Gründe für dieses Problem war meistens das Tragen einer Sehhilfe, wie zum Beispiel einer Brille. Insgesamt *M* = 7,65 Sekunden (*SD* = 9,05) haben die Teilnehmenden ihren Blick von dem mobilen Endgerät abgewandt, während sie die Aufgabe erfüllten.

Weiterhin haben die Teilnehmenden durchschnittlich *M* = 6,45 Sekunden (*SD* = 9,40) die Suchzeile fokussiert, während sie lediglich *M* = 1,38 Sekunden (*SD* = 3,89) ihren Fokus auf die Tastatur gerichtet haben. Die Tasten werden mit *M* = 0,22 Sekunden (*SD* = 0,87) für die Apptaste, *M* = 0,32 Sekunden (*SD* = 1,14) für die Hometaste und *M* = 0,51 Sekunden (*SD* = 2,04) für die Zurücktaste nur sehr kurz besehen. Die Vorschaubilder der Applikation, nachdem diese ausgewählt wurde, werden durchschnittlich *M* = 9,39 Sekunden (*SD* = 15,67) betrachtet. Für das Lesen der Rezensionen werden insgesamt *M* = 25,25 Sekunden (*SD* = 75,24) benötigt. Die nachfolgenden Ergebnisse beziehen sich nicht auf die reinen Fixationszeiten, sondern auf die Dauer einer Tätigkeit, welche die Teilnehmenden benötigt bzw. in Anspruch genommen haben, um die vorgegebene Aufgabe zu erfüllen. Insgesamt haben die Teilnehmenden *M* = 46,68 (*SD* = 30,03) Sekunden benötigt, um den Suchbegriff in die Suchleiste einzugeben. Auf der Oberfläche, auf der die Diagramme angezeigt wurden, um einzusehen, auf welche Rechte die Applikation zugreift und wie hoch die Wahrscheinlichkeit ist, dass aus den daraus gesammelten Informationen weitere persönliche Daten extrahiert werden können, befanden sich die Teilnehmenden lediglich *M* = 4,55 Sekunden (*SD* = 19, 97). In dem Fenster, welches angezeigt wurde, nachdem eine Applikation ausgewählt wurde, befinden sich die Teilnehmenden durchschnittlich *M* = 51,66 Sekunden (*SD* = 43,89). In diesem Fenster hatten sie die Möglichkeit, anschließend eine

Applikation zu installieren oder die Bilder und Rezensionen anzuschauen. Nach dem Anklicken des Installationsknopfes bis zur Eingabe des neuen Stichwortes werden die Tätigkeiten nicht genauer erfasst. Dieser Abschnitt umfasste durchschnittlich *M* = 794,73 Sekunden (*SD* = 176,06).

Die eben genannten Fixationszeiten sowie die Zeiten der genannten Tätigkeiten sind in Tabelle 76 im Anhang Y einzusehen. Darüber hinaus wurden die Zeiten nach den Gruppen aufgeteilt und sind ebenfalls der Tabelle 76 im Anhang Y zu entnehmen.

Nach der Durchführung eines Kruskal-Wallis-Tests, um zu ermitteln, ob ein signifikanter Unterschied zwischen den eben genannten Zeiten unter den Gruppen verzeichnet werden kann, resultieren signifikante Ergebnisse in den Zeiten „kein Signal“ mit χ^2 = 9,112; p <.02, „Leerlauf“ mit χ^2 = 10,53; p <.015, „Zurücktaste“ mit χ^2 = 8,498; p <.037 und „Diagramm“ mit χ^2 = 11,548; p <.009. Allerdings können diese Ergebnisse nach der Anwendung der Bonferroni-Korrektur mit p < .004 nicht mehr als signifikant angesehen werden (s. Tabelle 77, Anhang Y).

6.8.2.6 Vergleich der Anzahl der Fixationswechsel auf die jeweiligen Gebiete nach Gruppen

Durchschnittlich finden *M* = 19,54 Fokuswechsel (*SD* = 20) auf die Skala statt. Die Anzahl der Fokuswechsel wird gezählt, indem die Testperson den Blick auf das jeweilige Gebiet richtet. Wendet die Versuchsperson den Blick ab und refokussiert das Gebiet, so steigt die Anzahl der Fixationswechsel und wird wie bereits in Abschnitt 6.7.3.3 in die Spalte K der Auswertungstabelle eingetragen. Auf den Text finden durchschnittlich *M* = 50,56 Fokuswechsel (*SD* = 30,41) statt, während auf das Symbol *M* = 30,71 Fokuswechseln (*SD* = 23,20) stattfinden.

Bezüglich der Skala ist beim Vergleich zwischen den Gruppen A (*M* = 24,78 Sekunden; *SD* = 20,13), B (*M* = 27,71; *SD* = 20,64) und C (*M* = 26,80; *SD* = 17,54) auf den ersten Blick ein Unterschied zwischen Gruppe A und B von etwa drei Fokuswechseln zu sehen, während zwischen Gruppe B und C lediglich ein Unterschied von knapp einem Fokuswechsel erfasst werden kann. Zwischen Gruppe A und C beträgt der Unterschied folglich etwa zwei Fokuswechsel.

Bei näherer Betrachtung der Mittelwerte der Fokuswechsel auf das Symbol der Applikation im App-Markt ist die höchste Anzahl an Wechseln, wie schon bei der Fixationsdauer, bei Gruppe A mit 39,94 Fokuswechseln (*SD* = 27,73) wiederzufinden, während Gruppe B 30,47 Fokuswechsel (*SD* = 16,55) und Gruppe C 31,50 Fokuswechsel (*SD* = 39,95) aufweisen. Die Teilnehmenden der Gruppe D verzeichnen durchschnittlich 22,17 Fokuswechsel (*SD* = 13,23) und somit die geringste Anzahl an Fokuswechseln auf das Symbol. Betrachten wir die Fokuswechsel auf den Text, so ist lediglich zu beobachten, dass die

Gruppe B mit 61,24 Fokuswechseln (SD = 38,05) die höchste Anzahl an Wechseln zeigt, während die Gruppe C mit 60,70 (*SD* = 31,75) nur knapp weniger Fokuswechsel aufzeigt. Gruppe A wendet durchschnittlich 54,56 Fokuswechsel (*SD* = 35,27) für den Text auf, während bei Gruppe D mit *M* = 31,06 (*SD* = 11,34) die geringsten Fokuswechsel zu finden sind. Eine Übersicht alle Mittelwerte ist in Tabelle 78 im Anhang Y einzusehen.

Nach der Durchführung eines Kruskal-Wallis-Tests, um zu ermitteln, ob ein signifikanter Unterschied zwischen den eben genannten Fixationswechseln unter den Gruppen verzeichnet werden kann, resultierten signifikante Ergebnisse in den Kategorien „kein Signal“ mit $\chi^2 = 8{,}85$; $p < .03$, „Text“ mit $\chi^2 = 14{,}229$; $p < .003$ „Leerlauf“ mit $\chi^2 = 10{,}124$; $p < .018$, „Zurücktaste“ mit $\chi^2 = 7{,}651$; $p < .054$, „Tastatur“ mit $\chi^2 = 7{,}644$; $p < .054$ und „Diagramm“ mit $\chi^2 = 10{,}604$; $p < .014$. Nach der Anwendung der Bonferroni-Korrektur mit $p < .003$ kann lediglich bei den Fixationswechseln auf den Text ein signifikantes Ergebnis festgestellt werden (s. Tabelle 79, Anhang Y).

Nach der Prüfung auf Signifikanz mit Hilfe des Mann-Whitney-U-Tests können signifikante Unterschiede mittleren Effektes beim Vergleich der Fixationszeiten zwischen Gruppe A und B bezüglich der Kategorie „kein Signal“ ($U = 75$; $z = -2{,}525$; $p < .012$; $r = 0{,}43$), „Bilder“ ($U = 65$; $z = -2{,}325$; $p < .02$; $r = 0{,}39$) und „Rezension/Bewertung“ ($U = 63{,}5$; $z = -2{,}849$; $p < .004$; $r = 0{,}48$) identifiziert werden. Darüber hinaus ergeben sich signifikante Unterschiede beim Vergleich der Gruppen A, B und C mit der Gruppe D (s. Tabelle 80, Anhang Y).

Weiterhin können sechs signifikante Unterschiede eines mittleren Effektes zwischen den Gruppen A und D in den Kategorien „kein Signal“ ($U = 93{,}5$; $z = -2{,}235$; $p < .025$; $r = 0{,}37$), „Symbol“ ($U = 82$; $z = -2{,}533$; $p < .011$; $r = 0{,}42$), „Text“ ($U = 69$; $z = -2{,}944$; $p < .003$; $r = 0{,}49$), „Leerlauf“ ($U = 81$; $z = -2{,}568$; $p < .01$; $r = 0{,}42$), „Zurücktaste“ ($U = 97{,}5$; $z = -2{,}694$; $p < .007$; $r = 0{,}44$) und „Hometaste“ ($U = 115{,}5$; $z = -2{,}132$; $p < .033$; $r = 0{,}35$) festgestellt werden (s. Tabelle 81, Anhang Y).

Zwischen den Gruppen B und C können insgesamt fünf signifikante Unterschiede mittleren Effekts in den Kategorien „Tastatur“ ($U = 105{,}5$; $z = -2{,}307$; $p < .021$; $r = 0{,}37$), „Diagramm“ ($U = 118$; $z = -2{,}329$; $p < .02$; $r = 0{,}38$), „AuswahlApp“ ($U = 103{,}5$; $z = -2{,}033$; $p < .042$; $r = 0{,}33$), „Bilder“ ($U = 98{,}5$; $z = -2{,}193$; $p < .028$; $r = 0{,}36$) und „Rezension/Bewertung“ ($U = 79{,}5$; $z = -2{,}809$; $p < .005$; $r = 0{,}46$) ermittelt werden (s. Tabelle 82, Anhang Y).

Insgesamt vier signifikante Unterschiede mittleren Effektes sind in den Kategorien „Leerlauf“ ($U = 90{,}5$; $z = -2{,}62$; $p < .009$; $r = 0{,}42$), „Zurücktaste“ ($U = 115$; $z = -2{,}551$; $p < .011$; $r = 0{,}41$), „Apptaste“ ($U = 125{,}5$; $z = -2{,}24$; $p < .025$; $r = 0{,}36$) und „Tastatur“ ($U = 122{,}5$; $z = -1{,}99$; $p < .047$; $r = 0{,}32$)

wiederzufinden. Ein signifikanter Unterschied starken Effekts ist in der Kategorie „Text“ (U = 68; z = -3,277; p < .001; r = 0,53) zu sehen (s. Tabelle 83, Anhang Y).

Der letzte paarweise Vergleich zwischen den Gruppen B und D weist zwei signifikante Unterschiede mittleren Effektes auf. Dazu zählen die Kategorien „Text“ (U = 65,5; z = -2,891; p < .004; r = 0,48) und „Apptaste“ (U = 106,5; z = -2,203; p < .028; r = 0,37) (s. Tabelle 84, Tabelle 85, Anhang Y). Die Datensätze, die bei einem paarweisen Vergleich in beiden Fällen eine Normalverteilung aufzeigen, werden anschließend mit Hilfe des parametrischen t-Testes auf Signifikanz geprüft. Hierbei werden lediglich zwei signifikante Unterschiede eines starken Effektes zwischen den Gruppen A und D in der Kategorie „Symbol“ (t(35) = 2,689; p < .011; r = 0,41) und zwischen den Gruppen B und D in der Kategorie „Text“ (t(35) = 3,141; p < .005; r = 0,48) gefunden (Tabelle 86, Anhang Y).

6.8.3 Ergebnisse ausgewählter Applikationen

In Tabelle 87 im Anhang Y wird eine Übersicht von den Häufigkeiten der ausgewählten Apps gezeigt. Anhand dieser Tabelle ist zu erkennen, dass im Szenario Messenger von 82 Teilnehmenden 52 (63,4 %) die Applikation WhatsApp gewählt haben. In dieser Kategorie haben neun Teilnehmende (11 %) die Applikation FacebookMessenger und sieben Teilnehmende (8,5 %) die Applikation Telegramm gewählt. Die Applikation Hangouts, Wire und Line werden in dieser Kategorie von niemandem gewählt. In dem Szenario der Videokonferenz wird sich 49-mal (72 %) für die Applikation Skype und 14-mal (17,1 %) für die Applikation Viber entschieden. Nur ein bis zweimal werden die Applikationen Imo (1,2 %), TrueConf (2,4 %), Facebook Messenger (2,4 %), Kik (1,2 %), JusTalk (1,2 %), und Hangouts (2,4 %) gewählt. Für die Applikationen ZOOM, Glide, Tango, Google Duo und VideoCall Free wird sich nicht einmal entschieden.

Bei der Betrachtung des Szenarios des Wetters ist zu sehen, dass die Applikationen Wetter-Online 22-mal (26,8 %), Wetter.com 21-mal (25,6 %), Wetter.de 18-mal (22 %) und Morecast (UBIMET) 16-mal (19,5 %) gewählt werden. Die Applikationen WeatherZone, BayerAgrarWetter und Yr werden ein bis zweimal gewählt. Alle weiteren Applikationen (Yahoo Wetter, AccuWeather, Weather Live, Windy.com) werden nicht einmal gewählt.

Innerhalb des E-Mail-Szenarios wird die Applikation Outlook 40-mal mit 48,8 %, die Appllikation OpenMail 18-mal (22 %) und die Applikation Spark neunmal (11 %) gewählt. Die Applikationen BlueMail, Nine, K9Mail, E-Mail-MailChecker werden lediglich ein- bis viermal gewählt, wobei die Applikationen Maildroid und MyMail nicht gewählt werden.

Bezüglich des Szenarios Musik lässt sich feststellen, dass sich 61 Teilnehmende für die Applikation Spotify (74,4 %) und 18 Teilnehmende sich für die Applikation Soundcloud (22 %) entschieden haben. Die Applikationen Freie Musik MH Musik, Gratis Musik und Deezer werden nur einmal gewählt, während alle weiteren Apps (Free Music, Google Play, SongFlip, Audiomack und Musikspieler) nicht einmal für die Erfüllung der Aufgabe ausgewählt werden.

In der Kategorie Fitness haben 32 Teilnehmende (39 %) die Applikation Schrittzähler- Gratis Pedometer & Kalorienzähler und 25 Teilnehmende (30,5 %) die Applikation FitBit gewählt. Alle weiteren Applikationen (Wandern Schrittzähler Diät, Google Fit, Strava Training, Sportractive workout, Pacer Health Schrittzähler & Abnehmtrainer, Laufen zur Gewichtsabnahme, Endomondo) werden siebenmal oder weniger für die Erfüllung der Aufgabe genutzt.

In der Kategorie Spiele haben sich 38 Teilnehmende (46,3 %) für die Applikation Sudoku Free (Titan Inc Geduldsspiele) und 21 Teilnehmende (25,6 %) für die Applikation Sudoku classic (Quarzo Apps) entschieden. Alle weiteren Apps (Sudoku 2 (Magma Mobile), Sudoku (Volcano Entertainment), Sudoku (Card Games), Sudoku Master (Dat Viet Entertainment), Sudoku (Timeglass Works), Material Sudoku (OkayCode), Sudoku kostenlos deutsch (Marco Meyer)) werden ein- bis neunmal gewählt. Die Applikation Sudoku puzzle wird nicht einmal gewählt.

In der letzten Kategorie der Nachrichten ist zu sehen, dass die Applikation Die Zeit 51-mal mit 62,2 % gewählt wird. Alle weiteren Kategorien (Microsoft News, BBC News, CNN Braking News, News Suite, FlipBoard, Euronews, RT News) werden ein- bis achtmal gewählt, wobei Squid und GoogleNews nicht einmal gewählt werden.

6.8.4 Angemessenheit der Applikationsauswahl (Score- Vergleich)

Es wird davon ausgegangen, dass die Implementierung einer Datenschutzskala in einem App-Markt zu einer angemesseneren Auswahl einer Anwendung hinsichtlich der Datenschutzbewertung führt. Um das Auswahlverhalten in Bezug auf die neben der Applikation abgebildeten Datenschutzinformationen zu vergleichen, wird jeder Anwendung eine Bewertung entsprechend der Datenschutzkategorie von 1, was der Kategorie sehr kritisch entspricht, bis 5, was der Kategorie sehr sicher entspricht, gegeben. Nachdem die Mittelwerte für jede Gruppe von A bis D berechnet werden, können die höchsten Mittelwerte ausschließlich in Gruppe A (Messenger M = 3,10 , SD = 0,94; Videokonferenz M = 4,24 , SD = 0,54; Wetter M = 4,00 , SD = 1,00; E-Mail M = 4,10, SD = 0,94;) und Gruppe B (Musik M = 4,58, SD = 0,51; Fitness M = 4,83, SD = 0,71; Spiele M = 4,47 , SD = 1,07; Nachrichten M = 4,58 , SD = 1,07 ;) gefunden werden. Die niedrigsten Mittelwerte befinden sich mit Ausnahme von dem Szenario des

Messengers (Gruppe C, *M* = 2,61 , *SD* = 1,08) und der Videokonferenz (Gruppe B, *M* = 3,79 ,SD = 0,79) ausschließlich in Gruppe D (Wetter *M* = 2,63, *SD* = 0,96; E-Mail *M* = 3,00, *SD* = 0,67; Musik *M* = 3,89, *SD* = 0,74; Fitness *M* = 3,21, *SD* = 1,58; Spiele *M* = 3,05, *SD* = 1,03; Nachrichten *M* = 3,00, *SD* = 1,49;). Für den besseren Überblick werden die Ergebnisse in der Tabelle 88 im Anhang Y dargestellt.

Die Mittelwerte der Tabelle 89 im Anhang Y und der Abbildung 19 zeigen die Tendenz eines höheren Wertes bei den Gruppen mit Datenschutzskala als bei der Gruppe ohne Datenschutzskala. Dies lässt die Vermutung aufkommen, dass die Teilnehmenden mit einer Datenschutzskala Applikationen ausgewählt haben, die als weniger kritisch beziehungsweise als sicherer eingestuft wurden.

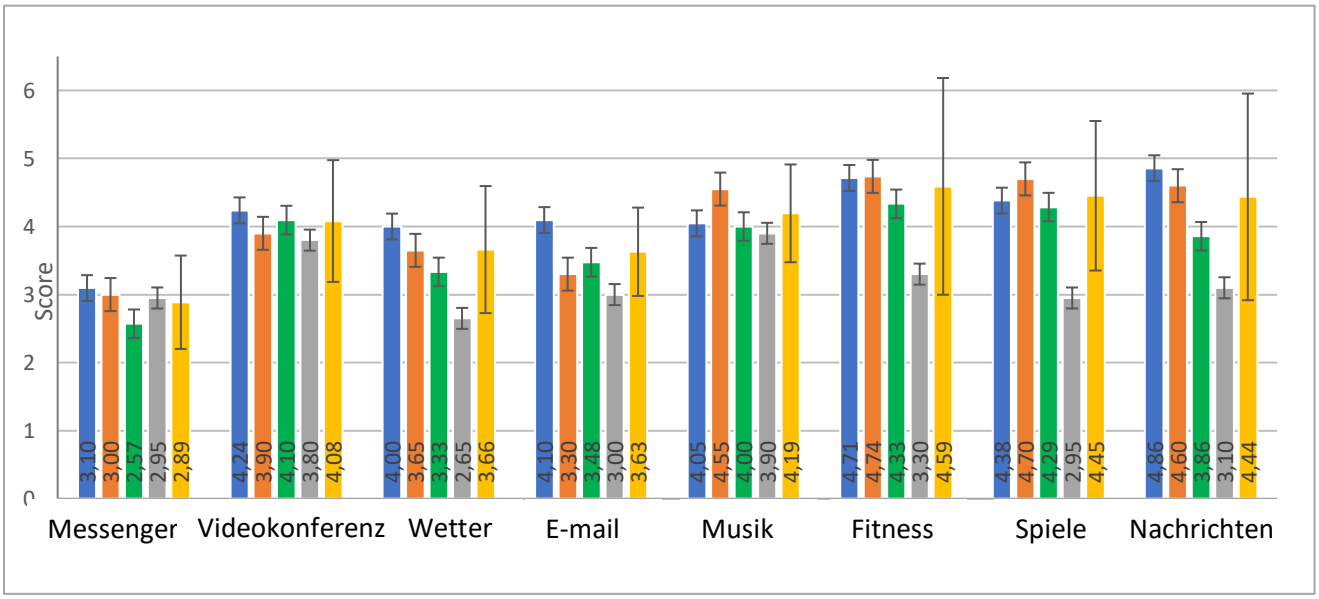


Abbildung 19. Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Gruppen sowie nach der Präsenz einer Datenschutzskala.

Diese Abbildung illustriert die Mittelwerte der Kategorien der Datenschutzskala, in die die ausgewählte Applikation eingeordnet wurde. Dabei spiegelt ein niedriger Mittelwert kritische Kategorien bezüglich des Datenschutzes und ein hoher Mittelwert sichere Kategorien des Datenschutzes wider. Die blauen Säulen enthalten die Datensätze der Gruppe A (Datenschutzskala mit Erläuterung; *n* = 21), die orangenen Säulen der Gruppe B (Datenschutzskala mit Erläuterung bei Nachfrage; *n* = 20), die grünen Säulen der Gruppe C (Datenschutzskala ohne Erläuterung; *n* = 21) und die grauen Säulen der Kontrollgruppe D (keine Datenschutzskala; *n* = 20). Die gelben Säulen bilden den Mittelwert aus den Gruppen A, B und C ab, sodass die Ergebnisse der Gruppen mit Datenschutzskala die der Gruppen ohne Datenschutzskala gegenübergestellt werden.

Um zu überprüfen, ob die Ergebnisse sich signifikant unterscheiden, wird zunächst ein Kolmogorov-Smirnov-Test auf Normalverteilung durchgeführt. Dieser ergibt, dass alle Datensätze von einer

Normalverteilung signifikant abweichen, sodass der nicht-parametrische Kruskal-Wallis-Test für mehr als zwei unabhängige Stichproben durchgeführt wird (s. Tabelle 90, Anhang Y). Dieser ergibt einen signifikanten Effekt bei den Applikationen in den Kategorien Wetter (χ^2 = 13,952; p < .003), E-Mail (χ^2 = 11,871; p < .008), Musik (χ^2 = 18,862; p < .000), Fitness (χ^2 = 18,649; p < .000), Spiele (χ^2 = 20,925; p < .000) und Nachrichten (χ^2 = 20,926; p < .000). Lediglich bei den Werten der Kategorien Messenger und Wetter kann kein signifikanter Unterschied festgestellt werden. Anschließend werden die ersten drei Gruppen zu einer Gruppe zusammengefasst, um einen Mann-Whitney-U-Test (s. Tabelle 91, Anhang Y) durchzuführen, der zwei Verteilungen auf signifikante Unterschiede überprüft. Der Test zeigt signifikante Unterschiede bei denselben Kategorien, die auch schon bei dem Kruskal-Wallis-Test als signifikant eingestuft wurden: Wetter (U = 564; z = -3,342; p < .001), E-Mail (U = 397; z = -2,627; p < .009), Musik (U = 477; z = -2,031; p < .042), Fitness (U = 332; z = -3,778; p < .000), Spiele (U = 212; z = -4,951; p < .000) und Nachrichten (U = 336; z = -3,776; p < .000).

Darüber hinaus werden die einzelnen Gruppen untereinander mit Hilfe des Mann-Whitney-U Tests auf signifikante Unterschiede untersucht. Beim Vergleich zwischen den Gruppen A und B (s. Tabelle 92, Anhang Y) kann lediglich ein signifikanter Unterschied in den Applikationskategorien E-Mail (U = 132; z = -1,92; p < .055), Videokonferenz (U = 139; z = -2,092; p < .036) und Musik (U = 93,5; z =-3,616; p < .000) gefunden werden. Beim Vergleich der Gruppen A und C (s. Tabelle 93, Anhang Y) wird lediglich ein signifikanter Unterschied in der Applikationskategorie Nachrichten (U = 169; z = -2,421; p < .015) festgestellt. Beim Vergleich der Gruppen A und D (Tabelle 94, Anhang Y) wird in den Kategorien Wetter (U = 69; z = -3,637; p < .000), E-Mail (U = 76; z = -3,*705*; p < .000), Fitness (U = 93,5; z = -3,251; p < .000), Spiele (U = 75,5; z = -3,6; p < .000) und Nachrichten (U = 73, z = -4,00; p < .000) ein signifikanter Unterschied festgestellt. Dieselben Applikationskategorien sind beim Kruskal-Wallis-Test ebenfalls signifikant, wobei dieser zusätzlich eine Signifikanz bei Musik aufzeigt.

Weiterhin kann beim Vergleich der Gruppen B und C lediglich ein signifikanter Unterschied (s. Tabelle 95, Anhang Y) der Kategorie Musik (U = 131,5; z = -2,524; p < .012) festgestellt werden. Beim Vergleich der Gruppen B und D (s. Tabelle 96, Anhang Y) werden in den Kategorien Wetter (U = 94,5; z = -2,602; p < .009), Musik (U = 81,5; z = -3,494; p < .000), Fitness (U = 73; z = -3,504; p < .000), Spiele (U = 63,5; z = -3,683; p < .000) und Nachrichten (U = 81; z = -3,259; p < .001) signifikante Unterschiede gefunden. Der letzte Vergleich zwischen den Gruppen C und D ergibt einen signifikanten Unterschied in den Kategorien Fitness (U = 132,5; z = -2,389; p < .017) und Spiele (U = 90,5; z = -3,527; p < .000) (Tabelle 97, Anhang Y).

Um zu prüfen, ob die Technikaffinität der Teilnehmenden, die im Abschnitt 6.8.1 aufgezeigt wird, einen Einfluss auf die Adäquatheit der Auswahl der Applikation hat, wird aufgrund der Abwesenheit einer

Normalverteilung ein weiterer Spearman-Rho-Test durchgeführt. Hierbei können keine signifikanten Ergebnisse gefunden werden (s. Tabelle 98, Anhang Y).

Ferner wird ebenfalls auf weitere Zusammenhänge zwischen der Adäquatheit der Auswahl der Applikation und dem Geschlecht, dem Alter, dem Bildungsabschluss, der Privatsphäre und den Stunden der Nutzung eines Endgerätes geprüft. Hierbei konnten jedoch keine signifikanten Ergebnisse festgestellt werden.

6.8.5 Interview

Wie schon in der Datenaufbereitung der Interviews im Abschnitt 6.7.4 erwähnt, wurde auch die Berechnung der folgenden Ergebnisse im Rahmen der Bachelorarbeit von Herrn Wichmann durchgeführt.

Zunächst werden die Entscheidungsmotive bei Auswahlverfahren der Applikation vorgestellt und deren Häufigkeiten aufgezeigt. Anschließend wird der Vergleich der Adäquatheit der Applikationsauswahl getrennt nach den Entscheidungsmotiven beziehungsweise nach der Relevanz der Datenschutzskala als Entscheidungsmotiv präsentiert.

6.8.5.1 Entscheidungsmotive bei Auswahlverfahren der Applikation

Durch die zusammenfassende qualitative Inhaltsanalyse nach Mayring (2015) ergeben sich nach Anwendung der induktiven-iterativen Vorgehensweisen zwölf Motive, die ausschlaggebend für die Auswahl einer bestimmten Applikation sind:

1. Datenschutzskala: für viele Teilnehmende ist die Datenschutzskala eine wichtige und hilfreiche Entscheidungsgrundlage, vor allem wenn die Auswahl ausschließlich aus den Teilnehmenden unbekannten Applikationen besteht.
2. Bekannt aus eigener Nutzung: dieses Entscheidungsmotiv wird den Teilnehmenden zugewiesen, wenn diese angeben, die Applikation bereits zu nutzen oder genutzt zu haben.
3. Bekannt, aber nicht selbst genutzt: bei diesem Entscheidungsmotiv berichten die Teilnehmenden über die Bekanntheit des Namens, des Symbols und des Herausgebers der Applikation, auch wenn die Applikation noch nicht selbst genutzt wurde.

4. Verbreitung im Umfeld: dieses Entscheidungsmotiv wird gewählt, wenn die Verbreitung der Applikation im Familien-, Freundes- und Bekanntenkreis für die Auswahl seitens der Teilnehmenden angegeben wird.
5. Reihenfolge im App-Markt: dieses Motiv wird bei der Begründung gewählt, dass die Auswahl einer bestimmten Applikation erfolgt, weil diese in der Auflistungsreihenfolge an erster Stelle beziehungsweise weit oben stand.
6. Symbolgestaltung: das Entscheidungsmotiv der Symbolgestaltung wird gewählt, wenn die Teilnehmenden als Auswahlgrund explizit die Gestaltung des Applikationsemblems genannt haben und die Bekanntheit oder Verbreitung keinen Einfluss auf die Auswahl hat.
7. Interface-Gestaltung, Screenshots: für dieses Motiv wird sich entschieden, wenn die Teilnehmenden auf Grund der Information über die Applikation im Play-Store von Google, welche nach der Auswahl im prototypisierten App-Markt präsentiert wurde, die Applikation wählen. Dabei verschafften sich einige Teilnehmende einen Überblick der Benutzeroberfläche der Applikation.
8. Erwartete Funktionalität und Eigenschaften: dieses Motiv wird gewählt, wenn die Teilnehmenden aus der Symbolgestaltung oder anhand des Namens auf enthaltene Funktionen oder Eigenschaften schließen.
9. Bewertungen: dieses Entscheidungsmotiv wird gewählt, wenn die Teilnehmenden auf Nutzerrezension im Google Play-Store zurückgreifen.
10. Anzahl der Downloads: dieses Motiv wird gewählt, wenn die Anzahl der Downloads im Google Play-Store als Entscheidungsmotiv verwendet wird.
11. Benennung der App: dieses Motiv wird gewählt, wenn die Teilnehmenden sich unabhängig von der Bekanntheit der Applikation und der Identifikation des Namens für eine Applikation entschieden haben, weil ihnen die Länge oder der Name an sich gefällt.
12. Datenschutz-Diagramme: dieses Motiv wird gewählt, wenn die Teilnehmenden sich auf Grund der Datenschutzdiagramme für die Applikation entschieden haben.

Jeder Auswahl werden dabei maximal drei Entscheidungsmotive zugewiesen, wobei nicht zwingend die Angabe von drei Motiven erfolgen muss. Ein häufiges Kriterium für die Applikationsauswahl ist die Bekanntheit. Die Häufigkeit der Nennung der Auswahlmotive ist in der Abbildung 20 illustriert.

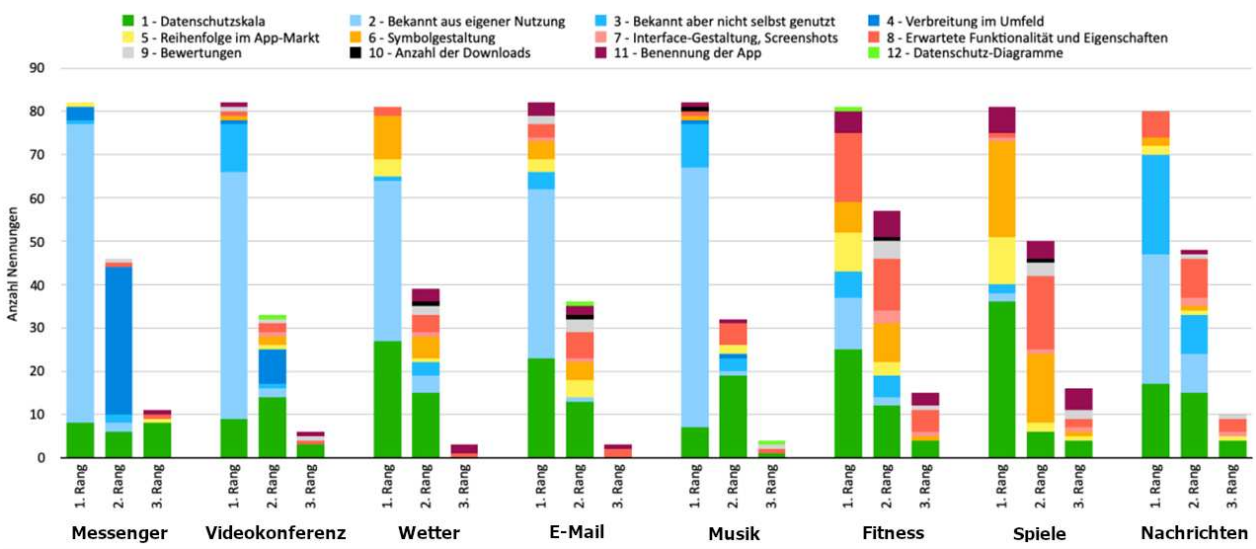


Abbildung 20. Entscheidungsmotive für die Auswahl der Applikationen über die Stichprobe *N* = 82.

Diese Abbildung bietet eine Übersicht der unterschiedlich häufigen Nutzung der Datenschutzskala als Entscheidungskriterium. Dabei zeigen die Ränge den Stellenwert für die getroffenen Entscheidungen bezüglich der Applikationsauswahl.

Anhand der Abbildung 20 ist die verschieden häufige Nutzung der Datenschutzskala als Entscheidungskriterium zu erkennen. In der Kategorie Messenger wird die Datenschutzskala 22-mal (Rang 1 = 8, Rang 2 = 6, Rang 3 = 8), bei der Videokonferenz 26-mal (Rang 1 = 9, Rang 2 = 14, Rang 3 = 3) und bei der Musik 27-mal (Rang 1 = 7, Rang 2 = 19, Rang 3 = 1) über alle Ränge als Entscheidungsmotiv genannt. Deutlich häufiger wird die Datenschutzskala in den Kategorien Spiele mit 46-mal (Rang 1 = 36, Rang 2 = 6, Rang 3 = 4), Wetter mit 42-mal (Rang 1 = 27, Rang 2 = 15, Rang 3 = 0) und Fitness mit 41-mal (Rang 1 = 25, Rang 2 = 12, Rang 3 = 4) von mehr als der Hälfte der Teilnehmenden als Auswahlkriterium aufgeführt. Bei dem Szenario der E-Mail wird die Datenschutzskala 36-mal (Rang 1 = 23, Rang 2 = 13, Rang 3 = 0) als Auswahlkriterium aufgeführt, während sie bei dem Szenario der Nachrichten 36-mal (Rang1 = 17, Rang 2 = 15, Rang 3 = 4) erwähnt wird. Eine Übersicht der Ergebnisse ist in Tabelle 99 im Anhang Y zu finden.

Abbildung 38 im Anhang Z zeigt die Entscheidungsmotive nach den einzelnen Gruppen von A - D getrennt. Über alle 4 Gruppen wurde die Bekanntheit aufgrund eigener Nutzung in den Szenarien Messenger, Videokonferenz und Musik als Entscheidungsmotiv angegeben. Bei den Szenarien Nachrichten, E-Mail und Wetter hat die Bekanntheit der Applikation ebenfalls einen hohen Einfluss auf das Auswahlverhalten, wobei in diesen Szenarien jedoch mehrere Ursachen für das Auswahlverhalten aufgezeigt werden. Bezüglich der Szenarien der Fitness und der Spiele ist eine heterogene Verteilung der Motive zu beobachten, wobei in der Gruppe B für die Kategorie Fitness die erwartete Funktionalität

der Eigenschaften als Motiv überwiegt, während in Gruppe D hingegen die Symbolgestaltung einen hohen Stellenwert einnimmt. Bezüglich der Spiele zeigt ebenfalls die Symbolgestaltung eine hohe Relevanz auf, während die Reihenfolge im App-Markt von Gruppe A über B, C bis hin zu Gruppe D stetig zunimmt. Eine Übersicht von den Ergebnissen ist in Tabelle 100,

Tabelle 101, Tabelle 102 und Tabelle 103 in Anhang Y zu sehen.

6.8.5.2 Vergleich der Adäquatheit der Applikationsauswahl getrennt nach den Entscheidungsmotiven

Werden die Mediane der App-Scores aller Szenarien getrennt nach den Gruppen verglichen, welche bereits in Abschnitt 6.7.4 beschrieben wurden, so ist in der Gruppe 1 (Datenschutzskala als wichtigstes Auswahlmotiv) in jedem Szenario der höchst mögliche Score (5) wiederzufinden, während dieser über Gruppe 2 (Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv) zu Gruppe 3 (Datenschutzskala hatte keinen Einfluss auf die Entscheidung) abnimmt (s. Tabelle 1).

Tabelle 1 *Median des App-Score getrennt nach Gruppen verschiedener Entscheidungsmotive*

		Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Gruppe 1	N	8	9	27	23	7	25	36	17
	Mdn	5	5	5	5	5	5	5	5
Gruppe 2	N	14	17	15	13	20	16	10	19
	Mdn	3	4	4	3	4	5	4,5	5
Gruppe 3	N	60	56	39	46	55	40	35	44
	Mdn	3	4	3	3	4	4,5	3	3

Anmerkung. Diese Tabelle zeigt die Mediane des App-Scores getrennt nach den Gruppen unterschiedlicher Relevanz der Datenschutzskala definiert in Abschnitt 6.7.4.

Zur Prüfung signifikanter Unterschiede bezüglich des App-Scores zwischen den eben genannten Gruppen wird ein Kruskal-Wallis-Test durchgeführt, welcher signifikante Unterschiede mit jeweils p = .000 zwischen den Gruppen über alle Szenarien hinweg bestätigt (Messenger χ^2 = 18,836; Videokonferenz χ^2 = 25,110; Wetter χ^2 = 41,565; E-Mail χ^2 = 44,548; Musik χ^2 = 16,289; Fitness χ^2 =

18,905; Spiele χ^2 = 41,237; Nachrichten χ^2 = 21,281). Eine Übersicht der Ergebnisse ist in Tabelle 104 im Anhang Y aufgeführt. Bei dem paarweise Vergleich zwischen den Gruppen 1 und 2 mit Hilfe des Mann-Whitney-U-Testes (s. Tabelle 105, Anhang Y) können signifikante Unterschiede in allen Szenarien außer in dem der Nachrichten festgestellt werden (Messenger *U* = 16,00; *z* = -3,127; *p* < .003; Videokonferenz *U* = 13,00; *z* = -4,150; *p* < .000; Wetter *U* = 86,50; *z* = -3,262; *p* < .002; E-Mail *U* = 37,00; *z* = -4,032; *p* < .000; Musik *U* = 20,50; *z* = -3,352; *p* < .001; Fitness *U* = 150,00 ; *z* = -2,596; *p* < .014; Spiele *U* = 98,00; *z* = -3,500; *p* < .001). Zwischen den Gruppen 1 und 3 (s. Tabelle 106, Anhang Y) können signifikante Unterschiede bei allen Szenarien mit einem p-Wert von p < .000 festgestellt werden (Messenger *U* = 51,00; *z* = -4,183; Videokonferenz *U* = 51,00; *z* = -4,562; Wetter *U* = 74,00; *z* = -6,069; E-Mail *U* = 63,50; *z* = -6,375; Musik *U* = 57,50; *z* = -3,788; Fitness *U* = 250,00; *z* = -4,132; Spiele *U* = 153,00; *z* = -6,237, Nachrichten *U* = 178,50, *z* = -3,637). Der Signifikanz-Test kann zwischen der zweiten und der dritten Gruppe (s. Tabelle 107, Anhang Y) lediglich 3 signifikante Unterschiede zwischen den Szenarien Wetter (*U* = 133,50; *z* = -3,220; *p* < .002), Spiele (*U* = 82,50; *z* = - 2,703; *p* < .010) und Nachrichten (*U* = 225,50; *z* = -3,285; *p* < .002) herausstellen.

6.8.6 Fragebogen

In den folgenden Kapiteln werden die Angaben der Teilnehmenden, die sie im Fragenbogen getätigt haben, aufgezeigt und analysiert. Zunächst werden die Ergebnisse zur Bekanntheit der ausgewählten Applikation vorgestellt. Nachfolgend wird die Bewertung der Datenschutzskala aufgezeigt. Anschließend soll die Einfachheit der Applikationsauswahl und die Vertrauenswürdigkeit der Applikationen näher betrachtet werden. Daraufhin werden die alltäglichen Bedenken der Nutzenden mobiler Endgeräte im Bereich der Privatsphäre aufgezeigt.

6.8.6.1 Bekanntheit der ausgewählten Applikation

Dieser Abschnitt veranschaulicht, ob die von den Teilnehmenden für die zu erfüllende Aufgabe ausgewählte Applikation bereits auf dem eigenen privaten Endgerät installiert ist oder sie die Applikation schon selbst benutzt haben. In Tabelle 108 im Anhang Y ist zu sehen, dass die für das Szenario des Messengers ausgewählte Applikation 66-mal (78,6 %) bereits installiert und verwendet wurde. Eine Person (1,2 %) hat die Applikation zwar installiert, jedoch noch nicht verwendet. Zwei weitere haben die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert. Insgesamt 13 Personen haben die Applikation weder installiert noch verwendet.

Bezüglich des Szenarios der Videokonferenz ist zu sehen, dass die ausgewählte Applikation 33-mal (39,3 %) bereits installiert und verwendet wurde. Sieben Personen (8,3 %) haben die Applikation zwar installiert, jedoch noch nicht verwendet. Weitere 21 (25 %) haben die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert. Insgesamt 21 Personen (25 %) hatten die Applikation weder installiert noch verwendet.

Bezüglich des Szenarios des Wetters ist zu sehen, dass die ausgewählte Applikation 14-mal (16,7 %) bereits installiert und verwendet wurde. Zwei Personen (2,4 %) haben die Applikation zwar installiert, jedoch noch nicht verwendet. Weitere 17 Teilnehmende (20,2 %) haben die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert. Insgesamt 29 Personen (34,5 %) haben die Applikation weder installiert noch verwendet. Insgesamt 20 Teilnehmende (23,8 %) haben keine Antwort bezüglich der ausgewählten Applikation.

Bezüglich des Szenarios der E-Mail ist zu sehen, dass die ausgewählte Applikation 18-mal (21,4 %) bereits installiert und verwendet wurde. Zwei Personen (2,4 %) haben die Applikation zwar installiert, jedoch noch nicht verwendet. Weitere 12 (14,3 %) haben die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert. Insgesamt 37 Personen (44 %) haben die Applikation weder installiert noch verwendet. Insgesamt 13 Teilnehmende (15,5 %) gaben keine Antwort bezüglich der ausgewählten Applikation.

Bezüglich des Szenarios der Musik ist zu sehen, dass die ausgewählte Applikation 41-mal (48,8 %) bereits installiert und verwendet wurde. Vier Personen (4,8 %) haben die Applikation zwar installiert, jedoch noch nicht verwendet. Elf weitere (13,1 %) haben die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert. Insgesamt 24 Personen (28,6 %) haben die Applikation weder installiert noch verwendet. Insgesamt zwei Teilnehmende (2,4 %) gaben keine Antwort bezüglich der ausgewählten Applikation.

Bezüglich des Szenarios der Spiele ist zu sehen, dass die ausgewählte Applikation zweimal (2,4 %) bereits installiert und verwendet wurde. Keine Person hat die Applikation zwar installiert, jedoch noch nicht verwendet. Zwei Teilnehmende (2,4 %) haben die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert. Weitere 78 Personen (92,9 %) haben die Applikation weder installiert noch verwendet.

Bezüglich des Szenarios der Fitness ist zu sehen, dass die ausgewählte Applikation neunmal (10,7 %) bereits installiert und verwendet wurde. Keine Person hat die Applikation zwar installiert, jedoch noch nicht verwendet. Zwölf Teilnehmende (14,3 %) haben die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert. Insgesamt 59 Personen (70,2 %) haben die Applikation

weder installiert noch verwendet. Nur ein Teilnehmer (1,2 %) gab keine Antwort bezüglich der ausgewählten Applikation.

Bezüglich des Szenarios der Nachrichten ist zu sehen, dass die ausgewählte Applikation neunmal (10,7 %) bereits installiert und verwendet wurde. Drei Personen (3,6 %) haben die Applikation zwar installiert, jedoch noch nicht verwendet. Weitere 23 (27,4 %) haben die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert. 47 Personen (56 %) haben die Applikation weder installiert noch verwendet.

Die Häufigkeiten werden nach Gruppen getrennt in Tabelle 109 im Anhang Y aufgezeigt.

Bezüglich des Szenarios des Messengers ist zu sehen, dass die Applikation am häufigsten von Gruppe A mit 85,7 % und am wenigsten von Gruppe B mit 68,4 % bereits installiert und verwendet wurde. Bei Gruppe C gaben 4,3 % der Teilnehmenden an, die Applikation zwar installiert, jedoch noch nicht verwendet zu haben. Bei allen anderen Gruppen gab es keine Person, welche diese Kategorie für die verwendete Applikation in dem Szenario des Messengers ausgewählt hat. Bei Gruppe D gaben 10,5 % der Teilnehmenden an, die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert zu haben. Bei allen anderen Gruppen gab es keine Person, welche diese Kategorie für die verwendete Applikation ausgewählt hat.

Bezüglich des Szenarios der Videokonferenz ist zu sehen, dass die Applikation am häufigsten von Gruppe D mit 57,9 % und am wenigsten von Gruppe A mit 33,3 % bereits installiert und verwendet wurde. Bei Gruppe A haben 15,3 % die Applikation zwar installiert, jedoch noch nicht verwendet, während bei Gruppe C lediglich 4,3 % diese Kategorie gewählt haben. Bei Gruppe B gaben 31,6 % der Teilnehmenden an, die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert zu haben, während bei der Gruppe D nur 10,5 % diese Kategorie wählten. Bei Gruppe B und D gaben jeweils 26,3 % der Teilnehmenden an, die Applikation noch nicht installiert und nicht verwendet zu haben, während bei Gruppe A 23,8 % diese Kategorie wählten.

Bezüglich des Szenarios des Wetters ist zu sehen, dass die Applikation am häufigsten von Gruppe B mit 26,3 % und am wenigsten von Gruppe A mit 9,5 % bereits installiert und verwendet wurde. Bei Gruppe A haben 4,8 % die Applikation zwar installiert, jedoch noch nicht verwendet, während bei Gruppe B und D keiner diese Kategorie gewählt hat. Bei Gruppe A gaben 33,3 % der Teilnehmenden an, die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert zu haben, während bei der Gruppe C nur 8,7 % diese Kategorie wählen. Bei Gruppe B gaben 47,4 % der Teilnehmenden an, die Applikation noch nicht installiert und nicht verwendet zu haben, während bei

Gruppe D 15,8 % diese Kategorie wählten. In diesem Szenario gaben 36,8 % der Teilnehmenden der Gruppe D, 30,4 % der Gruppe C, 15,8 % der Gruppe B und 14,3 % der Gruppe A keine Antwort an.

Bezüglich des Szenarios der E-Mail ist zu sehen, dass die Applikation am häufigsten von Gruppe B mit 31,6 % und am wenigsten von Gruppe A mit 14,3 % bereits installiert und verwendet wurde. Bei Gruppe D haben 10,5 % die Applikation zwar installiert, jedoch noch nicht verwendet, während bei Gruppe A, B und C keiner diese Kategorie gewählt hat. Bei Gruppe D gaben 26,3 % der Teilnehmenden an, die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert zu haben, während bei der Gruppe A nur 4,8 % diese Kategorie wählten. Bei Gruppe C gaben 52,2 % der Teilnehmenden an, die Applikation noch nicht installiert und nicht verwendet zu haben, während bei Gruppe B und D jeweils 42,1 % diese Kategorie wählten. In diesem Szenario gaben 38,1 % der Teilnehmenden der Gruppe A, 15,8 % der Gruppe B und 8,7 % der Gruppe C keine Antwort an.

Bezüglich des Szenarios der Musik ist zu sehen, dass die Applikation am häufigsten von Gruppe D mit 68,4 % und am wenigsten von Gruppe B mit 31,6 % bereits installiert und verwendet wurde. Bei Gruppe B und D haben jeweils 5,3 % die Applikation zwar installiert, jedoch noch nicht verwendet, während bei Gruppe C 4,8 % diese Kategorie gewählt haben. Bei Gruppe B gaben 21,1 % der Teilnehmenden an, die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert zu haben, während bei der Gruppe D nur 5,3 % diese Kategorie wählen. Bei Gruppe B gaben 42,1 % der Teilnehmenden an, die Applikation noch nicht installiert und nicht verwendet zu haben, während bei Gruppe A 19 % diese Kategorie wählten. In diesem Szenario gaben 4,8 % der Teilnehmenden der Gruppe A und 4,3 % der Gruppe C keine Antwort an.

Bezüglich des Szenarios der Fitness ist zu sehen, dass die Applikation am häufigsten von Gruppe A mit 14,3 % und am wenigsten von Gruppe D mit 5,3 % bereits installiert und verwendet werden. Keiner der Teilnehmenden gab an, die Applikation zwar installiert, jedoch noch nicht verwendet zu haben. Bei Gruppe B und D gaben jeweils 15,8 % der Teilnehmenden an, die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert zu haben, während bei der Gruppe C nur 13 % diese Kategorie wählten. Bei Gruppe D gaben 78,9 % der Teilnehmenden an, die Applikation noch nicht installiert und nicht verwendet zu haben, während bei Gruppe B 68,4 % diese Kategorie wählten. In diesem Szenario gaben 4,3 % der Teilnehmenden der Gruppe C keine Antwort an.

Bezüglich des Szenarios der Spiele ist zu sehen, dass die Applikation am häufigsten von Gruppe A mit 4,8 % und von Gruppe B und D nicht einmal bereits installiert und verwendet wurde. Keiner der Teilnehmenden gab an, die Applikation zwar installiert, jedoch noch nicht verwendet zu haben. Bei Gruppe D gaben 5,3 % der Teilnehmenden an, die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert zu haben, während die Teilnehmenden bei Gruppe B und C diese

Kategorie nicht einmal wählten. Bei Gruppe B gaben alle Teilnehmenden an, die Applikation noch nicht installiert und nicht verwendet zu haben, während bei Gruppe A 90,5 % diese Kategorie wählten.

Bezüglich des Szenarios der Nachrichten ist zu sehen, dass die Applikation am häufigsten von Gruppe D mit 15,8 % und am wenigsten von Gruppe B mit 5,3 % bereits installiert und verwendet zu wurde. Bei der Gruppe D gaben 5,3 % der Teilnehmenden an, die Applikation zwar installiert, jedoch noch nicht verwendet zu haben, während keiner der Teilnehmenden in der Gruppe B diese Kategorie wählte. Bei Gruppe B gaben jeweils 31,6 % der Teilnehmenden an, die Applikation bereits verwendet, jedoch derzeit nicht auf ihrem Smartphone installiert zu haben, während bei der Gruppe C nur 26,1 % diese Kategorie wählten. Bei Gruppe B gaben 63,2 % der Teilnehmenden an, die Applikation noch nicht installiert und nicht verwendet zu haben, während bei Gruppe D 52,6 % diese Kategorie wählten.

6.8.6.2 Ergebnisse zur Bewertung der Datenschutzskala

Beim Betrachten der Ergebnisse zur Bewertung der Datenschutzskala (s. Tabelle 110, Anhang Y) fällt auf, dass auf einer Skala von 1 = Trifft überhaupt nicht zu, bis 7 = Trifft völlig zu insgesamt bei positiven Aussagen durchweg eine positive Bewertung abgegeben wird (Vertrauenswürdigkeit (*M* = 5,38; *SD* = 1,24), Benutzerfreundlichkeit (*M* = 5,98; *SD* = 0,89), Verständnis (*M* = 6,16; *SD* = 0,87), Intuitivität (*M* = 5,65; *SD* = 1,34), Gültigkeit (*M* = 5,12; *SD* = 1,28), Zuverlässigkeit (*M* = 5,18; *SD* = 1,27), Einfluss (*M* = 5,32; *SD* = 1,68), Schutzgefühl (*M* = 5,77; *SD* = 1,40), Nachfragewunsch (*M* = 5,69; *SD* = 1,61), Nutzungsbereitschaft (*M* = 5,92; *SD* = 1,58), Applikationsvertrauenswürdigkeit (*M* = 6,03; *SD* = 1,21)). Den negativen Aussagen wird insgesamt deutlich weniger zugestimmt (Uneindeutigkeit (*M* = 2,16; *SD* = 1,26), Informationsarmut (*M* = 3,60; *SD* = 1,79), Komplexität (*M* = 2,21; *SD* = 1,55)).

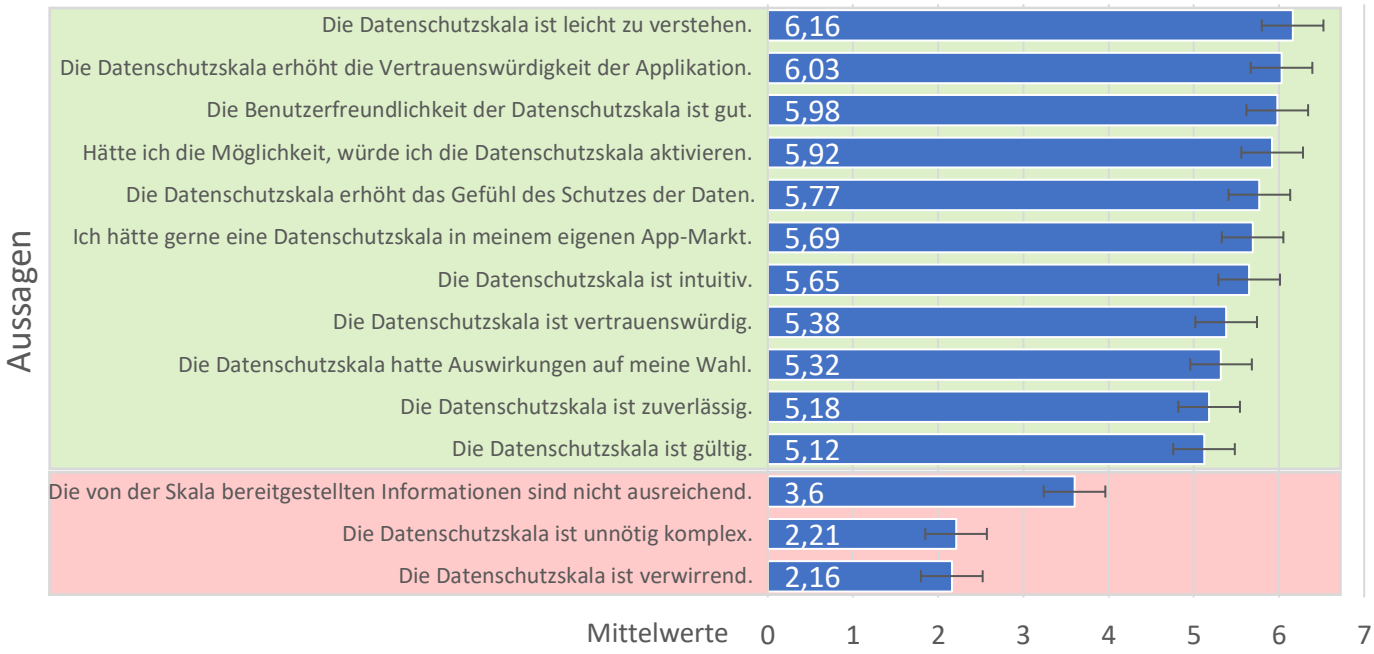


Abbildung 21. Bewertung der Datenschutzskala.

Diese Abbildung zeigt die Mittelwerte der Bewertungen der entsprechenden Aussagen bezüglich der Datenschutzskala mit 1 = Trifft überhaupt nicht zu bis 7 = Trifft völlig zu. Dabei werden die positiven Aussagen grün und die negativen Aussagen rot markiert.

Werden die Gruppen untereinander verglichen, so lässt sich eine Tendenz zur besseren Bewertung in Gruppe A wiederfinden (Vertrauenswürdigkeit (*M* = 5,67; *SD* = 1,32), Benutzerfreundlichkeit (*M* = 6,10; *SD* = 0,89), Verständnis (*M* = 6,33; *SD* = 0,91), Intuitivität (*M* = 5,48; *SD* = 11,63), Gültigkeit (*M* = 5,43; *SD* = 1,33), Zuverlässigkeit (*M* = 5,43; *SD* = 1,25), Einfluss (*M* = 5,86; *SD* = 1,56), Schutzgefühl (*M* = 5,86; *SD* = 1,32), Nachfragewunsch (*M* = 5,80; *SD* = 1,61), Nutzungsbereitschaft (*M* = 6,24; *SD* = 1,26), Applikationsvertrauenswürdigkeit (*M* = 6,24; *SD* = 0,94), Uneindeutigkeit (*M* = 2,10; *SD* = 1,14), Informationsarmut (*M* = 3,05; *SD* = 1,69), Komplexität (*M* = 2,10; *SD* = 1,30)), während Gruppe C (Vertrauenswürdigkeit (*M* = 5; *SD* = 1,27), Benutzerfreundlichkeit (*M* = 5,91; *SD* = 0,87), Verständnis (*M* = 6,13; *SD* = 0,87), Intuitivität (*M* = 5,74; *SD* = 1,05), Gültigkeit (*M* = 4,24; *SD* = 1,32), Zuverlässigkeit (*M* = 4,96; *SD* = 1,33), Einfluss (*M* = 4,78; *SD* = 1,83), Schutzgefühl (*M* = 5,65; *SD* = 1,64), Nachfragewunsch (*M* = 5,7; *SD* = 1,64), Nutzungsbereitschaft (*M* = 5,74; *SD* = 1,84), Applikationsvertrauenswürdigkeit (*M* = 5,83; *SD* = 1,3), Uneindeutigkeit (*M* = 2,17; *SD* = 1,03), Informationsarmut (*M* = 4,48; *SD* = 1,86), Komplexität (*M* = 2,04; *SD* = 1,49)) meist die schlechtesten Bewertungen gegeben hat. Die Gruppe B (Vertrauenswürdigkeit (*M* = 5,50; *SD* = 1,04), Benutzerfreundlichkeit (*M* =5,94; *SD* = 0,97), Verständnis (*M* =6; *SD* = 0,84), Intuitivität (*M* = 5,72; *SD* = 1,36), Gültigkeit (*M* = 5,25; *SD* = 1,07), Zuverlässigkeit (*M* = 5,18; *SD* = 1,24), Einfluss (*M* = 5,39; *SD* =

1,46), Schutzgefühl (*M* = 5,83; *SD* = 1,2), Nachfragewunsch (*M* = 5,56; *SD* = 1,67), Nutzungsbereitschaft (*M* = 5,78; *SD* = 1,59), Applikationsvertrauenswürdigkeit (*M* = 6,06; *SD* = 1,39), Uneindeutigkeit (*M* = 2,22; *SD* = 1,67), Informationsarmut (*M* = 3,11; *SD* = 1,41), Komplexität (*M* = 2,56; *SD* = 1,89)) befindet sich mit den abgegebenen Bewertungen meist zwischen den beiden Gruppen.

Anschließend wurden die unterschiedlichen Datensätze mit Hilfe des Kolmogorov-Smirnov-Tests auf Normalverteilung geprüft. Dieser schloss eine Normalverteilung bei allen Wertepaaren aus. Anschließend wurde der nicht-parametrische Kruskal-Wallis-Test angewandt, welcher jedoch lediglich einen signifikanten Unterschied bei dem Mangel an Information (χ^2 = 8 ,58; p < .01) herausstellen konnte (s. Tabelle 111, Anhang Y). Nach der Anwendung der Bonferroni-Korrektur verkleinert sich das Signifikanzniveau auf p < .003. Somit unterscheiden sich die Gruppen bezüglich der Bewertung der Skala nicht signifikant.

Um zu ermitteln, für welche Gruppen die Datensätze signifikant unterschiedlich sind, wurde wiederum auf den Mann-Whitney-U-Test zurückgegriffen. Dieser ergab keine signifikanten Unterschiede beim Vergleich der Gruppen A und B (s. Tabelle 112, Anhang Y). Bezüglich der Gruppen A und C (s. Tabelle 113, Anhang Y) konnte ein signifikanter Unterschied mittlerer Effektstärke bei der Auswirkung auf das Auswahlverhalten (*U* = 150,5*; z* = -2,2; *p* < .03) und bei dem Mangel an der Information (*U* = 133,5; *z* = -2,6; *p* < .01) festgestellt werden. Werden die Gruppen B und C (s. Tabelle 114, Anhang Y) verglichen, so ist nur ein signifikanter Unterschied mittlerer Effektstärke ebenfalls bei dem Mangel an Information zu sehen (*U* = 117; *z* = -2,4; *p* < .02).

6.8.6.3 Ergebnisse zur Einfachheit der Applikationsauswahl und Vertrauenswürdigkeit der Applikation

Bei der Betrachtung der Ergebnisse der Einfachheit der Applikationsauswahl und der Vertrauenswürdigkeit der Applikation auf einer Skala von 1 = Trifft überhaupt nicht zu, bis 7 = Trifft völlig zu sind die höchsten Mittelwerte, mit der Ausnahme vom Messenger bei der Einfachheit der Applikationsauswahl, allesamt in Gruppe A bis C wiederzufinden (s. Tabelle 115, Anhang Y). Somit könnte von der Tendenz ausgegangen werden, dass mit der Ausnahme vom Messenger die Datenschutzskala dazu geführt hat, dass die Teilnehmenden es als einfacher empfanden, eine geeignete Applikation zur Bewältigung der Aufgabe zu wählen und die Applikation als vertrauenswürdiger bewerteten als die Teilnehmenden ohne Datenschutzskala. Um dies zu überprüfen, wird auf Grund der Abwesenheit einer Normalverteilung, welche durch den Kolmogorov-Smirnov-Test gezeigt wird, ein Kruskal-Wallis-Test durchgeführt. Dieser zeigt signifikante Unterschiede in den Mittelwerten für die Vertrauenswürdigkeit der Applikation in den Kategorien E-Mail (χ^2 = 8,488;

p <.03) und Fitness (χ^2 = 12,133; p < .007). Für die Einfachheit kann nur ein signifikanter Unterschied in den Mittelwerten für die Kategorie Fitness (χ^2 =12.563; p < .006) gefunden werden (s. Tabelle 116, Anhang Y).

Um genauer zu betrachten, zwischen welchen Gruppen signifikante Unterschiede zu finden sind, wird ein paarweiser Vergleich zwischen allen Gruppen mit Hilfe des Mann-Whitney-U-Tests durchgeführt, weil der Großteil der Datensätze nicht normalverteilt ist. Beim Vergleich der Gruppen A und B (s. Tabelle 117, Anhang Y) können keine signifikanten Unterschiede ermittelt werden. Werden jedoch die Gruppen A und C (s. Tabelle 118, Anhang Y) verglichen, so ergeben sich signifikante Unterschiede mit einer mittleren Effektstärke bei der Einfachheit der Auswahl in den Szenarien Wetter (*U* = 154; *z* = -2,13; *p* < .03; *r* = 0,32), E-Mail (*U* = 129,50; *z* = -2,53; *p* < .012; *r* = 0,39), Musik (*U* = 152; *z* = -2,29; *p* < .022; *r* = 0,35), Fitness (*U* = 94,50; *z* = -3,007; *p* < .003; *r* = 0,47) und Spiele (*U* = 127; *z* = -2,58; *p* < .01 ; *r* = 0,39).

Bezüglich der Vertrauenswürdigkeit der Applikation ergeben sich Unterschiede bei dem folgenden Vergleich zwischen dem Szenario der E-Mail (*U* = 127,50; *z* = -2,39; *p* < .017; *r* = 0,37) und dem Szenario der Spiele (*U* = 127,5; *z* = -2,57; *p* < .01 ; *r* = 0,39). Werden dieselben Variablen zwischen der Gruppe A und D (s. Tabelle 119, Anhang Y) verglichen, so ist lediglich ein signifikanter Unterschied bezüglich der Einfachheit der Applikation im Szenario Fitness (*U* = 58; *z* = -3,034; *p* < .002; *r* = 0,52) zu finden, wobei bezüglich der Vertrauenswürdigkeit der Auswahl drei Unterschiede im Szenario der Videokonferenz (*U* = 122; *z* = -2,145; *p* < .032; *r* = 0,34), der E-Mail (*U* = 93,5; *z* = -2,59; *p* < .01; *r* = 0,42) und der Fitness (*U* = 65,5; *z* = -2,574; *p* < .01; *r* = 0,45) ermittelt werden können. Die paarweisen Vergleiche zwischen den Gruppen B und C (s. Tabelle 120, Anhang Y) ergeben signifikante Unterschiede mit einem mittleren Effekt bei den Szenarien Wetter (*U* = 125; *z* = -2,45; *p* < .014; *r* = 0,37) und Nachrichten (*U* = 140,5; *z* = -2,07; *p* < .039; *r* = 0,31) bezüglich der Einfachheit der Auswahl.

Bezüglich der Vertrauenswürdigkeit der Applikation ergeben sich signifikante Unterschiede bei den Szenarien Wetter (*U* = 135,5; *z* = -2,179; *p* < .029; *r* = 0,33), Nachrichten (*U* = 128; *z* = -2,40; *p* < .017; *r* = 0,36) und Fitness (*U* = 132; *z* = -2,01; *p* < .044 ; *r* = 0,32). Hinsichtlich der Gruppen B und D (s. Tabelle 121, Anhang Y) sind signifikante Unterschiede bezüglich der Vertrauenswürdigkeit der Applikation in den Szenarien Messenger (*U* = 106,5; *z* = -2,19; *p* < .028; *r* = 0,35) und Videokonferenz (*U* = 112; *z* = -2,06; *p* < .04; *r* = 0,33) mit einer mittleren Effektgröße und Fitness (*U* = 57,5; *z* = -3,03; *p* < .002 ; *r* = 0,53) mit einer großen Effektgröße zu beobachten. Zwischen den Gruppen C und D können keine signifikanten Unterschiede gefunden werden (s. Tabelle 122, Anhang Y). Zusätzlich zu dem nicht-parametrischen Mann-Whitney-U-Test werden bei den Datensätzen, die in beiden Gruppen eine Normalverteilung aufweisen, t-Tests für unabhängige Stichproben durchgeführt. Dazu gehören die

Datensätze zur Vertrauenswürdigkeit der Applikation Messenger zwischen allen Gruppen (s. Tabelle 123, Anhang Y) sowie der Applikation Spiele zwischen Gruppe B und D (s. Tabelle 124, Anhang Y). Bezüglich der Einfachheit der Auswahl werden die Datensätze der Fitness-Applikation zwischen den Gruppen B und C, B und D, und C und D und der E-Mail-Applikation der Gruppe B und D mit Hilfe eines t-Tests verglichen. Hierbei ergibt sich lediglich ein signifikantes Ergebnis zwischen den Gruppen B und D bezüglich der Vertrauenswürdigkeit der Applikation Messenger mit einem starken Effekt ($t(38) = 2{,}36$; $p < .024$; $r = 0{,}36$).

Um zu untersuchen, ob die Adäquatheit der Vertrauenswürdigkeit der Applikation sich zwischen den Gruppen unterscheidet, werden drei verschiedene Methoden angewandt, die bereits in Abschnitt 6.7.3.1 beschrieben wurden. Um die siebenstufige Likert-Skala, auf der angegeben wird, wie hoch die Vertrauenswürdigkeit in die Applikation seitens der Teilnehmenden ist, mit der fünfstufigen Datenschutzskala vergleichen zu können, wird bei der ersten Methode die Likert-Skala gestaucht, indem die ersten und letzten beiden Kategorien jeweils zu einer Kategorie zusammengefasst werden. In einem weiteren Schritt wird überprüft, wie viele der Teilnehmenden die gewählte Applikation im jeweiligen Szenario bezüglich der Vertrauenswürdigkeit adäquat, als vertrauenswürdiger oder als weniger vertrauenswürdig eingeschätzt haben.

Anhand Tabelle 125 im Anhang Y ist zu sehen, dass die ausgewählte Applikation im Szenario der Videokonferenz mit 33 richtigen Einschätzungen am adäquatesten beurteilt wird, während sie von 25 Einschätzungen als vertrauenswürdiger und von 40 Einschätzungen als weniger vertrauenswürdig eingeschätzt wird als in der Datenschutzskala angegeben.

Anschließend folgen die Szenarien der Fitness und der Spiele, die mit jeweils 29 Einschätzungen, der Musik mit 26, der E-Mail mit 24 und des Wetters mit 21 Einschätzungen adäquat beurteilt werden. Die geringsten adäquaten Einschätzungen sind bei dem Szenario des Wetters mit 17 Einschätzungen zu finden. Darüber hinaus werden die ausgewählten Applikationen in dem Szenario des Wetters mit insgesamt 45 Einschätzungen als weniger vertrauenswürdig beurteilt, als es in der Datenschutzskala angegeben ist. Darauf folgt das Szenario des Messengers und der Musik mit 35 Personen, das Szenario der E-Mail mit 34 Einschätzungen, der Videokonferenz mit 27 Einschätzungen, der Nachrichten mit 20 Einschätzungen und der Spiele mit 19 Einschätzungen. Das Szenario der Fitness wird mit den wenigsten Einschätzungen (N = 9) als weniger vertrauenswürdig beurteilt.

Dementsprechend werden die ausgewählten Applikationen des Szenarios der Fitness mit den meisten Einschätzungen (N = 36) als vertrauenswürdiger beurteilt als in der Datenschutzskala angegeben. Darauf folgt das Szenario der Nachrichten (32 Einschätzungen), der Spiele (30 Einschätzungen), des Messengers (25 Einschätzungen), der E-Mail (21 Einschätzungen) und der Musik (19 Einschätzungen).

Die Applikationen des Szenarios des Wetters werden am seltensten als vertrauenswürdiger eingeschätzt (17 Einschätzungen). Insgesamt wird bei der Anwendung dieser Methode 208-mal die Vertrauenswürdigkeit adäquat eingeschätzt, während 229-mal die Vertrauenswürdigkeit als niedriger und 196-mal als höher eingeschätzt wird als sie in der Datenschutzskala angegeben ist.

Beim Anwenden der zweiten Methode, der prozentualen Skala, sind lediglich 90 der 633 Beurteilungen adäquat, während 236-mal die Vertrauenswürdigkeit als niedriger und 307-mal als höher eingeschätzt wird als sie in der Datenschutzskala angegeben ist. Die Einschätzungen getrennt nach den Szenarien, wie sie bei der ersten Methode dargestellt wurden, sind der Tabelle 126 im Anhang Y zu entnehmen.

Die Ergebnisse der dritten Methode, bei der die Likert-Skala durch fünf dividiert wird, um sie mit der Datenschutzskala vergleichen zu können, zeigen lediglich 59 adäquate Beurteilungen, während 236-mal die Vertrauenswürdigkeit als niedriger und 261-mal als höher eingeschätzt wird als sie in der Datenschutzskala angegeben ist. Eine Übersicht getrennt nach den einzelnen Szenarien ist in der Tabelle 127 im Anhang Y zu sehen.

Bei Betrachtung der Differenzen zwischen der geschätzten Vertrauenswürdigkeit und der Kategorie der Datenschutzskala der ausgewählten Applikation zwischen den Gruppen wird bei der ersten Methode im Szenario des Messengers zu 33,3 % eine adäquate Antwort von Gruppe A abgegeben. Darauf folgt Gruppe B mit 27,8 %, Gruppe D mit 15,8 % und Gruppe C mit den wenigsten adäquaten Antworten (8,7 %). Dabei hat die Gruppe A zu 38,1 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 28,6 % als vertrauenswürdiger eingeschätzt als in der Datenschutzskala angegeben. Gruppe B hat zu 55,57 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 16,7 % als vertrauenswürdiger eingeschätzt. Dies entspricht dem geringsten Prozentsatz bezüglich der Einschätzung der Applikation als vertrauenswürdiger innerhalb aller Gruppen. Gruppe C hat zu 69,57 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 21,7 % als vertrauenswürdiger eingeschätzt. Somit weist Gruppe C den höchsten Prozentsatz bezüglich der Unterschätzung der Vertrauenswürdigkeit auf. Gruppe D hat zu 31,58 % die ausgewählte Applikation als weniger vertrauenswürdig und zu 52,6 % als vertrauenswürdiger eingeschätzt. Dies entspricht dem niedrigsten Prozentsatz bezüglich der Einschätzung als weniger vertrauenswürdig und dem höchsten Prozentsatz bezüglich der Einschätzung der Applikation als vertrauenswürdiger innerhalb aller Gruppen.

Bezüglich der Differenzen des Szenarios der Videokonferenz wird zu 47,8 % eine adäquate Antwort von Gruppe C abgegeben. Darauf folgte Gruppe A mit 42,9 %, Gruppe D mit 36,8 % und Gruppe B mit den wenigsten adäquaten Antworten (27,8 %). Dabei hat die Gruppe A zu 33,33 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 14,3 % als vertrauenswürdiger eingeschätzt als in

der Datenschutzskala angegeben. Gruppe B hat zu 55,57 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 11,1 % als vertrauenswürdiger eingeschätzt. Somit weist Gruppe B den höchsten Prozentsatz bezüglich der Unterschätzung der Vertrauenswürdigkeit und den geringsten Prozentsatz bezüglich der Überschätzung der Vertrauenswürdigkeit der Applikation innerhalb aller Gruppen auf. Gruppe C hat zu 30,44 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 21,7 % als vertrauenswürdiger eingeschätzt. Gruppe D hat zu 15,79 % die ausgewählte Applikation als weniger vertrauenswürdig und zu 42,1 % als vertrauenswürdiger eingeschätzt. Dies entspricht dem niedrigsten Prozentsatz bezüglich der Einschätzung als weniger vertrauenswürdig und dem höchsten Prozentsatz bezüglich der Einschätzung der Applikation als vertrauenswürdiger innerhalb aller Gruppen.

Die Differenzen des Szenarios des Wetters weisen zu 34,8 % eine adäquate Antwort von Gruppe C auf. Darauf folgte Gruppe A mit 33,3 %, Gruppe B mit 27,8 % und Gruppe D mit den wenigsten adäquaten Antworten (5,3 %). Dabei hat die Gruppe A zu 38,1 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 28,6 % als vertrauenswürdiger eingeschätzt als in der Datenschutzskala angegeben. Dies entspricht dem niedrigsten Prozentsatz bezüglich der Einschätzung als weniger vertrauenswürdig und dem höchsten Prozentsatz bezüglich der Einschätzung der Applikation als vertrauenswürdiger innerhalb aller Gruppen. Gruppe B hat zu 66,67 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 5,6 % als vertrauenswürdiger eingeschätzt. Somit weist Gruppe B den geringsten Prozentsatz bezüglich der Überschätzung der Vertrauenswürdigkeit der Applikation innerhalb aller Gruppen auf. Gruppe C hat zu 47,83 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 17,4 % als vertrauenswürdiger eingeschätzt. Gruppe D hat zu 73,68 % die ausgewählte Applikation als weniger vertrauenswürdig und zu 15,8 % als vertrauenswürdiger eingeschätzt. Somit weist Gruppe D den höchsten Prozentsatz bezüglich der Unterschätzung der Vertrauenswürdigkeit innerhalb aller Gruppen auf.

Die Differenzen des Szenarios der E-Mail weisen zu 44,4 % eine adäquate Antwort von Gruppe B auf. Darauf folgt Gruppe A mit 33,3 %, Gruppe C mit 21,7 % und Gruppe D mit den wenigsten adäquaten Antworten (21,1 %). Dabei hat die Gruppe A zu 38,1 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 23,8 % als vertrauenswürdiger eingeschätzt als in der Datenschutzskala angegeben. Dies entspricht dem niedrigsten Prozentsatz bezüglich der Einschätzung als weniger vertrauenswürdig innerhalb aller Gruppen. Gruppe B hat zu 44,44 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 11,1 % als vertrauenswürdiger eingeschätzt. Somit weist Gruppe B den geringsten Prozentsatz bezüglich der Überschätzung der Vertrauenswürdigkeit der Applikation innerhalb aller Gruppen auf. Die Gruppe C hat zu 39,13 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 34,8 % als vertrauenswürdiger eingeschätzt. Dies entspricht dem höchsten

Prozentsatz bezüglich der Einschätzung der Applikation als vertrauenswürdiger innerhalb der Gruppen. Gruppe D hat zu 47,37 % die ausgewählte Applikation als weniger vertrauenswürdig und zu 26,3 % als vertrauenswürdiger eingeschätzt. Somit weist Gruppe D den höchsten Prozentsatz bezüglich der Unterschätzung der Vertrauenswürdigkeit innerhalb aller Gruppen auf.

Die Differenzen des Szenarios der Musik weisen zu 44,4 % eine adäquate Antwort von Gruppe B auf. Darauf folgt Gruppe C mit 34,8 %, Gruppe A mit 28,6 % und Gruppe D mit den wenigsten adäquaten Antworten (21,1 %). Dabei hat die Gruppe A zu 47,62 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 19 % als vertrauenswürdiger eingeschätzt als in der Datenschutzskala angegeben. Gruppe B hat zu 16,67 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 38,9 % als vertrauenswürdiger eingeschätzt. Somit weist Gruppe B den geringsten Prozentsatz bezüglich der Unterschätzung sowie den höchsten Prozentsatz bezüglich der Überschätzung der Vertrauenswürdigkeit der Applikation innerhalb aller Gruppen auf. Gruppe C hat zu 52,17 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 13 % als vertrauenswürdiger eingeschätzt. Dies entspricht dem höchsten Prozentsatz bezüglich der Einschätzung der Applikation als weniger vertrauenswürdig sowie dem niedrigsten Prozentsatz bezüglich der Einschätzung der Applikation als vertrauenswürdiger innerhalb der Gruppen. Gruppe D hat zu 26,31 % die ausgewählte Applikation als weniger vertrauenswürdig und zu 42,1 % als vertrauenswürdiger eingeschätzt.

Die Differenzen des Szenarios Fitness weisen zu 44,4 % eine adäquate Antwort von Gruppe B auf. Darauf folgt Gruppe A mit 42,9 %, Gruppe C mit 34,8 % und Gruppe D mit den wenigsten adäquaten Antworten (15,8 %). Dabei hat die Gruppe A zu 4,76 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 33,3 % als vertrauenswürdiger eingeschätzt als in der Datenschutzskala angegeben. Somit weist Gruppe A den geringsten Prozentsatz bezüglich der Unterschätzung sowie der Überschätzung der Applikation innerhalb aller Gruppen auf. Die Gruppe B hat zu 5,6 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 44,5 % als vertrauenswürdiger eingeschätzt. Die Gruppe C hat zu 8,7 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 56,5 % als vertrauenswürdiger eingeschätzt. Dies entspricht dem höchsten Prozentsatz bezüglich der Einschätzung der Applikation als vertrauenswürdiger. Die Gruppe D hat zu 26,32 % die ausgewählte Applikation als weniger vertrauenswürdig und zu 42,1 % als vertrauenswürdiger eingeschätzt. Somit weist Gruppe D den höchsten Prozentsatz bezüglich der Unterschätzung der Vertrauenswürdigkeit der Applikation innerhalb aller Gruppen auf.

Die Differenzen des Szenarios der Spiele weisen zu 61,9 % adäquate Antworten von Gruppe A auf. Darauf folgt Gruppe B mit 38,9 %, Gruppe C mit 21,7 % und Gruppe D mit den wenigsten adäquaten Antworten (15,8 %). Dabei hat die Gruppe A zu 14,29 % die ausgewählten Applikationen als weniger

vertrauenswürdig und zu 19 % als vertrauenswürdiger eingeschätzt als in der Datenschutzskala angegeben. Somit weist Gruppe A den geringsten Prozentsatz bezüglich der Überschätzung der Applikation innerhalb aller Gruppen auf. Gruppe B hat zu 11,11 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 50 % als vertrauenswürdiger eingeschätzt. Somit weist Gruppe B den geringsten Prozentsatz bezüglich der Unterschätzung der Applikation innerhalb aller Gruppen auf. Die Gruppe C hat zu 26,08 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 52,2 % als vertrauenswürdiger eingeschätzt. Dies entspricht dem höchsten Prozentsatz bezüglich der Einschätzung der Applikation als vertrauenswürdiger als in der Datenschutzskala angegeben. Die Gruppe D hat zu 42,1 % die ausgewählte Applikation als weniger vertrauenswürdig und zu 26,3 % als vertrauenswürdiger eingeschätzt. Somit weist Gruppe D den höchsten Prozentsatz bezüglich der Unterschätzung der Vertrauenswürdigkeit der Applikation innerhalb aller Gruppen auf.

Die Differenzen des Szenarios der Nachrichten weisen zu 52,4 % eine adäquate Antwort von Gruppe A auf. Darauf folgt Gruppe B mit 44,4 %, Gruppe C mit 30,4 % und Gruppe D mit den wenigsten adäquaten Antworten (10,5 %). Dabei hat die Gruppe A zu 4,76 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 42,9 % als vertrauenswürdiger eingeschätzt als in der Datenschutzskala angegeben. Somit weist Gruppe A den geringsten Prozentsatz bezüglich der Unterschätzung sowie den höchsten Prozentsatz bezüglich der Überschätzung der Applikation innerhalb aller Gruppen auf. Gruppe B hat zu 16,67 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 38,9 % als vertrauenswürdiger eingeschätzt. Die Gruppe C hat zu 30,44 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 39,1 % als vertrauenswürdiger eingeschätzt. Die Gruppe D hat zu 47,37 % die ausgewählte Applikation als weniger vertrauenswürdig und zu 36,8 % als vertrauenswürdiger eingeschätzt. Dies entspricht dem höchsten Prozentsatz bezüglich der Einschätzung als weniger vertrauenswürdig und dem niedrigsten Prozentsatz bezüglich der Einschätzung der Applikation als vertrauenswürdiger innerhalb aller Gruppen.

Eine Übersicht über die Ergebnisse ist in Tabelle 128 im Anhang Y wiederzufinden. Darüber hinaus können der Tabelle detailliertere Angaben bezüglich der Häufigkeiten der Einschätzungen in jeder möglichen Differenz von -4 bis +4 entnommen werden.

Beim Betrachten der Ergebnisse der zweiten Methode fällt auf, dass eine deutlich geringere Anzahl an adäquaten Einschätzungen vorhanden ist. Der Grund hierfür ist die detailliertere Einteilung der Häufigkeiten in die prozentualen Kategorien, wie sie in Tabelle 129 im Anhang Y in der ersten Zeile zu sehen sind. Aus diesem Grund zeigen die Differenzen im Szenario des Messengers zwischen der geschätzten Vertrauenswürdigkeit und der Kategorie der Datenschutzskala der ausgewählten Applikation zwischen den Gruppen bei der zweiten Methode (prozentuale Skala) nur zu 28,6 % eine

adäquate Antwort von Gruppe A auf. Darauf folgte Gruppe D mit 15,8 %, Gruppe B mit 11,1 % und Gruppe C mit den wenigsten adäquaten Antworten (4,3 %). Dabei hat die Gruppe A zu 38,1 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 33,4 % als vertrauenswürdiger eingeschätzt als in der Datenschutzskala angegeben. Gruppe B hat zu 31,3 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 27,8 % als vertrauenswürdiger eingeschätzt. Dies entspricht dem geringsten Prozentsatz bezüglich der Einschätzung der Applikation als vertrauenswürdiger innerhalb aller Gruppen. Die Gruppe C hat zu 69,4 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 26,9 % als vertrauenswürdiger eingeschätzt. Somit weist Gruppe C den höchsten Prozentsatz bezüglich der Unterschätzung der Vertrauenswürdigkeit auf. Die Gruppe D hat zu 31,7 % die ausgewählte Applikation als weniger vertrauenswürdig und zu 52,7 % als vertrauenswürdiger eingeschätzt. Dies entspricht dem niedrigsten Prozentsatz bezüglich der Einschätzung als weniger vertrauenswürdig und dem höchsten Prozentsatz bezüglich der Einschätzung der Applikation als vertrauenswürdiger innerhalb aller Gruppen. Einen Überblick von den Häufigkeiten aller prozentualen Kategorien über alle Szenarien bietet die Tabelle 129 im Anhang Y.

Bei der dritten Methode (Division der Likert-Skala durch fünf) sind noch weniger adäquate Einschätzungen zu finden als bei der zweiten Methode, weil sich durch die Division der Skala ungerade Werte ergeben, deren Differenzen somit nur selten 0 ergeben.

Somit zeigen die Differenzen im Szenario des Messengers zwischen der geschätzten Vertrauenswürdigkeit und der Kategorie der Datenschutzskala der ausgewählten Applikation zwischen den Gruppen bei der dritten Methode (prozentuale Skala) nur zu 9,5 % eine adäquate Antwort von Gruppe A auf, während die anderen Gruppen nicht eine adäquate Antwort aufzeigen. Dabei hat die Gruppe A zu 38,2 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 52,4 % als vertrauenswürdiger eingeschätzt als in der Datenschutzskala angegeben. Die Gruppe B hat zu 61,3 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 38,9 % als vertrauenswürdiger eingeschätzt. Gruppe C hat zu 69,4 % die ausgewählten Applikationen als weniger vertrauenswürdig und zu 30,2 % als vertrauenswürdiger eingeschätzt. Somit weist Gruppe C den höchsten Prozentsatz bezüglich der Unterschätzung der Vertrauenswürdigkeit sowie den niedrigsten Prozentsatz bezüglich der Überschätzung auf. Die Gruppe D hat zu 31,7 % die ausgewählte Applikation als weniger vertrauenswürdig und zu 68,5 % als vertrauenswürdiger eingeschätzt. Dies entspricht dem niedrigsten Prozentsatz bezüglich der Einschätzung als weniger vertrauenswürdig und dem höchsten Prozentsatz bezüglich der Einschätzung der Applikation als vertrauenswürdiger innerhalb aller Gruppen. In der Tabelle 130 im Anhang Y wird erneut ein Überblick von den Häufigkeiten aller prozentualen Kategorien über alle Szenarien geboten.

Über die Häufigkeiten hinaus sollte verglichen werden, welche Gruppe in welchem Szenario die geringste Differenz zwischen der Einschätzung der Vertrauenswürdigkeit und der Kategorisierung der ausgewählten Applikation durch die Datenschutzskala aufweist und somit die Vertrauenswürdigkeit am adäquatesten beurteilt hat.

Für das Anwenden explorativer statistischer Verfahren müssen zunächst die Mittelwerte der Differenzen berechnet werden. Hierbei werden die Beträge der Differenzen verwendet, weil sich sonst die negativen und positiven Mittelwerte gegenseitig aufheben und es somit zur falschen Annahme einer adäquaten Einschätzung der Vertrauenswürdigkeit führen könnte. Die Berechnung der Mittelwerte wird bei allen drei Methoden durchgeführt und die Ergebnisse miteinander verglichen. Die Ergebnisse der ersten Methode werden in Tabelle 131, der zweiten Methode in Tabelle 124 und der dritten Methode in Tabelle 125 im Anhang Y, zum besseren Vergleich untereinander, aufgezeigt.

Bezüglich der ersten Methode fällt auf, dass insgesamt der niedrigste Betrag der Differenzen im Szenario der Musik mit *M* = 0,82 (*SD* = 0,71) und der höchste Wert im Szenario des Messengers mit *M* = 1,36 (*SD* = 0,95) wiederzufinden ist, während alle weiteren Szenarien folgende Beträge der Differenzen aufweisen: Videokonferenz *M* = 0,91 (*SD* = 0,98); E-Mail *M* = 1,09 (*SD* = 0,98); Nachrichten *M* = 1,1 (*SD* = 1,07); Spiele *M* = 1,13 (*SD* = 1,09); Fitness *M* = 1,15 (*SD* = 1,17); Wetter *M* = 1,21 (*SD* = 1,03).

Werden die Beträge der Differenzen zwischen den Gruppen A bis D verglichen, so fällt auf, dass sechs von acht Szenarien die niedrigsten Differenzen bei Gruppe A aufweisen (Messenger *M* = 1,05 (*SD* = 0,86); Videokonferenz *M* = 0,68 (*SD* = 0,82); Wetter *M* = 0,67 (*SD* = 0,48); E-Mail *M* = 0,95 (*SD* = 0,89); Spiele *M* = 0,75 (*SD* = 1,29); Nachrichten *M* = 0,81 (*SD* = 0,93)). Lediglich die Differenz des Szenarios der Fitness (*M* = 1,06 (*SD* = 1,43)) zeigt den zweithöchsten Wert, während das Szenario der Musik (*M* = 0,90 (*SD* = 0,79)) den höchsten Wert aufzeigt und somit bei der Anwendung dieser Methode bei Gruppe A die größte Abweichung zwischen der geschätzten Vertrauenswürdigkeit und der Kategorisierung bezüglich der Datenschutzskala darstellt.

Die Gruppe B enthält bei fünf Szenarien (Messenger *M* = 1,28 (*SD* = 1,07); Wetter *M* = 1,11 (*SD* = 0,96); E-Mail *M* = 1,00 (*SD* = 1,14); Spiele *M* = 0,89 (*SD* = 0,83); Nachrichten *M* = 0,89 (*SD* = 1,08)), die zweitniedrigsten Differenzen, während bei dem Szenario der Musik (*M* = 0,72 (*SD* = 0,75)) und dem Szenario der Spiele (*M* = 0,88 (*SD* = 0,99)) die niedrigsten Beträge der Differenzen zu verzeichnen sind. Beim Vergleich der vier Gruppen weist das Szenario der Videokonferenz (*M* = 0,88 (*SD* = 0,7)) in Gruppe B den zweithöchsten Wert auf.

In Gruppe C weisen insgesamt vier Werte (Messenger *M* = 1,52 (*SD* = 0,85); Wetter *M* = 1,30 (*SD* = 1,18); Spiele *M* = 1,26 (*SD* = 1,05); Nachrichten *M* = 1 (*SD* = 0,95)) die zweithöchsten Beträge der Differenzen auf. Die Szenarien Videokonferenz (*M* = 0,83 (*SD* = 0,98)), Musik (*M* = 0,78 (*SD* = 0,67)) und Fitness (*M* = 1,04 (*SD* = 0,98)) weisen den zweitniedrigsten Betrag der Differenzen auf. Eine Ausnahme stellt das Szenario der E-Mail in dieser Gruppe dar, welches mit *M* = 1,32 (*SD* = 1,13) den höchsten Betrag der Differenzen verglichen mit allen Gruppen aufzeigt.

In Gruppe D sind mit Ausnahme der Szenarien E-Mail (*M* = 1,06 (*SD* = 0,73)) und Musik (*M* = 0,89 (*SD* = 0,68)), welche die zweithöchsten Werte beinhalten, durchweg die höchsten Beträge der Differenzen zu verzeichnen (Messenger *M* = 1,58 (*SD* = 1,02); Videokonferenz *M* = 1,28 (*SD* = 1,27); Wetter *M* = 1,83 (*SD* = 1,04); Fitness *M* = 1,69 (*SD* = 1,25); Spiele *M* = 1,69 (*SD* = 0,95); Nachrichten *M* = 1,78 (*SD* = 1,17)).

Ferner soll geprüft werden, ob die Mittelwerte der eben genannten Beträge der Differenzen sich signifikant voneinander unterscheiden. Aufgrund der Abwesenheit einer Normalverteilung bei allen Werten, mit Ausnahme des Szenarios der Fitness, wird der Kruskal-Wallis-Test (s. Tabelle 134, Anhang Y) zur Identifikation der signifikanten Unterschiede bezüglich der Mittelwerte der Beträge der Differenzen angewandt. Dieser zeigt lediglich signifikante Unterschiede im Szenario des Wetters (χ^2 = 12,05; $p < .007$) und der Nachrichten (χ^2 = 8,861; $p < .031$).

Beim paarweisen Vergleich der einzelnen Szenarien zwischen den Gruppen A und B können, unter Verwendung des Mann-Whitney-U-Tests (s. Tabelle 135, Anhang Y), keine signifikanten Unterschiede ermittelt werden, während beim Vergleich der Gruppe A und C lediglich ein signifikantes Ergebnis mittlerer Effektstärke im Szenario der Spiele (*U* = 139; *z* = -2,09; $p < .036$; *r* = 0,33) resultierte (s. Tabelle 128, Anhang Y). Beim Vergleich der Gruppen A und D können ein signifikantes Ergebnis im Szenario des Wetters (*U* = 66,5; *z* = -3,782; $p < .000$; *r* = 0,61) mit großer Effektstärke und zwei signifikante Ergebnisse mit mittlerer Effektstärke in den Szenarien der Spiele (*U* = 80; *z* = -2,724; $p < .006$; *r* = 0,45) und der Nachrichten (*U* = 101; *z* = -2,574; $p < .01$; *r* = 0,41) identifiziert werden (s. Tabelle 129, Anhang Y). Zwischen den Gruppen B und C ist kein signifikanter Unterschied zu verzeichnen (s. Tabelle 138, Anhang Y), während zwischen den Gruppen B und D nur das Szenario der Nachrichten (*U* = 127; *z* = -2,217; $p < .026$; *r* = 0,36) mit einer mittleren Effektstärke als signifikant anzusehen ist (s. Tabelle 139, Anhang Y).

Beim letzten Vergleich zwischen Gruppe C und D resultieren drei signifikante Unterschiede einer mittleren Effektstärke in den Szenarien Wetter (*U* = 100; *z* = -2,058; $p < .039$; *r* = 0,32), Spiele (*U* = 76,5; *z* = -2,482; $p < .013$; *r* = 0,39) und Nachrichten (*U* = 90; *z* = -2,369; $p < .017$; *r* = 0,36) (s. Tabelle 140, Anhang Y).

Bezüglich der zweiten Methode (s. Tabelle 132, Anhang Y) fällt auf, dass insgesamt der niedrigste Betrag der Differenzen ebenfalls im Szenario der Musik mit *M* = 19,83 (*SD* = 14,76) und der höchste Wert jedoch im Szenario der Fitness mit *M* = 29,68 (*SD* = 23,89) wiederzufinden ist, während alle weiteren Szenarien folgende Beträge der Differenzen aufweisen: Videokonferenz *M* = 20,89 (*SD* = 18,47); E-Mail *M* = 24,36 (*SD* = 19,54); Nachrichten *M* = 28,96 (*SD* = 21,75); Spiele *M* = 29,33 (*SD* = 22,69); Fitness *M* = 1,15 (*SD* = 1,17); Wetter *M* = 27,19 (*SD* = 22,02).

Werden die Beträge der Differenzen zwischen den Gruppen A bis D verglichen, so fällt auf, dass fünf von acht Szenarien die niedrigsten Differenzen bei Gruppe A aufweisen (Messenger *M* = 19,84 (*SD* = 16,13); Wetter *M* = 16,27 (*SD* = 10,7); Fitness *M* = 26,96 (*SD* = 29,98); Spiele *M* = 20,42 (*SD* = 25,57); Nachrichten *M* = 23,41 (*SD* = 21,67)). Die Differenzen der Szenarien Videokonferenz (*M* = 18,42 (*SD* = 13,49)), E-Mail (*M* = 25 (*SD* = 17,31)) und Musik (*M* = 20,42 (*SD* = 14,68)) zeigen die zweitniedrigsten Werte auf.

Die Gruppe B enthält bei vier Szenarien (Messenger *M* = 29,63 (*SD* = 23,26); Wetter *M* = 24,54 (*SD* = 20,7); Spiele *M* = 25,93 (*SD* = 18,50); Nachrichten *M* = 25,93 (*SD* = 20,79)), die zweitniedrigsten Differenzen, während bei den Szenarien Videokonferenz (*M* = 16,67 (*SD* = 12,15)), E-Mail (*M* = 23,15 (*SD* = 22,79)) und Fitness (*M* = 26,96 (*SD* = 21,15)) die niedrigsten Beträge der Differenzen zu verzeichnen sind. Beim Vergleich der vier Gruppen weist das Szenario der Musik (*M* = 21,76 (*SD* = 16,2)) in Gruppe B den zweithöchsten Wert auf.

In Gruppe C weisen insgesamt sechs Werte (Messenger *M* = 31,52 (*SD* = 19,13); Videokonferenz *M* = 19,56 (*SD* = 18,57); Wetter *M* = 30,8 (*SD* = 23,63); Fitness *M* = 29,71 (*SD* = 19,27); Spiele *M* = 32,97 (*SD* = 21,09); Nachrichten *M* = 28,99 (*SD* = 18,61)) die zweithöchsten Beträge der Differenzen auf. Nur das Szenario der Musik weist in Gruppe C mit *M* = 17,75 (*SD* = 14,72) den niedrigsten Betrag der Differenzen verglichen mit allen anderen Gruppen auf, während das Szenario der E-Mail mit *M* = 30,3 (*SD* = 22,64), den höchsten Wert aufweist.

In Gruppe D sind mit Ausnahme der Szenarien E-Mail (*M* = 17,59 (*SD* = 12,09)) als niedrigster und Musik (*M* = 19,91 (*SD* = 14,33)) als zweitniedrigster Betrag der Differenzen durchweg die höchsten Beträge der Differenzen zu verzeichnen: Messenger *M* = 32,02 (*SD* = 22,95); Videokonferenz *M* = 29,17 (*SD* = 25,45); Wetter *M* = 37,96 (*SD* = 25,92); Fitness *M* = 35,42 (*SD* = 26,61); Spiele *M* = 39,06 (*SD* = 22,30) und Nachrichten *M* = 38,43 (*SD* = 24,94).

Darüber hinaus soll geprüft werden, ob die Mittelwerte der eben genannten Beträge der Differenzen sich signifikant voneinander unterscheiden. Aufgrund der Abwesenheit einer Normalverteilung bei allen Werten, mit Ausnahme des Szenarios der Fitness, wird der Kruskal-Wallis-Test (s. Tabelle 134,

Anhang Y) zur Identifikation der signifikanten Unterschiede bezüglich der Mittelwerte der Beträge der Differenzen angewandt. Dieser zeigt lediglich signifikante Unterschiede im Szenario des Wetters (χ^2 = 8,134; p < .043) und der Spiele (χ^2 = 9,310; p < .025).

Beim paarweisen Vergleich der einzelnen Szenarien zwischen den Gruppen A und B können, unter Verwendung des Mann-Whitney-U-Tests (s. 142, Anhang Y), keine signifikanten Unterschiede ermittelt werden, während beim Vergleich der Gruppe A und C lediglich ein signifikantes Ergebnis mittlerer Effektstärke im Szenario der Spiele (U = 139,5; z = -2,25; p < .024; r = 0,34) resultiert (s. Tabelle 143, Anhang Y).

Beim Vergleich der Gruppen A und D können zwei signifikante Ergebnisse im Szenario des Wetters (U = 93,5; z = -2,724; p < .006; r = 0,44) und der Spiele (U = 83,5; z = -2,49; p < .013; r = 0,41) mit mittlerer Effektstärke identifiziert werden(s. Tabelle 144, Anhang Y). Zwischen den Gruppen B und C (s. Tabelle 145, Anhang Y) sowie C und D (s. Tabelle 146, Anhang Y) ist kein signifikanter Unterschied zu verzeichnen, während zwischen den Gruppen B und D (s. Tabelle 147, Anhang Y) ein signifikanter Unterschied einer mittleren Effektstärke in dem Szenario der Spiele (U = 87,5; z = -2,01; p < .044; r = 0,34) identifiziert wird. Darüber hinaus wird mit allen Wertepaaren, die jeweils eine Normalverteilung aufzeigten, ein parametrischer t-Test für unabhängige Stichproben durchgeführt. Hierbei konnte lediglich ein signifikanter Unterschied (t(42) = - 2,584; p <.013; r = 0,37) mit einem starkem Effekt zwischen den Gruppen A und C im Szenario des Wetters festgestellt werden (s. Tabelle 148, Anhang Y).

Nach Anwendung der dritten Methode (s. Tabelle 133, Anhang Y) kann der niedrigste Betrag der Differenzen ebenfalls im Szenario der Musik mit M = 0,84 (SD = 0,63) verzeichnet werden. Der höchste Wert ist wie bei der zweiten Methode im Szenario der Fitness mit M = 1,26 (SD = 1,01) wiederzufinden. Während alle weiteren Szenarien folgende Beträge der Differenzen aufweisen: Videokonferenz M = 1,04 (SD =1,04); E-Mail M = 1,01 (SD = 0,78); Nachrichten M = 1,2 (SD = 0,88); Spiele M = 1,24 (SD = 0,94); Fitness M = 1,26 (SD = 1,01); Wetter M = 1,11 (SD = 0,87).

Beim Vergleichen der Beträge der Differenzen zwischen den Gruppen A bis D fällt auf, dass vier von acht Szenarien die niedrigsten Differenzen bei Gruppe A aufweisen (Messenger M = 0,86 (SD = 0,62); Wetter M = 0,7 (SD = 0,46); Spiele M = 0,87 (SD = 1,05); Nachrichten M = 0,99 (SD = 0,92)). Die Differenzen der Szenarien Fitness M = 1,16 (SD = 1,28)) und Musik (M = 0,87 (SD = 0,62)) zeigen die zweitniedrigsten Werte auf. Lediglich die Szenarien Videokonferenz (M = 1,05 (SD = 1,14)) und E-Mail (M = 1,04 (SD = 0,71)) zeigen den zweithöchsten Wert auf.

Die Gruppe B enthält bei sechs Szenarien (Messenger *M* = 1,2 (*SD* = 0,91); Videokonferenz (*M* = 0,86 (*SD* = 0,94)), Wetter *M* = 0,97 (*SD* = 0,82); E-Mail (*M* = 0,94 (*SD* = 0,88)) Spiele *M* = 1,1 (*SD* = 0,79); Nachrichten *M* = 1,08 (*SD* = 0,84)) die zweitniedrigsten Differenzen, während bei dem Szenario der Fitness (*M* = 1,14 (*SD* = 0,91)) wie auch in den anderen beiden Methoden der niedrigste Betrag der Differenzen zu verzeichnen ist. Beim Vergleich der vier Gruppen weist das Szenario der Musik (*M* = 0,94 (*SD* = 0,7)) in Gruppe B den höchsten Wert auf.

In Gruppe C weisen insgesamt fünf Werte (Messenger *M* = 1,25 (*SD* = 0,72); Wetter *M* = 1,26 (*SD* = 0,92); Spiele *M* = 1,38 (*SD* = 0,9); Nachrichten *M* = 1,18 (*SD* = 0,75)) die zweithöchsten Beträge der Differenzen auf. Das Szenario der Fitness weist mit *M* = 1,27 (*SD* = 0,83) den zweitniedrigsten Wert auf. Nur das Szenario der Videokonferenz weist in Gruppe C mit *M* = 0,83 (*SD* = 0,8) den niedrigsten Betrag der Differenzen verglichen mit allen anderen Gruppen auf, während das Szenario der E-Mail mit *M* = 1,27 (*SD* = 0,91) den höchsten Wert aufweist.

In Gruppe D sind ähnlich wie bei der ersten und zweiten Methode mit Ausnahme der Szenarien E-Mail (*M* = 0,75 (*SD* = 12,09)) und Musik (*M* = 0,85 (*SD* = 0,62)), welche beide die niedrigsten Beträge aufzeigen, durchweg die höchsten Beträge der Differenzen zu verzeichnen: Messenger *M* = 1,41 (*SD* = 0,91); Videokonferenz *M* = 1,43 (*SD* = 1,2); Wetter *M* = 1,52 (*SD* = 1,02); Fitness *M* = 1,48 (*SD* = 1,08); Spiele *M* = 1,64 (*SD* = 0,88) und Nachrichten *M* = 1,57 (*SD* = 0,98).

Es wird wiederholt geprüft, ob die Mittelwerte der eben genannten Beträge der Differenzen sich signifikant voneinander unterscheiden. Aufgrund der Abwesenheit einer Normalverteilung bei einigen Werten wurde der Kruskal-Wallis-Test (s. Tabelle 149, Anhang Y) zur Identifikation der signifikanten Unterschiede bezüglich der Mittelwerte der Beträge der Differenzen angewandt. Dieser zeigte lediglich einen signifikanten Unterschied im Szenario der Spiele ($\chi^2 = 9{,}78$; $p < .02$).

Beim paarweisen Vergleich der einzelnen Szenarien zwischen den Gruppen A und B können, unter Verwendung des Mann-Whitney-U-Tests (s. Tabelle 150, Anhang Y), keine signifikanten Unterschiede ermittelt werden, während beim Vergleich der Gruppe A und C (s. Tabelle 151, Anhang Y) wie bei den vorherigen Methoden lediglich ein signifikantes Ergebnis mittlerer Effektstärke im Szenario der Spiele ($U = 141{,}5$; $z = -2{,}17$; $p < .03$; $r = 0{,}33$) resultiert.

Beim Vergleich der Gruppen A und D (s. Tabelle 152, Anhang Y) konnten zwei signifikante Ergebnisse im Szenario des Messengers ($U = 124$; $z = -2{,}06$; $p < .039$; $r = 4{,}07$) und des Wetters ($U = 100{,}5$; $z = -2{,}5$; $p < .01$; $r = 14{,}46$) mit großer Effektstärke und im Szenario der Spiele ($U = 74{,}5$; $z = -2{,}74$; $p < .01$; $r = 0{,}46$) mit mittlerer Effektstärke identifiziert werden. Zwischen den Gruppen B und C (s. Tabelle 153, Anhang Y) ist wiederum kein signifikanter Unterschied zu verzeichnen, während zwischen den Gruppen

C und D (s. Tabelle 154, Anhang Y) wie auch in der ersten Methode ein signifikanter Unterschied einer mittleren Effektstärke in dem Szenario der Spiele (U = 83; z = -2,12; p < .03; r = 0,34) identifiziert wird. Zwischen den Gruppen B und D (s. Tabelle 155, Anhang Y) ist ähnlich wie bei der zweiten Methode ein signifikanter Unterschied bei dem Szenario der Spiele (U = 83; z = -2,12; p < .03; r = 0,36) zu verzeichnen.

Bei Anwendung dieser Methode herrscht eine Normalverteilung bei deutlich mehr Wertepaaren. Mit Hilfe des t-Tests können hier jedoch auch nur drei signifikante Unterschiede mit einem starken Effekt gefunden werden. Ein signifikanter Unterschied ist im Szenario des Wetters zwischen den Gruppen A und C (t(42) = -2,52; p <.015; r = 0,36) sowie A und D (t(37) = -3,35; p <.002; r = 0,48) zu sehen. Das Szenario des Messengers zeigte ebenfalls einen signifikanten Unterschied mit starkem Effekt zwischen den Gruppen A und D (t(38) = -2,216; p <.034; r = 0,34) auf (s. Tabelle 156, Anhang Y).

Darüber hinaus wird geprüft, ob ein Zusammenhang zwischen Technikaffinität und der Adäquatheit der Bewertung der Vertrauenswürdigkeit der Applikation besteht. Nach der Anwendung des Spearman-Rho-Testes mit der Variable der Technikaffinität und den Differenzen zwischen der angegebenen Vertrauenswürdigkeit und der tatsächlichen Einstufung der Applikation ergibt sich lediglich ein signifikantes Ergebnis bei der prozentualen Reskalierung in dem Szenario der Videokonferenz (r = -0,233; p <0,041) (s. Tabelle 157, Anhang Y). Ferner wird geprüft, ob weitere Zusammenhänge zwischen der Adäquatheit der Bewertung der Vertrauenswürdigkeit der Applikation und dem Geschlecht, dem Alter, dem Bildungsabschluss, der Privatsphäre und den Stunden der Nutzung eines Endgerätes bestehen. Hierbei kann lediglich ein signifikanter negativer Zusammenhang zwischen dem Alter und der Adäquatheit der Bewertung der Vertrauenswürdigkeit der Applikation innerhalb des Szenarios des Messengers (r = -0,224; p < .044) gefunden werden. Weiterhin kann ein signifikanter, negativer Zusammenhang zwischen der Adäquatheit der Bewertung der Vertrauenswürdigkeit der Applikation und dem Geschlecht innerhalb des Szenarios der Spiele bei allen Reskalierungsmethoden gefunden werden. Bei der Reskalierung auf eine fünfstufige Skala ergibt sich ein Zusammenhang mit r = -0,283 (p < .013). Bei der prozentualen Reskalierung kann ein Zusammenhang mit r = -0,225 (p < .05) festgestellt werden. Die Reskalierung mit Hilfe der Division ergab ebenfalls einen negativen Zusammenhang r = -0,238 (p < .038) (s. Tabelle 150, Tabelle 151, Tabelle 152, Tabelle 153, Tabelle 154, Anhang Y).

6.8.6.4 Ergebnisse zur Messung der Bedenken von Nutzenden mobiler Endgeräte hinsichtlich des Datenschutzes (MUIPC)

Ein Blick auf die Ergebnisse des MUIPC zeigt, dass ein überraschend hoher Prozentsatz der Teilnehmenden den Aussagen zustimmt. Insgesamt sind 84,2 % der Ansicht, dass der Standort ihres

Mobilgeräts zumindest vorübergehend überwacht wird. Nur 7,3 % stimmen dieser Aussage nicht zu. Die fehlenden 8,5 % sind unentschieden. Insgesamt 73,3 % befürchten, dass Anwendungen zu viele Informationen über sie sammeln. Etwa 19,5 % sind nicht dieser Meinung und 7,3 % sind unentschieden. Dabei befürchten 68,3 %, dass Anwendungen ihre Aktivitäten auf ihrem Mobilgerät überwachen, wobei 25,6 % dem nicht zustimmen und 6,1 % sich nicht sicher sind. Weiterhin haben 68,3 % das Gefühl, dass andere durch den Einsatz von Anwendungen mehr über sie wissen, als sie möchten. Hierbei stimmen 20,7 % nicht zu und 9,8 % sind unentschieden. Insgesamt 73,2 % glauben, dass Informationen über sie, die sie als privat betrachten, aufgrund ihrer Verwendung von Anwendungen nun besser für andere verfügbar sind als sie es möchten, wobei 12,1 % dies nicht glauben und 14,6 % unentschlossen sind. Ferner sind 73,2 % der Ansicht, dass aufgrund der Verwendung von Anwendungen Informationen über sie verfügbar sind, die bei ihrer Verwendung in die Privatsphäre eingreifen. Dabei stimmen 14,7 % dem nicht zu und 11,0 % sind unentschlossen. Weiterhin befürchten 69,5 %, dass Anwendungen ihre persönlichen Informationen für andere Zwecke verwenden können, ohne sie zu benachrichtigen oder um ihre Erlaubnis zu bitten. Hierbei sind 15,9 % nicht darüber besorgt, während 13,4 % unsicher sind. Insgesamt 76,8 % befürchten, dass die Anwendungen ihre Informationen für andere Zwecke verwenden, wenn sie den Anwendungen persönliche Informationen bereitstellen. Dabei sind 15,8 % darüber nicht besorgt und 7,3 % sind sich nicht sicher. Ferner befürchten 47,6 %, dass Apps ihre persönlichen Informationen mit anderen Instanzen teilen können, ohne deren Erlaubnis einzuholen. Dabei machen sich 26,9 % keine Sorgen und 24,4 % sind unentschieden. Schließlich geben 74,3 % an, wahrscheinlich in den nächsten zwölf Monaten ihre persönlichen Daten preiszugeben, um Anwendungen nutzen zu können. Hierbei geben 14,7 % an, dies nicht zu tun, und 9,8 % sind sich nicht sicher. Die genaue Aufteilung der Antworten auf einer Likert-Skala von 1 bis 7 ist in Tabelle 164 im Anhang Y.

Bei der Frage, wie oft ist in den letzten zwei Jahren vorgefallen ist, dass die persönlichen Daten des Teilnehmers oder der Teilnehmerin von Unternehmen oder E-Commerce Webseiten ohne die Genehmigung des Teilnehmers oder der Teilnehmerin verwendet wurden, haben 43,9 % angegeben, nicht einmal davon betroffen gewesen zu sein. Weitere 20,7 % haben angegeben, bereits ein bis zweimal die Erfahrung gemacht zu haben. Insgesamt 9,8 % gaben an, drei bis vier Vorfälle in den letzten zwei Jahren erfahren zu haben, während 25,6 % der Teilnehmenden angaben, dass ihre Daten ohne Einwilligung mehr als fünfmal verwenden wurden. Bezüglich der Frage, wie oft in den letzten zwei Jahren über die Verwendung und den potenziellen Missbrauch des Sammelns von Information gehört oder gelesen haben, haben 4,9 % der Teilnehmenden angegeben, dass dies kein Mal vorgefallen ist. Insgesamt 13,4 % der Teilnehmenden gaben an, ein bis zweimal von Datenmissbrauch gehört oder gelesen zu haben, während 20,7 % angaben, drei bis viermal davon Kenntnis genommen zu haben.

Weitere 61 % haben angegeben, mehr als fünfmal von Datenmissbrauch gehört oder gelesen zu haben. Die letzte Frage des MUIPCs sollte erfassen, wie oft die Teilnehmenden persönlich Opfer dessen waren, was sie als unangemessenen Eingriff in ihre Privatsphäre empfinden. Hier haben 50 % der Teilnehmenden angegeben, niemals diese Erfahrung gemacht zu haben, während 32,9 % angegeben haben, lediglich ein bis zweimal Opfer eines unangemessenen Eingriffs gewesen zu sein. Lediglich 7,3 % der Teilnehmenden haben angegeben, dass diese schlechte Erfahrung ihnen drei bis viermal widerfahren ist, wobei 9,8 % angegeben haben, den unangemessenen Eingriff auf ihre Privatsphäre erfahren zu haben (Tabelle 164, Anhang Y).

Weiterhin soll der Zusammenhang zwischen schlechten Erfahrungen und den Bedenken der Nutzenden über die Privatsphäre geprüft werden. Hierfür werden die Fragen bezüglich der schlechten Erfahrungen im MUIPC (Frage E2: Wie oft haben Sie persönlich Vorfälle innerhalb der letzten 2 Jahre erlebt, bei denen Ihre persönlichen Daten von Unternehmen oder E-Commerce-Webseiten ohne Ihre Genehmigung verwendet wurden? Und Frage E4: Wie oft waren Sie in den letzten zwei Jahren persönlich Opfer dessen, was Sie als unangemessenen Eingriff in ihre Privatsphäre empfanden?) mit den Bedenken, welche in den Fragen des Abschnittes E1 im Anhang U wiederzufinden sind, korreliert. Aufgrund der Abwesenheit einer Normalverteilung wird der Spearman-Rho-Test zwischen den Antworten der eben genannten Fragen durchgeführt. Beim Prüfen des Zusammenhanges zwischen den Antworten der Frage E2 mit denen aus E1 ergeben sich vier signifikante Korrelationen mit einer schwachen Effektstärke. Ein signifikanter Zusammenhang mit einer mittleren Effektstärke ergibt sich bei der Korrelation zwischen den Antworten der Frage E2 mit denen aus E4. Bezüglich der Aussagen:

Ich glaube, dass der Standort meines mobilen Gerätes zumindest zeitweise überwacht wird ($r(81) = 0{,}291$; $p < .008$),

Ich mache mir Sorgen, dass Applikationen zu viele Informationen über mich sammeln ($r(81) = 0{,}22$; $p < .048$),

Ich habe das Gefühl, dass aufgrund meiner Verwendung von Applikationen Informationen über mich verfügbar sind, die, wenn sie genutzt werden, in meine Privatsphäre eindringen ($r(80) = 0{,}243$; $p < .03$)

und

Wenn ich persönliche Informationen zur Verwendung von Applikationen herausgebe, habe ich Bedenken, dass die Applikationen meine Informationen für andere Zwecke benutzen ($r(81) = 0{,}258$; $p < .02$)

kann jeweils eine positive Korrelation mit einem schwachen signifikanten Effekt mit Hilfe des Spearman-Rho-Testes gefunden werden.

Beim Prüfen des Zusammenhanges zwischen den Antworten der Fragen E2 und E4:

Wie oft waren Sie in den letzten zwei Jahren persönlich Opfer dessen, was Sie als unangemessenen Eingriff in ihre Privatsphäre empfanden? ($r(81) = 0{,}413$; $p < .000$)

kann ebenfalls eine positive Korrelation, in diesem Fall mit einer mittleren Effektstärke festgestellt werden. Alle anderen Korrelationspaare ergeben kein signifikantes Ergebnis.

Weiterhin wird auf Zusammenhänge zwischen der eben genannten Frage E4 und den Bedenken im MUIPC geprüft. Nach der Durchführung des Spearman-Rho-Testes können neun signifikante Korrelationen festgestellt werden, darunter vier mit einer schwachen und fünf mit einer mittleren Effektstärke. Bezüglich der Aussagen:

Ich mache mir Sorgen, dass Applikationen zu viele Informationen über mich sammeln (r (81) = 0,296; $p < .007$),

Ich mache mir Sorgen, dass Applikationen meine Aktivitäten auf meinem mobilen Gerät überwachen (r (81) = 0,29; $p < .009$),

Ich glaube, dass aufgrund meiner Verwendung von Applikationen Informationen über mich, die ich für privat halte, jetzt besser für andere verfügbar sind als ich es möchte (r (81) = 0,276; $p < .013$)

und

Ich mache mir Sorgen, dass Applikationen meine persönlichen Daten mit anderen Instanzen teilen können, ohne meine Berechtigung einzuholen (r (80) = 0,244; $p < .029$),

kann jeweils eine positive Korrelation mit einem schwachen signifikanten Effekt mit Hilfe des Spearman-Rho-Testes gefunden werden.

Bezüglich der Aussagen:

Ich habe das Gefühl, dass andere durch meine Verwendung von Applikationen mehr über mich wissen als mir angenehm ist (r (81) = 0,314; $p < .004$),

Ich habe das Gefühl, dass aufgrund meiner Verwendung von Applikationen Informationen über mich verfügbar sind, die, wenn sie genutzt werden, in meine Privatsphäre eindringen (r (80) = 0,352; p < .001),

Ich mache mir Sorgen, dass Applikationen meine persönlichen Daten für andere Zwecke verwenden dürfen, ohne mich zu benachrichtigen oder meine Berechtigung einzuholen (r (80) = 0,36; p < .001),

Wenn ich persönliche Informationen zur Verwendung von Applikationen herausgebe, habe ich Bedenken, dass die Applikationen meine Informationen für andere Zwecke benutzen (r (81) = 0,33; p < .003)

und

Wie oft haben Sie persönlich Vorfälle innerhalb der letzten 2 Jahre erlebt, bei denen Ihre persönlichen Daten von Unternehmen oder E-Commerce-Webseiten ohne Ihre Genehmigung verwendet wurden? (r (81) = 0,413; p < .000)

kann jeweils eine positive Korrelation mit einem mittleren signifikanten Effekt mit Hilfe des Spearman-Rho-Testes gefunden werden.

6.8.6.5 Relevanz der Methoden zur Applikationsbewertung

Beim Vergleich der verschiedenen Applikationsbewertung sollten die Teilnehmenden angeben, welche der folgenden Bewertungen für sie am relevantesten ist. Hierbei sollten sie die Relevanz der Rezension (Einzelbewertungen), der Sternenbewertungen, der Aufrufe der Applikation im App-Markt, der Anzahl an Downloads der Applikation und der Privatsphäreskala für die Applikationsauswahl angeben. Anhand Tabelle 165 im Anhang Y ist zu erkennen, dass der höchste Mittelwert von 5,68 (SD = 1,2) bei der Privatsphäreskala zu finden ist. Darauf folgen die Rezensionen mit M = 5,54 (SD = 1,23). Der dritthöchste Mittelwert von 5,37 (SD = 1,25) ist bei der Sternenbewertung wiederzufinden, während die Anzahl an Downloads den zweitniedrigsten Mittelwert von 4,78 (SD = 1,5) aufzeigt. Der niedrigste Mittelwert von 4,26 (SD = 1,56) ist bei den Aufrufen der Applikation zu sehen.

Auf Grund der Abwesenheit einer Normalverteilung wird ein Friedman-Test (s. Tabelle 166, Anhang Y) über alle Bewertungsmethoden durchgeführt. Dieser ergibt mit χ^2 = 60,35 und p < .000 ein signifikantes Ergebnis. Um zu überprüfen, welche Bewertungsmethoden sich voneinander unterscheiden, werden zusätzlich zehn paarweise Vergleiche mit Hilfe des Wilcoxon-Tests durchgeführt, von denen acht ein signifikantes Ergebnis aufzeigen (Sterne und Rezension (z = -3,4; p < .249; r = 0,09); Aufrufe und

Rezension (z = -5,681; p < .000; r = 0,45); Downloads und Rezension (z = -4,003; p < .000; r = 0,31); (Datenschutzskala und Rezension (z = -0,904; p < .366; r = 0,07); Aufrufe und Sterne (z = -4,954; p < .000; r = 0,39); Downloads und Sterne (z = -3,287; p < .001; r = 0,26); Datenschutzskala und Sterne (z = -1,996; p < .046; r = 0,16); (Datenschutzskala und Aufrufe (z = -5,653; p < .000; r =0,45); Datenschutzskala und Downloads (z = -4,303; p < .000; r = 0,34); Downloads und Aufrufe (z = -2,887; p < .004; r = 0,27). Lediglich der Vergleich zwischen der Sternebewertung und der Rezension sowie der Datenschutzskala und der Rezension ergeben keine signifikanten Unterschiede (s. Tabelle 167, Anhang Y).

Bei dem Vergleich der Applikationsbewertungen zwischen den Gruppen fällt auf, dass die Anzahl an Downloads stets mit der niedrigsten Relevanz bewertet wird (Gruppe A: M = 4,29 SD = 1,65; B: M = 4,83 SD = 1,62; C: M = 4,09 SD = 1,44; D: M = 3,71 SD = 1,45), während die Downloads (Gruppe A: M = 4,62 SD = 1,53; B: M = 5,17 SD = 1,25; C: M = 4,35 SD = 1,72; D: M = 5,18 SD = 1,38) über alle Gruppen hinweg mit der zweitniedrigsten Relevanz bewertet werden. Nur in Gruppe A wird die Relevanz der Rezensionen mit M = 6,1 (SD = 0,89) am höchsten, die Datenschutzskala mit M = 5,86(SD = 1,11) am zweithöchsten und die Sternebewertung mit M = 5,29 (SD = 1,38) am dritthöchsten bewertet. Von Gruppe B bis D werden die Datenschutzskala (Gruppe B: M = 4,83 SD = 1,62; C: M = 4,09 SD = 1,44; D: M = 3,71 SD = 1,45) am höchsten, die Sternebewertung (Gruppe B: M = 5,50 SD = 0,86; C: M = 5,13 SD = 1,42; D: M = 5,76 SD = 1,09) am zweithöchsten und die Rezensionen (Gruppe B: M = 5,33 SD = 1,14; C: M = 5 SD = 1,54; D: M = 5,76 SD = 0,97) am dritthöchsten bewertet. Für den besseren Überblick werden die Mittelwerte getrennt nach den Gruppen in Tabelle 165 im Anhang Y aufgeführt.

Anschließend wird ein Kruskal-Wallis-Test durchgeführt, um zu prüfen ob die Gruppen sich signifikant unterscheiden. Dabei ergibt sich lediglich ein Unterschied bei den Rezensionen mit p < .025 (s. Tabelle 168, Anhang Y). Bei dem paarweisen Vergleich mit Hilfe des Mann-Whitney-U-Testes (s. Tabelle 169, Tabelle 170, Tabelle 171, Tabelle 172, Tabelle 173, Tabelle 174, Anhang Y) kann lediglich ein signifikanter Unterschied bezüglich der Rezensionen zwischen den Gruppen A und B (U = 115,5; z = -2,15; p < .031; r = 0,36) sowie A und C (U = 127,5; z = -2,79; p < .005; r = 0,42) festgestellt werden. Alle weiteren Vergleiche ergeben keine signifikanten Ergebnisse. Bei zwei normalverteilten Datensätzen wird ein t-Test mit unabhängigen Stichproben durchgeführt. Hieraus resultieren jedoch ebenfalls keine signifikanten Ergebnisse (s. Tabelle 175, Anhang Y).

6.8.7 Zusammenhang zwischen der Auswahl der Applikation (Score) und den Bedenken über den Datenschutz (MUIPC)

Um den Zusammenhang zwischen den Scores der ausgewählten Applikationen und dem Ergebnis des Fragebogens zur Messung der Bedenken von Mobilfunknutzern hinsichtlich des Datenschutzes zu ermitteln, werden mögliche Zusammenhänge zwischen den Scores und den 13 Items des MUIPCs geprüft. Hierfür werden zunächst alle Datensätze mit Hilfe des Kolmogorov-Smirnov-Tests auf Normalverteilung geprüft. Dieser ergibt, dass innerhalb des Datensatzes des Messenger-Scores und des Videokonferenz-Scores eine normale Verteilung herrschte. Bezüglich des MUIPCs konnte keine Normalverteilung bei allen der Items festgestellt werden. Darüber hinaus sind die Datensätze, welche erfassen, wie oft die Teilnehmenden über Datenmissbrauch gehört oder gelesen haben, beziehungsweise selbst Opfer eines Datenmissbrauchs waren, ebenfalls nicht normalverteilt. In Tabelle 176 im Anhang Y können sowohl die deskriptiven Werte als auch die Normalverteilung abgelesen werden.

Wegen der Abwesenheit einer Normalverteilung bei allen Datensätzen bezüglich des MUIPC wird die Spearman-Rho-Korrelation angewandt (s. Tabelle 177, Anhang Y). Zwischen dem Score der ausgewählten Applikation des Wetters und den Bedenken der Teilnehmenden bezüglich des Datenschutzes kann kein Zusammenhang festgestellt werden. Beim Prüfen des Zusammenhangs des E-Mail-Scores mit den Ergebnissen des MUIPCs ergeben sich zwei schwache und vier mittlere signifikante Effekte. Bezüglich der Aussagen:

Ich glaube, dass der Standort meines mobilen Gerätes zumindest zeitweise überwacht wird ($r(60) = 0{,}255$; $p < .05$),

Ich habe das Gefühl, dass andere durch meine Verwendung von Applikationen mehr über mich wissen als mir angenehm ist ($r(60) = 0{,}287$; $p < .02$) konnte jeweils eine positive Korrelation mit einem kleinen signifikanten Effekt mit Hilfe des Spearman-Rho-Testes gefunden werden.

Bei den Aussagen:

Ich habe das Gefühl, dass aufgrund meiner Verwendung von Applikationen Informationen über mich verfügbar sind, die, wenn sie genutzt werden, in meine Privatsphäre eindringen ($r(60) = 0{,}323$; $p < .01$),

Ich mache mir Sorgen, dass Applikationen meine persönlichen Daten für andere Zwecke verwenden dürfen ohne mich zu benachrichtigen oder meine Berechtigung einzuholen ($r(59) = 0{,}344$; $p < .01$),

Wenn ich persönliche Informationen zur Verwendung von Applikationen herausgebe, habe ich Bedenken, dass die Applikationen meine Informationen für andere Zwecke benutzen ($r(60) = 0{,}315$; $p < .01$) und

Ich mache mir Sorgen, dass Applikationen meine persönlichen Daten mit anderen Instanzen teilen können ohne meine Berechtigung einzuholen ($r(59) = 0{,}316$; $p < .01$) konnte jeweils eine positive Korrelation mit einem mittleren signifikanten Effekt mit Hilfe des Spearman-Rho-Testes gefunden werden. Alle anderen Korrelationspaare ergeben kein signifikantes Ergebnis.

Der gleiche Test wird zum Korrelieren des Musik-Scores und der Aussagen

Ich glaube, dass der Standort meines mobilen Gerätes zumindest zeitweise überwacht wird ($r(60) = -0{,}302$; $p < .02$) durchgeführt. In diesem Fall ergibt sich eine negative Korrelation mit mittlerer Effektstärke.

Bei näherer Betrachtung der Korrelation zwischen den Ergebnissen des MUIPCs und des Szenarios Fitness ist lediglich ein signifikanter Zusammenhang bei der Aussage:

Wie oft haben Sie in den letzten zwei Jahren über die Verwendung und den potenziellen Missbrauch des Sammelns von Informationen gehört oder gelesen? ($r(59) = 0{,}344$; $p < .01$) mit mittlerem Effekt zu finden.

Bei den Korrelationen zwischen den Ergebnissen des MUIPCs und des Szenarios Nachrichten ergibt sich ein positiver Zusammenhang bei der Aussage:

Ich mache mir Sorgen, dass Applikationen meine Aktivitäten auf meinem mobilen Gerät überwachen ($r(60) = 0{,}266$; $p < .04$) mit kleinem Effekt.

Bei den Korrelationen zwischen den Ergebnissen des MUIPCs und dem Score der Szenarien Spiele und Messenger ergeben sich keine signifikanten Zusammenhänge. Bezüglich der Videokonferenz ergab lediglich die Korrelation zwischen dem Score dieser und der Aussage des MUIPCs

Wenn ich persönliche Informationen zur Verwendung von Applikationen herausgebe, habe ich Bedenken, dass die Applikationen meine Informationen für andere Zwecke benutzen ($r(60) = 0{,}267$; $p < .04$) einen kleinen signifikanten Effekt.

Die Ergebnisse aller Spearman-Rho-Korrelationen können der Tabelle 177 im Anhang Y entnommen werden.

6.9 Diskussion

In dem folgenden Kapitel werden die Ergebnisse nach Hypothesen geordnet diskutiert. Hierbei wird zunächst der Einfluss der Datenschutzskala auf die Einfachheit der Applikationsauswahl und die Vertrauenswürdigkeit der Applikationen diskutiert (Hypothese 1). Anschließend wird näher betrachtet, ob die Implementierung einer Datenschutzskala in den App-Markt Einfluss auf das Auswahlverhalten der Applikationen hat. Hierbei wird insbesondere darauf geachtet, ob durch die Einbettung der Datenschutzskala in den App-Markt Applikationen häufiger gewählt werden, die als „sicher“ und „sehr sicher“ gekennzeichnet sind (Hypothese 2). In dem dritten Unterkapitel wird diskutiert, ob die Datenschutzskala einen Einfluss auf die Entscheidungszeiten zu der Wahl von Applikationen für die gestellten Aufgaben mit sich bringt. Hierbei soll ermittelt werden, ob bei Wiederholung des Auswahlprozesses mit implementierter Datenschutzskala eine Reduzierung der Entscheidungszeit zu verzeichnen ist (Hypothese 3). Das vierte Unterkapitel beschäftigt sich mit dem Einfluss der Datenschutzskala auf die Fixationszeiten der Teilnehmenden bezüglich der verschiedenen Bereiche im App-Markt und vergleicht die Zeiten der vier Gruppen untereinander (Hypothese 4).

Mit dem fünften Unterkapitel beginnt die Diskussion der explorativen Ergebnisse. Hierbei wird näher betrachtet, ob sich die Entscheidungszeiten zwischen den Szenarien, wie zum Beispiel „Musik“ und „Messenger“, unterscheiden. Anschließend werden im sechsten Unterkapitel die Entscheidungszeiten der einzelnen Szenarien zwischen den Gruppen untereinander verglichen. In dem siebten Unterkapitel wird diskutiert, welchen Einfluss die Bekanntheit einer Applikation seitens der Teilnehmenden auf deren Auswahlverhalten hat. Die Bewertung der Datenschutzskala ist Bestandteil des achten Unterkapitels, wobei der Fokus besonders auf die Eignung der Datenschutzskala zur Illustrierung der Aggressivität der Applikationen liegt. Das neunte Unterkapitel beinhaltet die Diskussion der Ergebnisse des MUIPCs, während das zehnte Unterkapitel den Zusammenhang dieser mit den Ergebnissen der Applikationsauswahl behandelt. Abschließend werden im letzten Unterkapitel die Ergebnisse der Interviews, welche mit Hilfe von Videokonfrontationen geführt wurden, diskutiert.

6.9.1 Zur Hypothese 1: Diskussion der Einfachheit der Applikationsauswahl und Vertrauenswürdigkeit der Applikation

Hypothese 1:

Die Gruppen, welche eine Datenschutzskala zur Verfügung haben und mehr Informationsgehalt über diese erhalten, bewerten die Vertrauenswürdigkeit der Applikation adäquater hinsichtlich deren

Aggressivität als jene Gruppen ohne Datenschutzskala oder mit weniger Informationsgehalt über diese.

Hypothese 1a:

Die Gruppe (A) der Nutzenden, die eine Datenschutzskala mit einer detaillierten Beschreibung erhält, bewertet die Vertrauenswürdigkeit der Applikation adäquater hinsichtlich deren Aggressivität als die Gruppe (B), die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält. Außerdem wird angenommen, dass die Gruppe (A) die Vertrauenswürdigkeit auch exakter bewertet als die Gruppe (C), welche zur Datenschutzskala keine detaillierte Beschreibung erhält und die Gruppe (D), die keine Datenschutzskala erhält.

Bei der Betrachtung der Mittelwerte bezüglich der Beträge der Differenzen zwischen der Likert-Skala, auf der sie die Vertrauenswürdigkeit der Applikationen bewerten sollten, und der Datenschutzskala, welche die Applikation in fünf Risikogruppen kategorisiert, fällt auf, dass bei allen drei angewandten Methoden die geringsten Mittelwerte meist in der Gruppe A wiederzufinden sind. In Gruppe B sind ebenfalls bei allen drei Methoden am häufigsten die zweitniedrigsten Werte zu finden. Die Gruppe C weist ebenfalls der Hypothese entsprechend bei allen drei Methoden die zweithöchsten Werte auf, während die Gruppe D bei allen Methoden die meisten höchsten Beträge der Differenzen enthält.

Aufgrund der Tatsache, dass die erste Methode die Skala von sieben auf fünf Stufen staucht, resultieren hier die meisten adäquaten Ergebnisse mit einer Differenz zwischen diesen Skalen von null. Grund dafür ist die Zusammenführung der ersten beiden und der letzten beiden Stufen zu jeweils einer Stufe. Durch die Verringerung der Stufen ist die Wahrscheinlichkeit höher, eine adäquate Antwort abzugeben. Dies ist vor allem an den Differenzen der Vertrauenswürdigkeit und der Datenschutzskala zu erkennen. Während in der ersten Methode 208 Schätzungen richtig liegen, sind es in der zweiten Methode nur 90 und in der dritten Methode nur 59. Hinzu kommen noch weitere Vor- und Nachteile der einzelnen Methoden, welche jedoch schon in Abschnitt 6.7.3.1 näher erläutert wurden. Generell kann davon ausgegangen werden, dass eine höhere Anzahl von Stufen in der Skala eine geringere Übereinstimmung zwischen der eingeschätzten Vertrauenswürdigkeit und der Kategorisierung der Datenschutzskala mit sich bringt. Aus den Mittelwerten der Beträge der Differenzen lässt sich eine deutliche Tendenz entsprechend der Hypothese 1 bei allen drei Methoden aufweisen. So sind bei allen drei Methoden jeweils in Gruppe A am häufigsten die niedrigsten und somit adäquatesten Werte wiederzufinden. Hieraus kann geschlossen werden, dass die Gruppe A, mit Datenschutzskala und einer vorgelegten Erläuterung über diese, eine Tendenz aufweist, die Applikation adäquater zu beurteilen als die Gruppen B, C und D.

Nach der Durchführung des Kruskal-Wallis-Testes kann jedoch lediglich in den ersten beiden Methoden eine Signifikanz in dem Szenario des Wetters aufgezeigt werden. Weiterhin kann ein signifikantes Ergebnis im Szenario der Spiele bei der zweiten und dritten Methode sowie im Szenario der Nachrichten, jedoch nur bei der ersten Methode gefunden werden. Bei den paarweisen Vergleichen zwischen den Gruppen ergeben sich mit Hilfe des Mann-Whitney-U-Tests nur zehn signifikante Unterschiede in der ersten, vier in der zweiten und sechs in der dritten Methode. Um auszuschließen, dass die Signifikanz der Ergebnisse von der Methode abhängt, werden nur die Ergebnisse als signifikant angesehen, deren Signifikanz in allen drei Methoden bestätigt wurde.

Hierunter fallen die paarweisen Vergleiche zwischen den Gruppen A und C sowie A und D im Szenario der Spiele. Ferner ist im Szenario des Wetters zwischen der Gruppe A und D bei allen drei Methoden ein signifikantes Ergebnis wiederzufinden. Die Mittelwerte der Beträge der Differenzen zwischen der geschätzten Adäquatheit und der Kategorisierung der Applikation durch die Datenschutzskala, die bei allen drei Methoden die niedrigsten Werte meist in Gruppe A aufweisen, tragen zu einer Annahme der Hypothese 1a bei. Aufgrund der Tatsache, dass sich jedoch nur ein Mittelwert signifikant von Gruppe C und zwei von Gruppe D unterscheiden, kann die Hypothese nur teilweise bestätigt werden.

Hypothese 1b:

Die Gruppe (B) der Nutzenden, die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält, bewertet die Vertrauenswürdigkeit der Applikation adäquater hinsichtlich deren Aggressivität als die Nutzenden (Gruppe C), die eine Datenschutzskala ohne detaillierte Beschreibung erhalten und die Gruppe (D), die keine Datenschutzskala erhält.

Die zweitniedrigsten Mittelwerte der Beträge der Differenzen sind, unter Anwendung aller drei Methoden, meist in Gruppe B wiederzufinden. Somit kann auch hier von einer Tendenz entsprechend der Hypothese davon ausgegangen werden, dass die Teilnehmenden die Vertrauenswürdigkeit der gewählten Applikation adäquater als Gruppe C und D, jedoch nicht als Gruppe A beurteilt haben. Bei der Betrachtung der paarweisen Vergleiche bezüglich der Szenarien zwischen den Gruppen fällt jedoch auf, dass kein einziger Unterschied als signifikant resultierte. Weil lediglich eine der Hypothese entsprechende Tendenz der Mittelwerte der Beträge der Differenzen aufgezeigt werden kann, jedoch nicht ein signifikanter Unterschied zwischen den Gruppen zu finden ist, kann die Hypothese 1b nicht weiter aufrechterhalten werden. Somit konnten die Teilnehmenden der Gruppe B keine adäquatere Einschätzung der Vertrauenswürdigkeit durch die Datenschutzskala erzielen.

Hypothese 1c:

Die Gruppe (C) der Nutzenden, die eine Datenschutzskala ohne detaillierte Beschreibung gezeigt bekommt, bewertet die Vertrauenswürdigkeit der Applikation adäquater hinsichtlich deren Aggressivität als die Gruppe (D), die keine Datenschutzskala erhält.

Die zweithöchsten Mittelwerte der Beträge der Differenzen sind, unter Anwendung aller drei Methoden, meist in Gruppe C wiederzufinden. Somit kann, wie in Hypothese 1a und 1b, auch hier von einer Tendenz entsprechend der Hypothese 1c ausgegangen werden, sodass die Teilnehmenden die Vertrauenswürdigkeit der gewählten Applikation adäquater als Gruppe D, jedoch nicht als Gruppe A und B beurteilt haben. Die paarweisen Vergleiche bezüglich der Szenarien zwischen den Gruppen zeigen jedoch wieder keinen Unterschied, der bei allen drei Methoden als signifikant resultiert. Weil lediglich eine der Hypothesen entsprechende Tendenz der Mittelwerte der Beträge der Differenzen aufgezeigt werden kann, jedoch kein signifikanter Unterschied zwischen den Gruppen zu finden ist, kann auch die Hypothese 1c nicht weiter aufrechterhalten werden. Somit konnten die Teilnehmenden der Gruppe C keine adäquatere Einschätzung der Vertrauenswürdigkeit durch die Datenschutzskala erzielen.

Allgemein ist jedoch bei allen drei Gruppen eine Tendenz entsprechend der Hypothese 1 ersichtlich, wobei die Mittelwerte der Gruppe A drei signifikante Unterschiede aufweisen. Aus diesem Grund kann die Hypothese insgesamt nur teilweise bestätigt werden. Die Tendenzen lassen vermuten, dass unter Verwendung einer größeren Stichprobe die Signifikanz der Ergebnisse gesteigert werden kann, sodass eine Annahme der Hypothese unter einer umfangreicheren Testung sehr wahrscheinlich ist.

Abgesehen von den Vergleichen zwischen den Gruppen fällt auf, dass die gewählten Applikationen im Szenario der Musik unabhängig der Methode stets am adäquatesten bewertet wurden. Alle anderen Szenarien weisen je nach angewandter Methode unterschiedliche Ergebnisse auf.

Bei der Betrachtung der Mittelwerte bezüglich der Beträge der Differenzen zwischen der Likert-Skala, auf der sie die Vertrauenswürdigkeit der Applikationen bewerten sollten, und der Datenschutzskala, welche die Applikation in fünf Risikogruppen kategorisiert, fällt auf, dass bei allen drei angewandten Methoden die geringsten Mittelwerte meist in der Gruppe A wiederzufinden sind. So weist die Gruppe A lediglich bei den drei Szenarien E-Mail, Musik und Spiele höhere Werte auf.

Die Mittelwerte des Szenarios der Videokonferenz sind bei den Gruppen A und B gleich, während die Szenarien E-Mail, Spiele und Musik einen höheren Mittelwert in der Gruppe A aufweisen. Allerdings kann bei dem Vergleich der Mittelwerte aller Szenarien zwischen Gruppe A und B nicht ein signifikanter

Unterschied festgestellt werden. Werden die Mittelwerte der Gruppe A und C verglichen, so sind mit Ausnahme des Szenarios der Videokonferenz die höchsten Mittelwerte aller anderen Szenarien bei der Gruppe A wiederzufinden. Nach den Signifikanztests kann jedoch lediglich jeweils ein signifikanter Unterschied zwischen den Mittelwerten im Szenario der E-Mail und der Spiele beobachtet werden. Werden die Mittelwerte der Gruppen A und D miteinander verglichen, so stimmen die Ergebnisse größtenteils mit der Aussage der Hypothese überein. Mit Ausnahme des Szenarios Messenger verzeichnen alle weiteren sieben Szenarien die höchsten Mittelwerte bei Gruppe A. Nach dem paarweisen Vergleich können bei drei Szenarien signifikante Unterschiede festgestellt werden. Hierzu zählen das Szenario der E-Mail, der Fitness, jedoch auch der Videokonferenz, in dem der Mittelwert in Gruppe D höher ist als in Gruppe A. Bei den übrigen fünf Szenarien kann lediglich eine Tendenz einer adäquateren Beurteilung bezüglich der Vertrauenswürdigkeit beobachtet werden.

Aus Tabelle 115 im Anhang Y ist zu entnehmen, dass mit Ausnahme der Kategorie Messenger die Mittelwerte für die Einfachheit der Auswahl der Applikation in den Gruppen mit Datenschutzskala am höchsten sind. Beim Bewerten der Vertrauenswürdigkeit der Applikation können durchweg die höchsten Mittelwerte in den Gruppen mit Datenschutzskala wiedergefunden werden. Darüber hinaus ergibt sich aus den Ergebnissen, dass für die Applikationskategorien Videokonferenz, Wetter, E-Mail, Fitness und Nachrichten die Applikationen signifikant besser auf ihre Vertrauenswürdigkeit von Teilnehmenden, welche die Datenschutzskala zur Verfügung hatten, beurteilt wurden, als die, die keine Datenschutzskala zur Verfügung hatten. Diese Ergebnisse lassen sich wiederum mit der Popularität der Applikation erklären. Am Beispiel der Videokonferenzapplikation Skype kann gesehen werden, dass eine populäre Applikation in Kombination mit einer sicheren Klassifizierung auf der Datenschutzskala zu einer höheren Bewertung bei der Vertrauenswürdigkeit führt als bei einer Applikation ohne Datenschutzskala. Eine populäre Applikation mit einer unsicheren Klassifizierung, innerhalb einer Kategorie, wie die Messengerapplikation WhatsApp, führt zu einer geringeren Bewertung der Vertrauenswürdigkeit, weil die Applikation aufgrund ihrer Popularität trotz der unsicheren Einstufung auf der Datenschutzskala gewählt wird. Dabei ist sich die Testperson der Unsicherheit jedoch bewusst und gibt somit eine geringere Vertrauenswürdigkeit für die Applikation an.

Ist die Applikation nicht bekannt und kategorisiert die Datenschutzskala sie als sicher, wird die Vertrauenswürdigkeit der Applikation als hoch bewertet. Eine unpopuläre Applikation mit einer unsicheren Einstufung durch die Datenschutzskala wird meist nicht gewählt und hat somit keinen Einfluss auf die Bewertung. Eine populäre Applikation ohne Datenschutzskala ist stark von ihrem Ruf und ihrer Nachrichtenaktualität abhängig, was aus den Interviews herauszulesen ist.

Ein ähnliches Verhalten ist bei der Einfachheit der Auswahl zu sehen. Dort haben lediglich die Kategorien Wetter und Fitness einen signifikant höheren Mittelwert. In diesen beiden Kategorien gibt es keine favorisierte Applikation, was dazu geführt hat, dass die Datenschutzskala den Teilnehmenden die Auswahl signifikant vereinfacht hat.

Ein Zusammenhang zwischen der Technikaffinität und der Adäquatheit der Bewertung der Vertrauenswürdigkeit der Applikation kann lediglich bei der prozentualen Methode der Reskalierung im Szenario der Videokonferenz festgestellt werden.

Es ist jedoch davon auszugehen, dass dieser negative Zusammenhang eher zufällig signifikant ist, vor allem, weil bei den anderen Reskalierungsmethoden kein signifikanter Zusammenhang ermittelt werden kann.

Bei Prüfen der Zusammenhänge zwischen der Adäquatheit der Bewertung der Vertrauenswürdigkeit der Applikation und dem Geschlecht, dem Bildungsabschluss, der Privatsphäre und den Stunden der Nutzung eines Endgerätes können keine signifikanten Ergebnisse gefunden werden. Somit haben die eben genannten Variablen ebenfalls keinen Einfluss auf die Adäquatheit der Bewertung der Vertrauenswürdigkeit der Applikation. Beim Alter kann lediglich ein signifikanter, negativer Zusammenhang bezüglich des Szenarios des Messengers festgestellt werden. Somit kann davon ausgegangen werden, dass ältere Nutzende die Messenger adäquater bezüglich ihrer Vertrauenswürdigkeit bewerten als jüngere Nutzende. Diese Erkenntnis kann damit begründet werden, dass jüngere Nutzende durch den häufigen Umgang mit diversen Messengers ein gewisses Vertrauen aufbauen, selbst wenn dieses Vertrauen unbegründet ist. Allein durch häufige Nutzung und die Uneinsehbarkeit der Konsequenzen, welche bereits in Abschnitt 2.2.9 erläutert wurden, bewerten die Endnutzenden die Applikation als vertrauenswürdig.

6.9.2 Zur Hypothese 2: Diskussion über die Angemessenheit ausgewählter Applikationen

Wie schon in Abschnitt 2.2.4 beschrieben, ist es den Endnutzenden derzeit nicht möglich nachzuverfolgen, an wen ihre Daten ausgehändigt werden. Selbst bei der Nutzung von Applikationen eines spezifischen Anbieters kann nicht ausgeschlossen werden, dass dieser seine Daten an Dritte weitergibt, wodurch derzeit die größten Unternehmen im Bereich der Suchmaschinen, des Online-Einkaufs und sozialer Medien die meisten Gewinne machen. Umso bedeutender wird die Kontrolle der eigenen Daten beim Herunterladen und Nutzen von Applikationen. Diese Kontrolle sollte mit Hilfe der Datenschutzskala ermöglicht werden. In Abschnitt 6.8.4 wurde bereits erläutert, wie aus dem Auswahlverhalten ein Score errechnet werden kann.

Hypothese 2:

Mit zunehmender Information über die Applikationen bezüglich des Datenschutzes werden weniger aggressive Applikationen gewählt.

Hypothese 2a:

Die Gruppe (A) der Nutzenden, die eine Datenschutzskala mit einer detaillierten Beschreibung erhält, wählt weniger aggressive Applikationen als die Gruppe (B), die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält, die Gruppe (C) die keine detaillierte Beschreibung erhält und die Gruppe (D), die keine Datenschutzskala erhält.

Zwischen den Gruppen A und B konnten zwar drei signifikante Unterschiede bezüglich der Scores in den Szenarien Videokonferenz, E-Mail und Musik festgestellt werden, wobei das Szenario Musik jedoch den höchsten Score in Gruppe B erlangte. Auch bei Vergleichen der Gruppe A mit der Gruppe C kann festgestellt werden, dass die Mittelwerte aller Szenarien höher in Gruppe A als in Gruppe C sind. Allerdings zeigt nur das Szenario der Nachrichten einen signifikant höheren Mittelwert bei Gruppe A mit Vergleich zu Gruppe C. Somit kann hier nur von einer Tendenz der Gruppe A gesprochen werden, eine Auswahl sicherer Applikationen im Vergleich zu Gruppe B zu tätigen. Werden die Gruppen A und D miteinander verglichen, so entsprechen die Ergebnisse eher der aufgestellten Hypothese. In Gruppe D sind bei sechs von acht Szenarien die tiefsten Mittelwerte wiederzufinden. Darüber hinaus sind auch die Mittelwerte der anderen beiden Szenarien niedriger als die, die in Gruppe A wiederzufinden sind. Beim Betrachten der signifikanten Unterschiede zeigen fünf der acht Szenarien einen großen Effekt auf. So kann in diesem Fall davon ausgegangen werden, dass die Gruppe A eine deutlich sicherere Auswahl bezüglich der Datensicherheit im Vergleich zu Gruppe B tätigte.

Somit kann die Hypothese 2a nur teilweise beibehalten werden.

Hypothese 2b:

Die Gruppe (B) der Nutzenden, die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält, wählt weniger aggressive Applikationen als die Gruppe (C), die eine Datenschutzskala ohne detaillierte Beschreibung gezeigt bekommt und die Gruppe (D), die keine Datenschutzskala erhält.

Werden die Gruppen B und C verglichen, so fällt auf, dass sechs der acht Szenarien einen höheren Mittelwert in Gruppe B aufweisen. Lediglich das Szenario der Videokonferenz und der E-Mail weisen einen höheren Mittelwert in Gruppe C auf. Aufgrund der Tatsache, dass lediglich ein signifikanter

Unterschied im Szenario der Musik zwischen der Gruppe B und C mit einem mittleren Effekt festgestellt wird, kann hier ebenfalls nur von einer Tendenz gesprochen werden.

Beim Vergleich der Gruppen B und D sind alle höheren Mittelwerte mit Ausnahme des Szenarios Videokonferenz in Gruppe B wiederzufinden. Weiterhin können fünf signifikante Unterschiede im Szenario des Wetters mit einem mittleren Effekt, im Szenario der Musik, der Fitness, der Spiele und der Nachrichten mit einem großen Effekt ermittelt werden. Das Szenario der Videokonferenz, bei dem der größere Mittelwert in Gruppe D wiederzufinden ist, weist dementsprechend keinen signifikanten Unterschied auf.

Somit kann die Hypothese 2b für sechs der acht Szenarien beibehalten werden.

Hypothese 2c:

Die Gruppe (C) der Nutzenden, die eine Datenschutzskala ohne detaillierte Beschreibung erhält, wählt weniger aggressive Applikationen als die Gruppe (D), die keine Datenschutzskala erhält.

Werden die Gruppen C und D miteinander verglichen, so sind hier die höchsten Mittelwerte von sieben der acht Szenarien in Gruppe C wiederzufinden. Allerdings können lediglich die Szenarien Fitness und Spiele einen signifikanten Unterschied aufweisen, weshalb auch hier nur von einer Tendenz der datenschutzfreundlicheren Auswahl bei Gruppe C im Vergleich zu Gruppe D die Rede sein kann.

Weiterhin ist anzumerken, dass beim Vergleichen der Datenschutzscores der verschiedenen Applikationskategorien zwischen den verschiedenen Gruppen auffällt, dass die höchsten Mittelwerte der Scores in den Applikationskategorien Messenger, Videokonferenz, Wetter und E-Mail in der Gruppe A liegen und die höchsten Mittelwerte der Scores in den Applikationskategorien Musik, Fitness, Spiele und Nachrichten in der Gruppe B liegen. Bei der Prüfung auf einen signifikanten Unterschied mit Hilfe des Mann-Whitney-U Tests ergibt sich jedoch kein signifikanter Unterschied.

Betrachten wir jedoch die niedrigsten Scores, so fällt auf, dass mit Ausnahme der Applikationskategorien Messenger und Videokonferenz, diese stets in Gruppe D (ohne Datenschutzskala) wiederzufinden sind. Beim Test auf signifikante Unterschiede (Kruskal-Wallis-Test) können in allen Applikationskategorien, außer der des Messengers und der Videokonferenz, signifikante Unterschiede festgestellt werden. Somit hat die Datenschutzskala einen signifikanten Einfluss auf das Auswahlverhalten und führt bei den Kategorien Wetter, E-Mail, Musik, Fitness, Spiele und Nachrichten zu einer Auswahl von weniger invasiven Applikationen. Die nicht vorhandene Signifikanz beim Vergleich von Messenger und Videokonferenz lässt sich mit der Popularität der Applikationen erklären. Aus den Interviews geht hervor, dass die meisten Versuchspersonen eine

Applikation auswählten, die sie bereits kennen. Auch aus dem ersten Teil des Fragebogens geht hervor, dass meist die Applikation für die Aufgabe ausgewählt wird, die den Nutzenden bereits bekannt ist, beziehungsweise von den Nutzenden verwendet wird. Des Weiteren zeigen die Ergebnisse, dass sich 63,4 % der Teilnehmenden für die Applikation WhatsApp entschieden haben und sich die restlichen 36,6 % zwischen den übrigen Applikationen aufteilen. Ähnliche Ergebnisse sind für die Appkategorie Videokonferenz ablesbar, in der Skype von 72 % der Teilnehmenden und Viber von 17,1 % der Teilnehmenden gewählt wurden, wobei sich die restlichen 10,9 % zwischen den anderen Applikationen aufteilen. Werden die Werte mit denen der Kategorie Wetter verglichen, welche deutlich homogener verteilt sind, ist zu erkennen, weshalb hier keine signifikanten Unterschiede gefunden werden können (Wetter-Online = 26,8 %, Wetter.com = 22 %, Wetter.de = 22 %, Morecast = 19,5 %, Weatherzone = 2,4 %, Bayer Agrar Wetter = 2,4 %, Yr = 1,2 %). Somit könnte der Schluss gezogen werden, dass mit ansteigender Popularität der Applikation der Einfluss der Datenschutzskala sinkt. Einen ähnlichen Befund kann Staiano et al. (2014) in der Studie, welche im Abschnitt 2.2.7 vorgestellt wurde, vorzeigen. Dieser ergibt, dass mit ansteigender Nutzung der Applikation ein geringeres Einstufen der persönlichen Daten einhergeht.

Darüber hinaus ist die Wichtigkeit der Beschreibung der Datenschutzskala anhand der Vergleiche zwischen der Gruppe D und den einzelnen Gruppen A, B und C zu erkennen. Während in Gruppe A signifikante Unterschiede in sechs und in Gruppe B signifikante Unterschiede in fünf Kategorien wiederzufinden sind, so lassen sich zwischen C und D nur zwei Applikationskategorien, Fitness und Spiele, aufzeigen, deren Mittelwerte signifikant voneinander abweichen. Trotzdem ist zu erwähnen, dass alle Mittelwerte der Gruppen A bis C, mit Ausnahme von der Kategorie Messenger, höher sind als die Mittelwerte der Gruppe D.

Anhand der Ergebnisse ist ein signifikanter Einfluss der Datenschutzskala auf das Auswahlverfahren in den Kategorien Wetter, E-Mail, Musik, Fitness, Spiele und Nachrichten zu erkennen. Dies führt zu einer Auswahl weniger invasiver Applikationen. Diese Erkenntnisse bezüglich der Berücksichtigung der Datenschutzskala stimmen auch mit der Studie von Tsai et al. (2011), welche im Abschnitt 2.2.11 vorgestellt wurde, überein. Die Studie zeigt eine höhere Bereitschaft eines finanziellen Aufwandes bei Onlineeinkaufsportalen, die durch ein Symbol, welches die verschiedenen Portale bzw. die Datenschutzfreundlichkeit kennzeichnet, auf. Auch hier spiegelt sich im Verhalten der Teilnehmenden der Wunsch nach Datensicherheit und Privatsphäre wider. Sobald die Nutzenden die Möglichkeit haben, die Aggressivität des Online-Portals bzw. der Applikation bezüglich der Privatsphäre zu beurteilen, indem intuitive und saliente Datenschutzinformationen angeboten werden, neigen sie eher dazu von Internetpräsenzen Einkäufe zu tätigen, die eine mittlere bis hohe Privatsphäre anbieten, selbst wenn der Preis höher ist als der auf den anderen Webseiten.

Auch die Ergebnisse aus der Studie von Kelley et al. (2013), die ebenfalls in Abschnitt 2.2.11 erwähnt wurden, können in der vorliegenden Studie verifiziert werden. Kelley et al. (2013) nutzt eine Datenschutz-Fakten-Checkliste, welche unmittelbar vor dem Herunterladen auf der ersten Seite der Applikation im App-Markt präsentiert wird. Allerdings nutzt der Autor für die Studie ausschließlich unbekannte Applikationen. Dies hat zur Folge, dass der immense Einfluss der Bekanntheit bzw. der Popularität einer Applikation, auf den im nächsten Abschnitt (6.9.7) eingegangen wird, unentdeckt geblieben ist. Demzufolge haben die Datenschutzinformationen bzw. die Kontexthinweise einen höheren Einfluss auf die Auswahl als es in dieser Studie aufgezeigt werden kann. Ein ähnlicher Einfluss kann nur bei den Szenarien Spiele, Wetter und Fitness aufgezeigt werden, weil diese Applikationen zu den unbekannteren gehören.

Ein Zusammenhang zwischen der Technikaffinität und dem Score der ausgewählten Applikationen kann nicht festgestellt werden. Somit ist nicht davon auszugehen, dass die teilweise sehr unterschiedliche Technikaffinität seitens der Versuchspersonen keinen Einfluss auf das Auswahlverhalten der Applikationen hat. Auch weitere Zusammenhänge zwischen dem Score der ausgewählten Applikation und dem Geschlecht, dem Alter, dem Bildungsabschluss, der Wertstellung der Privatsphäre und der Stunden der Nutzung des Endgerätes ergeben keine signifikanten Ergebnisse, sodass davon ausgegangen wird, dass weder die soziodemographischen Daten noch die Wertstellung der Privatsphäre oder Stunden der Nutzung des Endgerätes Einfluss auf das Auswahlverhalten der Applikation haben. Aus diesem Grund sind die eben genannten Kontrollvariablen nicht als Störvariablen, zumindest für den Zweck dieser Studie, anzusehen.

6.9.3 Zur Hypothese 3: Diskussion zum Vergleich der Differenzen der Entscheidungszeiten der Applikation in chronologischer Reihenfolge

Hypothese 3:

Die Gruppen, welche eine Datenschutzskala zur Verfügung haben und mehr Informationsgehalt über diese erhalten, zeigen einen stärkeren Abfall der Entscheidungszeit über die Zeit als jene Gruppen ohne Datenschutzskala oder mit weniger Informationsgehalt über diese.

Beim Vergleich der Differenzen der Entscheidungszeiten der Teilnehmenden in den Szenarien in chronologischer Reihenfolge ist lediglich eine Tendenz der Mittelwerte bei den Gruppen A, B und C, also mit Datenschutzskala, zu erkennen, dass die Personen in diesen Gruppen für die Auswahl im ersten Szenario längere Zeit als für die Auswahl im zweiten Szenario benötigen, während in Gruppe D die Teilnehmenden weniger Zeit im ersten Szenario als im zweiten zur Auswahl der Applikation

benötigen. Alle weiteren Mittelwerte scheinen auf den ersten Blick eher zufällig und keine Effekte zu beinhalten. Dies bestätigt auch der Kruskal-Wallis-Test, welcher lediglich einen signifikanten Unterschied zwischen der Differenz der Entscheidungszeiten des ersten und des zweiten Szenarios aufzeigt. Dieser signifikante Unterschied ist allerdings nach der Bonferroni-Korrektur nicht mehr gegeben.

Hypothese 3a:

Die Gruppe (A) der Nutzenden, die eine Datenschutzskala mit einer detaillierten Beschreibung erhalten, zeigt einen stärkeren Abfall der Entscheidungszeit (von Suche bis Installation der Applikation) über die Zeit als die Gruppe (B), die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält, die Gruppe (C), die eine Datenschutzskala ohne detaillierte Beschreibung erhält und die Gruppe (D), die keine Datenschutzskala erhält.

Der paarweise Vergleich anhand des t-Testes kann einen signifikanten Unterschied bei denselben Differenzen zwischen der Gruppe A und B, B und D sowie C und D feststellen. Dies führt zu einer teilweisen Bestätigung der Hypothese 3a, wobei lediglich der Unterschied der Gruppen A und B als signifikant resultiert. Die Signifikanz zwischen den Gruppen A und C sowie A und D bleibt jedoch aus. Weiterhin postuliert die Hypothese einen signifikanten Unterschied der Differenzen der Entscheidungszeiten zwei aufeinanderfolgender Szenarien zwischen den Gruppen, was jedoch nicht der Fall ist, weil lediglich zwischen dem ersten und dem zweiten Szenario ein signifikanter Unterschied gefunden werden kann. Auch der positive Wert bei den Differenzen zwischen dem siebten und achten Szenario entspricht nicht der postulierten Hypothese.

Hypothese 3b:

Die Gruppe (B) der Nutzenden, die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält, zeigt einen stärkeren Abfall der Entscheidungszeit (von Suche bis Installation) über die Zeit als die Gruppe (C), die eine Datenschutzskala ohne detaillierte Beschreibung erhält und die Gruppe (D), die keine Datenschutzskala erhält.

Aus den paarweisen Vergleichen kristallisiert sich heraus, dass lediglich zwischen der Gruppe B und D ein signifikanter Unterschied bezüglich der Differenzen der Entscheidungszeiten zwischen dem ersten und zweiten Szenario zu sehen ist. Allerdings zeigen die Mittelwerte der Differenzen in Gruppe B zwischen dem zweiten und dritten, dem fünften und sechsten sowie dem sechsten und siebten Szenario einen positiven Wert. Dies widerspricht der Aussage eines sukzessiven stärkeren Abfalles in der Entscheidungszeit. Somit kann die Hypothese 3b nicht bestätigt werden.

Dieselben Argumente gegen die Bestätigung der Hypothese 3a sprechen gegen eine Bestätigung der Hypothese 3c:

Die Gruppe (C) der Nutzenden, die eine Datenschutzskala ohne detaillierte Beschreibung erhält, zeigt einen stärkeren Abfall der Entscheidungszeit (von Suche bis Installation) über die Zeit als die Gruppe (D), die keine Datenschutzskala erhält.

Hier ist auch lediglich nach der Durchführung eines t-Tests ein signifikanter Unterschied zwischen dem ersten und dem zweiten Szenario beim Vergleich der Gruppe C mit D wiederzufinden. Darüber hinaus sind bei den Mittelwerten der Differenzen der Entscheidungszeiten der Gruppe C zwischen dem sechsten und siebten Szenario sowie dem siebten und achten Szenario positive Werte zu sehen. Somit kann die Hypothese 3c auch nur für die Differenzen der Entscheidungszeiten zwischen dem ersten und zweiten Szenario im Vergleich zu Gruppe D bestätigt werden, muss jedoch generell abgelehnt werden.

Eine mögliche Erklärung, dass die Gruppen A, B und C eine längere Entscheidungszeit bei der ersten als bei der zweiten Applikation benötigt haben, könnte die Datenschutzskala gewesen sein, die zunächst einmal betrachtet und verstanden werden muss. Der signifikante Unterschied zwischen Gruppe A und B könnte daraus resultieren, dass der Gruppe A eine Einleitung in die Datenschutzskala präsentiert wurde und eine höhere Aufmerksamkeit der Teilnehmenden in dieser Gruppe auf der Datenschutzskala vorlag. Von einer höheren Betrachtungszeit auf die Datenschutzskala ist aufgrund der Fixationszeiten nicht auszugehen. Weiterhin lassen die geringen signifikanten Unterschiede eher auf eine zufällige Signifikanz schließen, vor allem muss bei dieser explorativen Auswertung bedacht werden, dass die Auswahlzeiten verschiedener Szenarien z.B. der Gruppe Messenger und Wetter in eine Variable zusammengeführt werden. Dem ist so, weil aufgrund der verschiedenen Reihenfolgen die Hälfte der Personen in jeder Gruppe die Szenarien Messenger und die andere Hälfte der Personen die Szenarien Wetter als erstes durchlaufen musste. Nun ergibt sich jedoch die Problematik, dass die Teilnehmenden zur Wahl einer Applikation in einem bestimmen Szenario, wie z.B. das des Wetters, generell mehr Zeit benötigten als für die Wahl einer Applikation im Szenario des Messengers. Dies könnte einer der Gründe sein, weshalb bei diesen Tests nur wenige Ergebnisse als signifikant resultieren.

Eine weitere Erläuterung der Abwesenheit von signifikanten Unterschiedenen wäre die einfache Gestaltung der Datenschutzskala, welche dazu führt, dass die Teilnehmenden dazu in der Lage sind, eine informiertere Entscheidung mit Effizienz zu treffen, ohne längere Entscheidungszeiten zu benötigen.

6.9.4 Zur Hypothese 4: Diskussion zum Vergleich der Fixationszeiten

Hypothese 4:

Die Fixationsdauer auf die Datenschutzskala steigt mit der Information über diese.

Beim Vergleich der Fixationszeiten auf die Datenschutzskala kann anhand der sich sehr ähnelnden Mittelwerte zwischen den Gruppen bereits angenommen werden, dass kein signifikanter Unterschied zu finden ist. Diese Annahme hat sich nach der Durchführung des Signifikanztestes bestätigt. Somit kann davon ausgegangen werden, dass die Informationsmenge über die Skala keinen Einfluss auf die Betrachtungszeit der Versuchspersonen auf die Skala ausübt. Aus diesem Grund kann weder die Hypothese 4a noch die Hypothese 4b bestätigt werden.

Hypothese 4a:

Die Fixationsdauer der Datenschutzskala ist höher bei der Gruppe (A) der Nutzenden, die eine Skala mit detaillierter Beschreibung bekommen, als bei der Gruppe (B), die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält, und Gruppe (C), die eine Datenschutzskala ohne detaillierte Beschreibung erhält.

Hypothese 4b:

Die Fixationsdauer der Datenschutzskala ist höher bei der Gruppe (B) der Nutzenden, die nur bei Bedarf eine detaillierte Beschreibung der Datenschutzskala durch eigenständiges Klicken auf die Skala erhält als bei der Gruppe (C), die eine Datenschutzskala ohne detaillierte Beschreibung erhält.

Obwohl die Hypothese nicht bestätigt werden kann, scheint die Betrachtungszeit auf das Symbol der Applikation in einem positiven Zusammenhang mit der Informationsmenge über die Skala zu stehen. Ein inverses Verhalten ist bezüglich der Fixationszeiten des Textes und der Informationsmenge über die Skala zu beobachten. Die Gruppe A, welche eine Datenschutzskala mit vorheriger Erläuterung zur Verfügung gestellt bekam, hat deutlich weniger Zeit bei der Fixation des Textes aufgewandt als die Gruppe B und diese wiederum als die Gruppe C. Aus diesem Verhalten könnte geschlossen werden, dass die Erläuterung der Datenschutzskala dazu geführt hat, länger auf das Symbol zu schauen und weniger den Text zu beachten. Eine mögliche Erklärung dieses Verhaltens wäre, dass die Datenschutzskala mit Erläuterung eine höhere Bedeutung für die Teilnehmenden hat, weil sie bereits die Funktion der Skala kennen und diese somit in ihr Entscheidungsverhalten miteinfließt. Aus diesem Grund wird dem Text in Gruppe A im Vergleich zu den anderen Gruppen weniger Beachtung geschenkt, weil die Teilnehmenden dieser Gruppe zusätzlich ein weiteres Instrument zur Verfügung haben, um die Applikationen, in diesem Fall bezüglich des Datenschutzes, einschätzen zu können. Dies könnte die

Teilnehmenden dazu verleitet haben, weniger Zeit für das Lesen des Textes und mehr Zeit für das Betrachten des Symbols aufgewandt zu haben. Allerdings kann ein signifikanter Unterschied lediglich zwischen der Gruppe A und C bezüglich der Fixationszeiten auf den Text gefunden werden. Die Abwesenheit der Signifikanz zwischen den Gruppen A und B sowie zwischen den Gruppen B und C ist mit den Rahmenbedingungen zu erläutern, die aus Gruppe B eine hybride Gruppe gemacht haben. Haben sich die Teilnehmenden dazu entschlossen auf die Datenschutzskala zu klicken, so wurde ihnen dieselbe Erläuterung präsentiert, welche sich Gruppe A zu Beginn der Studie durchlesen musste. Haben sie dies jedoch unterlassen, so erhielten sie keinerlei weitere Informationen über die Datenschutzskala, welches den Rahmenbedingungen der Gruppe C entspricht.

6.9.5 Diskussion zum Vergleich der Entscheidungszeiten zwischen den Szenarien

Bereits bei näherer Betrachtung der Mittelwerte fällt auf, dass für die Entscheidung bei der Applikationsauswahl teilweise ähnliche Zeiten, teilweise jedoch auch sehr verschiedene Zeiten benötigt werden. Beispielsweise werden für das Szenario der Videokonferenz und der Musik jeweils durchschnittlich knapp über 11 Sekunden benötigt, um eine Entscheidung zu treffen, während die Teilnehmenden bei der Auswahl einer E-Mail-Applikation deutlich mehr Zeit benötigt haben (ca. 28 Sekunden). Ein weiteres Paar, welches eine ähnliche Entscheidungszeit aufweist, ist das Szenario des Wetters und der Nachrichten mit jeweils knapp über 17 Sekunden. Alle weiteren Wertepaare unterscheiden sich um fast mindestens zwei Sekunden. Somit ist davon auszugehen, dass die Entscheidungszeiten zwischen den Szenarien sich überwiegend signifikant unterscheiden, was sowohl im Friedman-Test als auch im Wilcoxon-Test bestätigt wurde. Die Versuchspersonen benötigen für die Szenarien Musik, Videokonferenz und Messenger deutlich weniger Zeit für eine Entscheidung als in den Szenarien der Spiele, Fitness und E-Mail. Wie auch im späteren Verlauf der Diskussion mehrfach erwähnt wird, hat die Popularität der Apps, also ihre Bekanntheit, einen besonders hohen Einfluss auf die Entscheidungszeit sowie auf das Auswahlverhalten allgemein. Vor allem bei der Entscheidungszeit ist zu erkennen, dass bei Szenarien, die über eine sehr verbreitete und bekannte Applikation verfügen, wie beispielsweise Spotify im Szenario der Musik, Skype im Szenario der Videokonferenz und WhatsApp im Szenario des Messengers, die Teilnehmenden dazu neigen, diese populäre Applikation ohne zu zögern auszuwählen. Dies könnte der Grund dafür sein, dass die geringsten Entscheidungszeiten in diesen drei Szenarien wiederzufinden sind. Die längste Entscheidungszeit im Szenario der E-Mail ist damit zu erklären, dass die Teilnehmenden es gewohnt sind, das E-Mail-Programm des Anbieters zu nutzen. In unserem Fall haben wir den Teilnehmenden ein fiktives E-Mail-Konto bei dem Anbieter Google erstellt, jedoch absichtlich nicht das Programm dieses E-Mail-Anbieters zur Verfügung gestellt. Aus diesem Grund ist davon auszugehen, dass die Teilnehmenden weitere

Faktoren in ihrer Entscheidung für die Auswahl der Applikation einfließen lassen haben. Auch die Tatsache, dass beim E-Mail-Schriftverkehr teilweise wichtige und offizielle Dokumente versandt werden, trägt dazu bei, mehr Zeit in eine möglichst adäquate Auswahl zu investieren. Auf die Bekanntheit der Applikationen wird detaillierter im Kapitel 6.9.2 und 6.9.7 Bezug genommen.

6.9.6 Diskussion zu Entscheidungszeiten zwischen den Gruppen

Beim Vergleich der Mittelwerte zwischen den Gruppen A bis D fällt auf, dass sich in Gruppe D die Teilnehmenden für die Szenarien Messenger, Videokonferenz, Wetter und Musik am wenigsten Zeit zur Auswahl der Applikationen genommen haben, während die geringsten Entscheidungszeiten für die Szenarien E-Mail, Fitness, Spiele und Nachrichten in Gruppe B wiederzufinden sind. Hierbei könnte davon ausgegangen werden, dass die Teilnehmenden, die eine Datenschutzskala vorliegen hatten, sich besonders bei Applikationen, die sensible Daten erfassen können, wie zum Beispiel Messenger und Videokonferenz, sich mehr Zeit für die Entscheidung genommen haben als die Teilnehmenden in Gruppe D ohne Datenschutzskala. Dieses Phänomen kann wieder darauf zurückzuführen sein, dass die Teilnehmenden zur Ausführung der Aufgaben in Gruppe D ohne weitere Bedenken ihre favorisierten Applikationen gewählt haben, die sie auch im Alltag auf ihren privaten Geräten verwenden. Die Gruppen mit Datenschutzskala (A bis C) könnten diese in ihren Entscheidungen berücksichtigt haben, um eine informierte Auswahl zu treffen. Zu dem E-Mail-Szenario, welches zu der Applikation mit sensiblen Daten zählt, jedoch trotzdem die längste Entscheidungszeit in Gruppe D aufweist, ist wiederum anzumerken, dass die Teilnehmenden meist die Applikation des Anbieters der E-Mail-Dienstleistung wählen, der jedoch in dieser Studie bewusst nicht angeboten wird. Der Ausschluss dieser Applikation wurde getätigt, um eine homogene Auswahl in dem Szenario zu vermeiden. Die Mittelwerte weisen weder bei der Verwendung des Kruskal-Wallis-Tests noch des Mann-Whitney-U-Tests eine Signifikanz auf. Lediglich beim paarweisen Vergleich können fünf signifikante Unterschiede einzelner Szenarien ermittelt werden, welche jedoch aufgrund der hohen Anzahl der Tests eher zufällig erscheinen.

6.9.7 Diskussion zur Bekanntheit der ausgewählten Applikation

Bei näherem Betrachten der Auswahl der Applikation für das Erfüllen der Messengeraufgabe ist auffällig, dass über alle Gruppen hinweg von den meisten Personen eine Applikation gewählt wird, die sie bereits auf ihrem eigenen Smartphone installiert haben und verwenden. Lediglich in Gruppe B haben sechs Personen sich für eine Applikation entschieden, die sie weder installiert noch verwendet

haben. Diese Häufigkeiten sind dadurch zu erklären, dass besonders WhatsApp im Alltag von den meisten Personen für Messengerdienste benutzt wird. Dies ist auch aus der Tabelle 87 im Anhang Y zu ersehen: insgesamt 52 Teilnehmende (63,4 %) haben sich für WhatsApp entschieden, wobei die zweithäufigste Applikation, der Facebook-Messenger, lediglich neunmal (11 %) gewählt wird. Auch aus den Interviews geht hervor, dass die Bekanntheit der Applikation einen großen Einfluss auf das Auswahlverhalten hat. Viele der Teilnehmenden begründeten ihre Auswahl mit dem bereits vorhandenen Wissen über die Bedienung der Applikation und den somit erleichterten Verhältnissen mit der Einrichtung dieser. Der doch womöglich wichtigste Grund, der genannt wird, sind die bereits vorhandenen Kontakte innerhalb dieser Applikation und die Gewissheit, dass ein Großteil der Endnutzenden diese Applikation auf ihrem Smartphone verwenden. Den Teilnehmenden wird verdeutlicht, dass sie jede Applikation, die zur Auswahl steht, benutzen können und sie sich in die Situation hineinversetzen sollen, dass sie ein neues Smartphone ohne jegliche vorinstallierten Applikationen vor sich finden. Darüber hinaus werden ihnen fiktive Daten zu ihrer Person und zu ihrer Kontaktperson zur Verfügung gestellt. Somit soll sichergestellt werden, dass die Person sich darüber im Klaren ist, unabhängig ihrer bereits auf dem eigenen Smartphone installierten Applikationen eine beliebige Anwendung zur Bewältigung der vorgegebenen Aufgabe auswählen zu können. Auf der anderen Seite werden die Teilnehmenden darum gebeten, sich während des Versuches möglichst alltäglich zu verhalten. Diese Aussage wird bewusst getätigt, da es Ziel dieser Studie ist, den Einfluss einer Datenschutzskala zu erfassen, wenn diese zum jetzigen Zeitpunkt in einen App-Markt implementiert werden würde, sodass die Endnutzenden mobiler Endgeräte bereits zum jetzigen Zeitpunkt ein Sortiment von favorisierten oder oft benutzten Applikationen haben. Hierbei ist es schwierig, den Teilnehmenden zu verdeutlichen, dass sie zwar unabhängig ihrer bereits verwendeten Applikationen handeln, jedoch auf der anderen Seite ein möglichst alltägliches Verhalten aufzeigen sollen. Dieses Problem zeigt sich vor allem bei sehr bekannten Applikationen, wie z.B. WhatsApp und Skype, bei denen es in einer alltäglichen Situation auch darauf ankommt, dass die zu kontaktierende Person dieselbe Applikation auf ihrem Smartphone installiert hat. Somit ist auch ein ähnliches Verhalten bei dem Szenario der Videokonferenz ersichtlich, in dem 59 der Teilnehmenden (72 %) sich für die Applikation Skype entschieden haben. Diese hohe Anzahl, welche die der Applikation WhatsApp noch übertrifft, könnte damit erklärt werden, dass die zur Alternative aufgeführten Applikationen (Viber, TrueConf, Imo) noch unbekannter als die im Szenario des Messengers (z.B. Facebook, Telegramm und Threema) sind. Dementsprechend kann auch bei diesen beiden Szenarien von nur einem geringen oder gar keinem Einfluss der Datenschutzskala auf das Auswahlverhalten ausgegangen werden, was auch in Kapitel 6.9.2 bereits erläutert wurde. In dem Szenario der Musik, welches ebenfalls eine sehr populäre Applikation (Spotify) beinhaltet, ist zu erkennen, dass diese bekannte Applikation noch häufiger gewählt wird (61 Teilnehmer, 74,4 %), obwohl der prozentuelle Anteil vor

allem in den Gruppen A (52,4 %), B (31,6 %) und C (47,8 %) niedriger ist als in den Szenarien des Messengers und der Videokonferenz. Einer der Gründe für dieses Verhalten könnte die Notwendigkeit und der Gebrauch der verschiedenen Applikationen sein. Für viele Leute über alle Altersgruppen hinweg ist es bereits selbstverständlich, mit dem Smartphone auf dem Weg der Textnachrichten zu kommunizieren. WhatsApp sowie die anderen Messenger bieten darüber hinaus an, Sprachnachrichten und Photographien versenden zu können, was die Kommunikation mit dem Gegenüber erleichtern und vereinfachen kann. Das Hören von Musik mit dem Handy bzw. über Streaming-Anbieter wird meist nur von jüngeren Nutzenden genutzt, während Nutzende eines höheren Alters eher auf den CD-Player und das Radio zurückgreifen. Darüber hinaus hören ältere Personen im Durchschnitt seltener Musik als Personen im jüngeren Alter (Statista Research Department, 2020).

Bezüglich des Szenarios des Wetters ist eine sehr viel homogenere Verteilung über alle Gruppen zu sehen. Es zeigt sich eher ein Trend, eine Applikation zu wählen, die weder installiert noch verwendet wurde. Vor allem in den Gruppen A (38,1 %), B (45,4 %) und C (39,1 %) entscheidet sich die Mehrzahl der Teilnehmenden, eine Applikation zu wählen, die bei ihnen noch nie Verwendung fand. Lediglich bei Gruppe D (31,6 %) wählte die Mehrzahl der Teilnehmenden eine Applikation aus, die sie bereits verwendet, jedoch derzeit nicht installiert hatten. Ein ähnliches Verhalten lässt sich in den Szenarien E-Mail, Fitness, Spiele und Nachrichten feststellen. Bei den eben genannten Szenarien lässt sich jedoch über alle Gruppen hinweg, also auch in der Gruppe D, der höchste Mittelwert in der Kategorie „nicht installiert und nicht verwendet“ finden.

Dieses Verhalten könnte darauf zurückzuführen sein, dass es in den eben genannten Szenarien keine Applikationen gibt, welche zur Erfüllung der gestellten Aufgabe so dominierend sind, wie beispielsweise WhatsApp im Bereich der Messengerdienste.

Bezüglich des Szenarios der Fitness finden Applikationen in diesem Bereich seltener Verwendung als Applikationen, die der primären Funktion des Smartphones, der Kommunikation, dienen. Somit ist davon auszugehen, dass ein höherer Anteil der Teilnehmenden über keine Fitness-Applikation auf ihrem persönlichen mobilen Endgerät verfügt (Alexander Kunst, 2019). Dies würde die hohe Anzahl an gewählten Applikationen erklären, die von den Teilnehmenden weder installiert noch verwendet wurden.

In der Kategorie der Spiele haben in fast jeder Gruppe über 90 % der Teilnehmenden eine Applikation gewählt, die sie weder installiert noch verwendet haben. Dabei ist es naheliegend, dass nur sehr wenige der Teilnehmenden die zur Verfügung stehenden Applikationen kannten, weil es sich hierbei um zehn verschiedene Versionen einer Sudokuanwendung handelt und somit die Wahrscheinlichkeit,

dass die Applikation von allen Teilnehmenden bereits verwendet wurde, sehr gering ist. Nur wenige der Teilnehmenden haben eine Sudokuapplikation auf ihrem mobilen Endgerät installiert. Darüber hinaus ist es unwahrscheinlich, dass sie weitere Sudokuapplikationen kennen, weil es nur selten Gründe dafür gibt, mehrere dieser Applikationen zu verwenden, weil die Funktion meist die gleiche ist und kein Mehrwert daraus gezogen werden kann.

Aus diesem Grund ist es für die meisten Teilnehmenden nicht möglich gewesen, eine bereits verwendete oder installierte Applikation auszuwählen.

Bei der näheren Betrachtung der Häufigkeiten der gewählten Applikationen im Szenario der Nachrichten fällt auf, dass über alle Gruppen hinweg circa 26 % bis 31 % die Applikation bereits verwendet, jedoch nicht installiert haben. Dieser im Vergleich zu den anderen Szenarien hohe Anteil an Teilnehmenden, welche die Applikation zwar kennen, jedoch nicht auf ihrem eigenen Smartphone nutzen, ist damit zu erklären, dass viele Teilnehmende die Nachrichten im Browser lesen und die Applikation nicht installieren. So wird es auch im Interview kommuniziert. Ein ähnliches Verhalten ist auch im Szenario des Wetters wiederzusehen.

Allgemein ist zu beobachten, dass die Bedenken um die Privatsphäre umgekehrt proportional zur Bekanntheit der Applikationen sind, was an den Kategorien Messenger und Videokonferenz aufgrund der häufigen Auswahl von WhatsApp und Skype zu erkennen ist. Im Gegensatz dazu werden bei den Kategorien Wetter, Fitness und Nachrichten vermehrt als sicher gekennzeichnete Applikationen ausgewählt. In den Kategorien Videokonferenz, Wetter, E-Mail, Fitness und Nachrichten sind die Teilnehmenden, die eine Datenschutzskala zur Verfügung hatten, signifikant adäquater beim Evaluieren der Vertrauenswürdigkeit der Applikationen.

Diese Ergebnisse können, wie schon vorher erwähnt, durch die Bekanntheit der Applikationen erklärt werden. Am Beispiel von Skype führt eine bekannte Applikation in Kombination mit einer sicheren Kennzeichnung auf der Datenschutzskala zu einer höheren Bewertung der Vertrauenswürdigkeit als eine bekannte Applikation ohne Datenschutzskala. Eine bekannte Applikation in Kombination mit einer unsicheren Kennzeichnung auf der Datenschutzskala führt zu einer geringeren Bewertung der Vertrauenswürdigkeit. Trotz der unsicheren Kennzeichnung auf der Datenschutzskala wird die Applikation aufgrund ihrer Bekanntheit ausgewählt. Durch die Kennzeichnung der Applikation als „unsicher“ wird diese jedoch mit einer geringeren Vertrauenswürdigkeit bewertet. Wenn die Applikation nicht bekannt ist und die Datenschutzskala sie als sicher kennzeichnet, wird die Vertrauenswürdigkeit der Applikation als hoch bewertet. Eine unbekannte Applikation mit einer unsicheren Kennzeichnung auf der Datenschutzskala wird in der Regel nicht ausgewählt und hat somit keinen Einfluss auf die Bewertung. Eine bekannte Applikation ohne Datenschutzskala ist stark von ihrer

Reputation abhängig, was aus den Interviews ersichtlich ist. Ein ähnliches Muster ist bei der Einfachheit der Auswahl zu erkennen. Dies hat bei den Kategorien Wetter und Fitness zu einer signifikant einfacheren Applikationsauswahl für die Gruppen A, B und C, mit Datenschutzskala, geführt.

Anhand der Ergebnisse ist ein signifikanter Einfluss der Datenschutzskala auf das Auswahlverfahren in den Kategorien Wetter, E-Mail, Musik, Fitness, Spiele und Nachrichten zu erkennen. Dies führt zu einer Auswahl weniger invasiver Applikationen. Die fehlende Signifikanz in den Kategorien Messenger und Videokonferenz lässt sich wiederum durch die Bekanntheit der Applikationen (Skype und WhatsApp) erklären. Die Interviews zeigen, dass die meisten Teilnehmenden eine Applikation gewählt haben, die sie bereits kennen. Die Datenschutzskala wird von den Teilnehmenden mehrheitlich positiv bewertet.

Dass die Popularität die Bedenken gegenüber einer Applikation verringert, konnte bereits in der Studie von Gu et al. (2017) belegt werden, die in Abschnitt 2.2.13 erwähnt wurde.

6.9.8 Diskussion zur Bewertung der Datenschutzskala

Die Tendenz, dass die Gruppe A die positiven Aussagen höher bewertet, könnte damit zusammenhängen, dass die Gruppe eine detaillierte Erklärung der Datenschutzskala bekommen hat und somit einerseits die Datenschutzskala mehr beachtet hat, andererseits über Hintergrundwissen der Funktionsweise der Datenschutzskala verfügt. Dies wird auch den signifikanten Unterschied zwischen Gruppe A und C sowie Gruppe B und C über die Aussage der Informationsarmut erklären. Die Gruppe C mit der höchsten Bewertung bei der Informationsarmut bekam keine Erläuterung über die Datenschutzskala und hatte auch nicht die Möglichkeit, eine Beschreibung der Datenschutzskala aufzurufen. Trotzdem wird auch hier die Datenschutzskala durchweg positiv bewertet. Der signifikante Unterschied zwischen den Gruppen A und C bezüglich der Auswirkung auf die Applikationsauswahl könnte durch die fehlende Beschreibung der Skala bei Gruppe C bedingt sein. Während Gruppe A durch die vorgesetzte Erläuterung der Datenschutzskala in Papierform über die Funktion und die Interpretation der Skala aufgeklärt wurde, hatte Gruppe C keine Möglichkeit nähere Information über die Skala zu erlangen. Aus der Videokonfrontation ist zu entnehmen, dass aus diesem Grund bei einigen Teilnehmenden Skepsis gegenüber der Skala, deren Herkunft und deren Entwickler aufkam. Ein weiterer Effekt, der nicht zu vernachlässigen ist, könnte die geringere Augenscheinvalidität sein, welche bei Gruppe A eventuell aufgetreten sein könnte. Auf Grund der vorgesetzten Erläuterung der Datenschutzskala ist es möglich, dass die Teilnehmenden bereits vermuten konnten, dass die Datenschutzskala ein wesentlicher Bestandteil des Experiments sein könnte. Andererseits hätten die

Gruppen B und C eine ähnliche Vermutung aufstellen können, weil die Datenschutzskala auffällig am rechten Seitenrand des App-Marktes platziert ist.

6.9.9 Diskussion zum Measuring Mobile Users Concerns for Information Privacy (MUIPC)

Die meisten Teilnehmenden sind darüber besorgt gewesen, dass Applikationen ihr mobiles Endgerät überwachen und ihre Aktivitäten an diesem Gerät aufnehmen. Darüber hinaus haben sie das Gefühl, dass durch ihr mobiles Endgerät mehr Informationen über ihre Privatsphäre an Dritte weitergegeben werden als sie es wünschen. Zusammenfassend ist den Personen bewusst, dass ihre Daten durch Applikationen in Umlauf gebracht werden, was größtenteils auf Missfallen stößt. Der größte Teil der Teilnehmenden erlebte in den letzten zwei Jahren mindestens ein bis zweimal Vorfälle, in denen ihre persönlichen Daten von Unternehmen oder Webseiten ohne ihre Genehmigung verwendet wurden. Darüber hinaus haben über 95 % der Teilnehmenden bereits von Vorfällen gehört oder gelesen, in denen es zu Missbrauch des Sammelns der Daten kam. Die Hälfte der Stichprobe gibt an, selbst Opfer dessen gewesen zu sein, was sie als unangemessenen Eingriff auf ihre Privatsphäre empfinden.

Dieses Verhalten erinnert stark an der Theorie des Privacy Paradoxes, welche besagt, dass die Nutzenden trotz des Bedürfnisses ihre persönlichen Daten zu schützen, diese aushändigen, um einen relativ geringen Gegenwert, zum Beispiel eine Applikation, zu erhalten. Dieses Phänomen wurde bereits in der Theorie in Kapitel 2.2.8 erläutert. Dies bestätigt auch die Angabe der Teilnehmenden, dass dreiviertel von ihnen höchstwahrscheinlich persönliche Informationen aushändigen würden, um eine Applikation nutzen zu können. Ein ähnliches Verhalten konnte auch im Bereich der Connected Cars beobachtet werden. In einer vom Autor betreuten Bachelorarbeit wird ebenfalls eine gewisse Besorgnis bezüglich der Abgabe personenbezogener Daten laut. Allerdings fließen diese Bedenken kaum in die Kaufentscheidung mit ein, weil der Preis des Automobils und dessen Marke für die Konsumenten eine deutlich wichtigere Rolle einnehmen.

Beim Prüfen des Zusammenhanges zwischen den schlechten Erfahrungen von dem Eingriff in die Privatsphäre und der Bedenken bezüglich jenes Eingriffs ergeben sich bezüglich der Frage nach der Häufigkeit der Datennutzung ohne Einwilligung fünf signifikante Korrelationen. Vier Korrelationen davon weisen eine schwache Effektstärke auf, während eine Korrelation eine mittlere Effektstärke ausweist.

Beim Prüfen des Zusammenhanges zwischen den Bedenken und der Frage, wie oft man sich in den letzten zwei Jahren als Opfer eines unangemessenen Eingriffs in die Privatsphäre empfand, können vier signifikante Korrelationen mit einer schwachen Effektstärke und fünf signifikante Korrelationen

mit einer mittleren Effektstärke festgestellt werden. Aufgrund dieser erheblichen Anzahl an ausschließlich positiven Korrelationen, die größtenteils eine Signifikanz aufweisen, ist davon auszugehen, dass mit steigender Häufigkeit der schlechten Erfahrungen bezüglich des Eingriffes in die Privatsphäre auch die Zustimmung in die von dem MUIPC vorgegebenen Bedenken steigt. Diese Ergebnisse stimmen auch mit den Ergebnissen der Studie von Gu et al. (2017) überein, die in Abschnitt 2.2.13 erwähnt wurde, in der nachgewiesen wird, dass die Bedenken über die Privatsphäre stark abhängig von schlechten Erfahrungen sind, welche die Nutzenden zuvor gemacht haben.

Darüber hinaus ergeben die Zusammenhänge zwischen den beiden Fragen (E2: *Häufigkeit der Datennutzung ohne Einwilligung* und E4: *Häufigkeit des Empfindens Opfer eines Eingriffes in die Privatsphäre zu sein*) und der sechsten Aussage des MUIPCs (*Wenn ich persönliche Informationen zur Verwendung von Applikationen herausgebe, habe ich Bedenken, dass die Applikationen meine Informationen für andere Zwecke benutzen*.) jeweils ein signifikantes Ergebnis. Somit steigen die Bedenken, dass persönliche Informationen für andere, nicht vom Nutzenden gewollte Zwecke benutzt werden, mit der steigenden Häufigkeit schlechter Erfahrungen bezüglich des Eingriffes in die Privatsphäre.

Hierbei könnten Parallelen zu den Ergebnissen der Studie von Solove (2006) gezogen werden, welche einen Zusammenhang zwischen dem sekundären Gebrauch von persönlichen Daten und der Angst und Unsicherheit darüber, wie diese Daten verwendet werden, feststellen kann.

6.9.10 Diskussion zum Zusammenhang zwischen der Auswahl der Applikation (Score) und den Bedenken über den Datenschutz (MUIPC)

Beim Betrachten der Zusammenhänge zwischen der Auswahl der Applikation und den Bedenken über den Datenschutz fällt auf, dass in den meisten Szenarien kaum ein Zusammenhang besteht. Allerdings sind im Szenario der E-Mail gleich sechs positive Zusammenhänge, zwei mit einem kleinen Effekt und vier mit einem mittleren Effekt, zu erkennen. Eine positive Korrelation bedeutet, dass mit Steigerung des Scores der ausgewählten Applikation eine höhere Übereinstimmung mit den Aussagen des MUIPCs einhergeht. So wählen Nutzende, die der Meinung sind, dass andere durch die Verwendung von Applikationen mehr über sie wissen als ihnen angenehm ist, eine Applikation für die Bewältigung der Aufgabe im Szenario der E-Mail, die als sicherer eingestuft wird als Personen, welche mit der Aussage weniger übereinstimmen. Ähnliche Beobachtungen können bei der Aussage gemacht werden, dass unter der *Verwendung von Applikationen Informationen über die Nutzenden verfügbar sind und wenn diese genutzt werden, in dessen Privatsphäre eindringen*. Auch Nutzende, welche besorgt sind, dass ihre persönlichen Daten für einen anderen Zweck verwendet werden dürfen, ohne sie vorher zu

benachrichtigen oder eine Berechtigung einzuholen, wählen zumindest im Szenario der E-Mail eine deutlich datenschutzfreundlichere Applikation aus. Dieses Verhalten ist auch bei Nutzenden festzustellen, die Bedenken haben, dass die Applikation ihre Information für andere Zwecke benutzt und diese mit anderen Instanzen teilt, ohne vorher ihre Berechtigung einzuholen. Beim Betrachten der anderen Szenarios fällt auf, dass bei vielen keine Zusammenhänge festzustellen sind oder nur ein bis zwei Zusammenhänge gefunden werden, die jedoch zufällig erscheinen. Die hohe Anzahl an Zusammenhängen im Szenario der E-Mail könnte damit zu erklären sein, dass die E-Mail heutzutage als offizielles Kommunikationsinstrument gesehen wird, mit dem wichtige und sensible digitale Briefe und Dokumente versendet werden. Aus diesem Grund könnte davon ausgegangen werden, dass die Nutzenden besonders im Bereich der E-Mail-Applikation auf die Sicherheit dieser achten und die Sicherheit durch die Besorgnisse bezüglich des Datenschutzes im Alltag gesteigert wird.

In der Studie von Malhotra et al. (2004), die in Abschnitt 2.2.11 beschrieben wurde, konnte ein positiver Zusammenhang zwischen der Besorgnis im Bereich des Datenschutzes und der Menge an Information, die von anderen verlangt wird, festgestellt werden. Diese Ergebnisse konnte nur bezüglich des E-Mail-Szenarios bestätigt werden, bei allen anderen Szenarien konnte kein Zusammenhang zwischen dem Bedenken und der Auswahl der Applikation festgestellt werden.

6.9.11 Diskussion zur Relevanz der Methoden zur Applikationsbewertung

Beim Betrachten der Mittelwerte fällt auf, dass die unterschiedlichen Applikationsbewertungen sich in der Relevanz für die Applikationsauswahl unterscheiden. Dieser Unterschied resultiert nach Anwendung des Friedman-Tests als signifikant. Der Wilcoxon-Test bestätigt diese Ergebnisse, wobei lediglich zwischen den Wertpaaren der Rezension und der Sternebewertung sowie der Datenschutzskala und den Rezensionen kein signifikanter Unterschied entdeckt werden kann.

Beim Betrachten der Mittelwerte der verschiedenen Methoden zur Applikationsbewertung fällt auf, dass die Datenschutzskala insgesamt als am relevantesten valutiert wird. Dies spiegelt wiederum den Bedarf einer in dem App-Markt implementierten Datenschutzskala wider. Die zweitwichtigste Bewertungsmethode bei der Auswahl einer Applikation belegt die Rezension. Dies könnte daran liegen, dass die Nutzenden somit Information über die Handhabung, die Funktion und gegebenenfalls die Probleme der Applikation in Erfahrung bringen können, ohne die Applikation vorher herunterladen oder installieren zu müssen. Etwas verwunderlich ist, dass die Sternebewertung den dritten Rang bezüglich der Relevanz bei der Applikationsauswahl erlangt. Hier wird davon ausgegangen, dass die Nutzenden eine kurze symbolisierte Information über die Güte der Applikation vorziehen, statt längere

Einzelbewertungen durchzulesen. Dies könnte damit zusammenhängen, dass die Nutzenden sowohl die Sternebewertung als auch die Rezension gleichzeitig betrachten, wobei die Rezension als Grund für die entsprechende Benotung mit Hilfe der Sternebewertung angesehen wird. So betrachten die Endnutzenden zunächst die besten und schlechtesten Sternebewertungen und erfassen die größten Vor- und Nachteile der Applikation, indem sie die entsprechenden Rezensionen lesen. Als am wenigsten relevant wird die Anzahl an Downloads und an Aufrufen bewertet. Eine mögliche Erklärung für die untergeordnete Relevanz dieser Bewertungsmethoden ist die mangelnde Relation bzw. die Schwierigkeit diese Werte miteinander zu vergleichen. Darüber hinaus muss bei der Betrachtung dieser Zahlen berücksichtigt werden, ob die Applikation lediglich nationale oder auch internationale Bekanntheit genießt. Durch die Abwesenheit einer Kategorisierung dieser Zahlen fällt es den Nutzenden schwer zu erfassen, ob die Anzahl an Downloads bzw. Aufrufen als häufig oder selten anzusehen ist. Mit Hilfe des Friedman-Test kann belegt werden, dass die Mittelwerte der verschiedenen Bewertungsmethoden sich signifikant unterscheiden. Werden die Mittelwerte der Applikationsbewertungsmethoden nach Gruppen getrennt betrachtet, so fällt auf, dass von Gruppe B bis D die Bewertungsmethoden in der Rangfolge nahezu identisch mit den aufsummierten Ergebnissen aller Gruppen sind. Lediglich die Mittelwerte der Gruppe A differieren von den restlichen Gruppen, wobei die Relevanz der Rezension den höchsten Stellenwert belegt. Bei genauerer Betrachtung der Mittelwerte fällt jedoch auf, dass die Gruppe A die Relevanz der Datenschutzskala im Vergleich mit den Gruppen B und C höher eingeschätzt hat, die Datenschutzskala jedoch nur den zweiten Rang erlangt, weil den Rezensionen der höchste Relevanzwert über alle Methoden und Gruppen zugesprochen wird. Werden jedoch die signifikanten Unterschiede der Mittelwerte der Bewertungsmethoden betrachtet, so fällt auf, dass sich lediglich die Rezensionen von den anderen Datensätzen unterscheiden. Nach Durchführung des Mann-Whitney-U-Tests stellte sich heraus, dass lediglich die Rezensionen beim Vergleich der Gruppen A und B sowie A und C sich signifikant von den anderen Datensätzen unterscheiden. Somit kann davon ausgegangen werden, dass sich die Relevanz der Bewertungsmethoden zwischen den Gruppen mit Ausnahme der Rezensionen kaum unterscheidet. Zusammengefasst bewerten die Teilnehmenden der Studie die Datenschutzskala als am relevantesten, wobei die Signifikanztests bestätigen, dass hierbei ein signifikanter Unterschied zu den anderen Bewertungsmethoden vorhanden ist. Wie erwartet ergibt sich beim Vergleich zwischen den Gruppen kein signifikanter Unterschied. Somit kann davon ausgegangen werden, dass die Datenschutzskala über alle Gruppen hinweg als sehr relevant für die Applikationsauswahl angesehen wird.

6.9.12 Diskussion der Videokonfrontation anhand des Interviews

Der Grund für die Videokonfrontation ist es zu erfassen, weshalb sich die Teilnehmenden für eine bestimme Applikation entschieden haben und was sie dazu bewegt hat, diese Entscheidung zu fällen.

Als relevantestes Entscheidungsmotiv konnte die Bekanntheit der Applikation identifiziert werden. Vor allem in den Kategorien Messenger, Videokonferenz und Musik ist sie das Motiv, welches am meisten genannt wird. In den Szenarien der Fitness und der Spiele können die Auswahlfaktoren bei weniger geläufigen Anwendungen untersucht werden. Bezüglich dieser beiden Szenarien können die erwartete Funktionalität und die Symbolgestaltung als hauptsächliche Entscheidungsmotive identifiziert werden. Die Datenschutzskala wird über alle Szenarien hinweg mit unterschiedlicher Häufigkeit und Gewichtung berücksichtigt. Bezüglich der Szenarien Musik und Messenger trifft dies jedoch lediglich auf weniger als 10 % zu. Weiterhin wird nach der Bekanntheit der Applikation als zweithäufigstes Entscheidungsmotiv die Verbreitung im persönlichen Umfeld genannt, was auf die Befürchtung der Ausgrenzung aus den sozialen Gruppen zurückzuführen ist (Doolaard et al., 2020). Darüber hinaus ist die vertraute Handhabung ein weiterer Grund, eine bereits bekannte Applikation zu wählen.

Im Rahmen der bereits im Abschnitt 6.8.5 erwähnten Bachelorarbeit von Herrn Wichmann wird dazu die folgende Hypothese aufgestellt:

Je stärker die Datenschutzskala in die Auswahlentscheidung einbezogen wird, desto sicherer sind die gewählten Apps.

Nach der Auswertung der Ergebnisse kann mit Ausnahme des Szenarios der Nachrichtenapplikation bei allen weiteren Szenarien ein signifikanter Unterschied zwischen der Gruppe 1, bei der die Datenschutzskala das relevanteste Entscheidungsmotiv ist und der Gruppe 2, bei der die Skala das zweit- oder drittwichtigste Entscheidungsmotiv ist, festgestellt werden. Ferner können signifikante Unterschiede zwischen der Gruppe 1 und der Gruppe 3, bei der die Skala keine Relevanz für das Auswahlverhalten hat, bei allen Szenarien festgestellt werden. Zwischen der Gruppe 2 und der Gruppe 3 können lediglich signifikante Unterschiede bei dem Szenario des Wetters, der Spiele und den Nachrichten gefunden werden. So kann gezeigt werden, dass die Datenschutzskala die Teilnehmenden dazu bewegte, ein datenschutzfreundliches Verhalten an den Tag zu legen. Während zwischen der Gruppe 1 und der Gruppe 2 sowie der Gruppe 1 und der Gruppe 3 bei nahezu alle Szenarien signifikante Unterschiede aufgezeigt werden können, sind zwischen der Gruppe 2 und der Gruppe 3 lediglich drei signifikante Unterschiede wiederzufinden. Diese Ergebnisse lassen darauf schließen, dass die Datenschutzskala als primäres Entscheidungsmotiv einen signifikanten Einfluss auf das Auswahlverhalten hat, wobei dieser Einfluss in der Gruppe, welche die Skala als zweit- oder

drittwichtigstes Motiv angesehen hat, nur in den Szenarien des Wetters, der Spiele und der Nachrichten zu beobachten ist.

Somit kann die Hypothese nur teilweise aufrechterhalten werden.

Ferner konnten aus den Fragebögen und den Interviews durchaus unterschiedliche Meinungen bezüglich des „One-to-one“-Marketings, welches in Abschnitt 2.2.1 erläutert wurde, gefunden werden. Für das „One-to-one“-Marketing“ werden persönliche Informationen wie Nutzerdaten, Positionen, Kaufverhalten und weitere gesammelt und analysiert. Hierbei stellt sich die Frage, ob die Nutzenden, welche dieser personalisierten Werbung kritisch gegenüberstehen, sich eher verärgert stimmen, sobald ihnen diese Art von Werbung präsentiert wird. Aus den Transkriptionen der Interviews (welche auf dem Datenträger zu finden sind) ist zu entnehmen, dass sich einige Teilnehmende einerseits für das Anzeigen personalisierter Werbung aussprechen und dies damit begründen, dass sie es bei Notwendigkeit einer Werbung bevorzugen würden, Artikel und Dienstleistungen angezeigt zu bekommen, die ihrem Interesse entsprechen. Andererseits empfand die Mehrheit der Teilnehmenden jedoch die personalisierte Werbung als unerwünschten Eingriff in ihre Privatsphäre und empfindet diesen als manipulativ und unangebracht.

6.10 Probleme und Ausblick

Die erste Hürde bei diesem Versuch war schon wie im vorherigen Experiment die Einholung der Erlaubnis seitens der Ethikkommission aufgrund des Aufbaus des Experimentes, dessen Einleitung den Teilnehmenden den wahren Grund der Studie verschwieg und lediglich erläuterte, dass es sich bei dem Experiment um die Untersuchung der Benutzerfreundlichkeit eines App-Marktes handle. Aus diesem Grund bedurfte der Ethikantrag mehrere Änderungen, wobei im Endeffekt drei Monate vergingen, bis die Ethikkommission die Durchführung stattgegeben hat.

Ein weiteres Problem stellte die Sammlung der Daten bezüglich der Aggressivität der Applikationen dar, weil die mobilen Endgeräte bereits mit dem Betriebssystem Android 8 Oreo versehen waren, die Applikationen, die für die Sammlung der Zugriffsanfragen programmiert wurden, aber nur unter Android 7.12 Nougat stabil lief. Für das Aufspielen der älteren Versionen auf dem Endgerät musste wie bereits in Abschnitt 6.5.1 erklärt, dass Gerät zunächst gerootet und die Android Version mit Hilfe des OST-Tools aufgespielt werden. Dabei kam es zu Komplikationen bedingt durch eine unerwartete Trennung des Endgeräts zum Computer, welche zur Folge hatte, dass das Aufspielen des Images unterbrochen wurde und das Gerät nicht mehr nutzbar war. Das Gerät konnte nur durch fremde Hilfe wiederhergestellt werden. Nach dem Abschließen der Studie mussten die Daten wie bereits in

Abschnitt 6.5.1 erläutert, ausgewertet werden. Die Auswertung wurde an der Universität von Karlstad in Schweden vollzogen. Hierbei kam es allerdings zu Verzögerungen, was dazu führte, dass die Arbeit an dieser Dissertation aufgrund der fehlenden Ergebnisse nicht fortgeführt werden konnte, weil die Ergebnisse zur Erstellung der Datenschutzskala notwendig waren. Aufgrund der Ungewissheit, wann diese Ergebnisse zur Verfügung stehen würden, wurde sich in Absprache mit dem Doktorvater dazu entschieden, die Einordnung der Applikationen in die Datenschutzskala randomisiert vorzunehmen. Diese Entscheidung wurde getroffen, weil der Versuch lediglich untersuchen sollte, ob die Datenschutzskala Auswirkungen auf das Auswahlverhalten hat. Dabei wurde jedoch nicht bedacht, dass einige Applikationen bereits einen gewissen Ruf haben, die Daten der Nutzenden zu schützen oder diese zu sammeln und weiterzugeben. Dies führte im anschließenden Experiment zu Irritierungen seitens weniger Versuchspersonen, weil diese bereits einige Applikationen und deren Umgang mit den Daten kannten, die Datenschutzskala die Applikation jedoch nicht entsprechend kategorisierte. So wurde beispielsweise die Applikation „Telegramm“ als „sehr kritisch“ eingeordnet, obwohl die Applikation für den sicheren Umgang mit den Daten und den Nachrichten der Endnutzenden bekannt ist, weil der Hersteller mit einer Ende-zu-Ende-Verschlüsselung der Textnachrichten wirbt. Dies könnte sich möglicherweise auf die Entscheidungen der Teilnehmenden ausgewirkt haben. Es besteht die Gefahr, dass die Applikation trotz der schlechten Klassifizierung ausgewählt wurde. Diese Unstimmigkeit wurde jedoch nur von zwei der 82 Teilnehmenden angemerkt. Ferner zeigen die Ergebnisse, dass trotz dieser Diskrepanz bei einigen Applikationen zwischen Datenschutzskala und bisherigem Ruf die Datenschutzskala einen signifikanten Einfluss auf das Auswahlverhalten der Endnutzenden hat.

Dieser Einschränkung soll zukünftig entgegengewirkt werden, indem wie von Beginn an geplant die Daten aus der Applikationsverhaltensanalyse ausgewertet werden und somit eine Datenschutzskala entworfen werden kann, welche die Zugriffe der Applikationen auf die Daten berücksichtigt und eine realistischere Illustration bietet.

Darüber hinaus wurde beim Vortragen der Arbeit auf der HCII Copenhagen 2020 angemerkt, dass die Skala auch missinterpretiert werden könnte und die Endnutzenden davon ausgehen könnten, dass die Funktion der Applikation sicher oder kritisch sein könnte. Am Beispiel des Messengers würde es bedeuten, dass der Messenger zwar zuverlässig und sicher Nachrichten versendet und empfängt, jedoch eine große Menge an Daten wie z.B. die Position oder andere Daten auf dem Gerät ausliest und weitergibt. Während des Interviews mit der Videokonfrontation wurden die Teilnehmenden allerdings gefragt, wie sie die Datenschutzskala interpretieren. Hierbei resultierte, dass fast alle Teilnehmenden die Funktion der Skala richtig interpretiert und verstanden haben, dass die Skala anzeigt, auf wieviel Zugriffsberechtigungen wie häufig zugegriffen wird. Darüber hinaus ist vorgesehen, dass bei

Implementierung der Skala in den App-Markt eine kurze Einleitung, wie in Gruppe A, zur Verfügung gestellt wird und somit eine Missinterpretation der Skala vermieden werden kann.

Diese Arbeit hat explorativen Charakter, und es sei darauf hingewiesen, dass auch die Interpretation von den Ergebnissen der statistischen Tests Grenzen hat. Ein Mangel an festgestellter statistischer Signifikanz bedeutet nicht, dass keine Wirkung vorliegt.

Ein weiteres Problem stellte die Teilnehmenden dar, die eine Sehhilfe, insbesondere eine Brille, zur Bedienung des mobilen Endgerätes benötigten. Aufgrund der Verwendung einer Eye-Tracking-Brille musste den Teilnehmenden, die eine Brille als Sehhilfe benötigten, somit zwei Brillen aufgesetzt werden. Dies führte dazu, dass die Augenbewegung unter diesen Bedingungen nur teilweise oder gar nicht aufgezeichnet werden konnte. Dem wurde versucht entgegenzuwirken, indem die Testperson während des Interviews gebeten wurde, genauer zu beschreiben auf welche Merkmale sie sich konzentrierten. Aufgrund der mangelhaften Aufzeichnung der Augenbewegung konnte die Analyse des Eye-Tracking-Videos in zehn Fällen nicht durchgeführt werden.

Allgemein stellte die Eye-Tracking-Auswertung eine große Hürde dar. Wie schon in Abschnitt 6.7.3.2 erläutert, konnten die Blickdaten des Eye-Tracking-Videos nicht gespeichert werden, weil der Speichervorgang eine geraume Zeit in Anspruch genommen hätte und der Versuchsablauf vorsah, das Eye-Tracking-Video in der Videokonfrontation den Teilnehmenden vorzuführen. Somit wäre die Speicherung der Blickdaten mit einer hohen Wartezeit während des Versuches verbunden, die es unbedingt zu vermeiden galt. Darüber hinaus war ebenfalls unklar, ob eine automatisierte Auswertung der Blickdaten erfolgreich durchgeführt werden konnte, selbst wenn die Blickdaten vorhanden wären. Aufgrund des Wechsels der Bedienoberflächen vom Startbildschirm über die Auswahl und die Installation zur Bedienung der Applikation wäre es ebenfalls schwierig geworden, Bereiche zu definieren, in denen die Blicke und deren Dauer gemessen worden wären.

Darüber hinaus könnte auch die eingeschränkte Auswahl der Applikation zu einem nicht alltagskonformen Verhalten geführt haben bzw. das eigentliche Nutzerverhalten verzerrt haben. So bezweifelte ein Teilnehmer, dass er in der Realität die meisten von den Applikationen nicht heruntergeladen hätte (Datenträger, VP32, Abs. 25). Ferner haben einige Teilnehmende explizit auf das Fehlen ihnen bekannter Applikation hingewiesen.

Zukünftig sollten auch Studien mit unbekannten Apps durchgeführt werden, um eine Verzerrung bedingt durch die Bekanntheit oder die Bewertungen der Applikationen zu vermeiden und den Einfluss der Datenschutzskala unabhängig von den eben genannten Störvariablen zu erfassen.

Hierbei ist jedoch zu vermerken, dass auch diese Ergebnisse nicht der Realität entsprechen, weil die Datenschutzskala bei der Implementierung in den App-Markt bereits bekannte Applikationen kategorisieren wird.

Eine weitere Einschränkung ist die Anwendung der Think Aloud Technik nach dem Ausführen einer Tätigkeit. Die ursprüngliche Methode dieser Technik sieht vor, dass die Personen während des Ausführens einer Aufgabe die Gedanken laut mitteilen. Damit die Teilnehmenden ein alltägliches Verhalten aufzeigen und die verbale Wiedergabe der Gedanken davon abweicht, wurde sich dazu entschieden, die Teilnehmenden mit Hilfe der Videokonfrontation im Anschluss des eigentlichen Versuches zu befragen. Hierbei besteht die Gefahr einer Gedächtnisverzerrung, welche jedoch durch Zeigen des Videos so gering wie möglich gehalten werden sollte.

In dieser Studie nahmen keine minderjährigen Personen teil (unter 18). Folglich blieb eine große Nutzerbasis für die Kategorie Spiele, Soziale Netzwerke, Nachrichtendienste und Lifestyle unberücksichtigt. Darüber hinaus waren 56 % der Studienteilnehmenden in einem Alter von 20 bis 29 Jahre, während 21 % der Altersgruppe von 30 bis 39 angehörten. Der Alterspanne von 40 bis 49 gehörten lediglich 11 % der Teilnehmenden an, wobei nach Angaben der Bundeszentrale für politische Bildung (2020) der Anteil der eben genannten Altersgruppen etwa gleich verteilt sein sollte. Auf Grund der Tatsache, dass diese Verteilung im Rahmen der Studie nicht gegeben war, kann davon ausgegangen werden, dass in Hinblick auf das Alter die Ergebnisse als nur bedingt repräsentativ für die deutsche Gesamtbevölkerung angesehen werden dürfen. Trotz des Versuches, eine möglichst heterogene Stichprobe zu akquirieren, liegt das durchschnittliche Alter bedingt durch das universitäre Umfeld deutlich unter dem deutschen Gesamtdurchschnitt.

6.11 Fazit

Das Ziel dieser Studie ist, den Endnutzenden von mobilen Endgeräten eine datenschutzfreundlichere Applikationsauswahl bei der Erfüllung von alltäglichen Aufgaben zu ermöglichen und die Auswirkung für die Implementierung einer Datenschutzskala in den App-Markt auf das Applikationsauswahlverhalten seitens der Teilnehmenden zu untersuchen. Die Skala soll die Häufigkeit der Zugriffe auf die persönlichen Daten seitens der Applikation illustrieren. Dabei wurde die Skala schon während der Auflistung der zur Verfügung stehenden Applikationen direkt neben diesen platziert. Das empirische Experiment umfasst den Entwurf und die Bewertung von fünf unterschiedlichen Datenschutzskalen. Anschließend werden Aufbau und Durchführung des Experimentes detailliert beschrieben und die Aufbereitung der Rohdaten näher erläutert. Schließlich

werden die Ergebnisse der Nutzerstudie, die sich auf das Auswahlverhalten von den 82 Teilnehmenden näher betrachtet, vorgestellt und diskutiert.

Die wichtigsten Erkenntnisse aus den gesammelten Daten und der statistischen Analyse dieser Studie sind folgende:

a. Eine unilaterale Datenschutzskala kann zu einer besseren Beurteilung der Vertrauenswürdigkeit der Applikationen führen und die Auswahl dieser erleichtern;
b. die Gruppen mit einer Datenschutzskala können im Vergleich zur Kontrollgruppe eine adäquatere Entscheidung bzgl. der Wahrung der Privatsphäre treffen;
c. aus den Ergebnissen der Fragebögen geht hervor, dass die Datenschutzskala ein geeignetes Instrument ist, um sowohl die Transparenz zu steigern als auch die Privatsphäre der Nutzenden zu schützen;
d. Die Ergebnisse der MUIPC-Analyse deuten darauf hin, dass die Teilnehmenden Bedenken haben, dass ihr Gerät überwacht und ihre Aktivitäten auf diesem Gerät aufgenommen werden. Ferner haben sie das Gefühl, dass mehr Informationen über ihre Privatsphäre an Dritte weitergegeben werden als sie wünschen. Den Teilnehmenden ist also bewusst, dass ihre Daten durch die Applikation in Umlauf gebracht werden, was bei ihnen größtenteils auf Missfallen stoß. Darüber hinaus wählten die Teilnehmenden mit größeren Bedenken bezüglich des Eingriffes in ihre Privatsphäre häufiger als „sehr sicher“ gekennzeichnete Applikationen aus.
e. Aus den Blickbewegungsdaten (Eye-Tracker-Daten) geht hervor, dass die Datenschutzskala weder einen Einfluss auf die Entscheidungszeiten noch auf die Fixationszeiten hat.
f. Dieses Verhalten könnte durch den intuitiven Aufbau der Skala, welche nur einen kleinen kognitiven Aufwand voraussetzt, erklärt werden. Die Teilnehmenden sind in der Lage, eine informierte Entscheidung mit Effizienz zu treffen, ohne eine längere Entscheidungszeit zu benötigen.
g. Die Teilnehmenden benötigen in den Szenarien Musik, Videokonferenz und Messenger signifikant weniger Zeit für ihre Entscheidung als in den Szenarien Spiele, Fitness und E-Mail. Dabei wird die Bekanntheit als besonders großer Einflussfaktor genannt. Je bekannter die Applikation ist, desto weniger zögerten die Teilnehmenden, diese auszuwählen.
h. Die Datenschutzskala wird von den Teilnehmenden als relevanteste Methode zur Bewertung der Applikation gewählt.
i. In den Interviews wird bezüglich der Szenarien Messenger, Videokonferenz und Musik die Bekanntheit der Applikationen als relevantestes Entscheidungsmotiv angegeben. Bei den Szenarien der Fitness und der Spiele, die weniger populäre Applikationen enthalten, wird Funktionalität und Symbolgestaltung als hauptsächliches Entscheidungskriterium gewählt.

Ferner kann ein signifikanter Einfluss der Datenschutzskala als primäres Entscheidungsmotiv auf das Auswahlverhalten festgestellt werden.

Generell wird die Datenschutzskala von den Teilnehmenden als positiv und hilfreich empfunden. Darüber hinaus führt die Skala zu einer Sensibilisierung der Nutzenden hinsichtlich des Datenschutzes, was zu einem datenschutzfreundlicheren Auswahlverhalten führt. Allerdings kann dieses Phänomen bei bekannten Applikationen nur teilweise beobachtet werden, weil die Nutzenden dazu neigen, die Bekanntheit der Applikationen zu priorisieren und sich somit im Zweifelsfall für eine kritische jedoch bekannte Applikation entscheiden. Auch wenn die Datenschutzskala eine kurze Einführung für die richtige Interpretation erfordert, hat sie das Potenzial, Applikationen daran zu hindern, immer größere Mengen an Daten zu sammeln und diese an Dritte weiterzugeben. Aggressive Applikationen müssten mit einer kritischen Kennzeichnung rechnen, welche die Nutzenden dazu verleitet, eine weniger in die Privatsphäre eingreifende Alternative auszuwählen.

7 Empirischer Versuch 3 – Akzeptanz und Verwendung einer temporären Zugriffsberechtigung

Das folgende Kapitel umfasst die dritte empirische Untersuchung, welche das Ziel hat, die Benutzerfreundlichkeit und Akzeptanz einer temporären Zugriffsberechtigung zu erforschen. Gegenwärtig ist es nur möglich, die von den Applikationen angeforderten Rechte bzw. Zugriffberechtigungen auf unbestimmte Zeit zu gewähren. Die Nutzenden haben also nur die Wahl, ob sie die gewünschten Rechte gewähren oder die Anwendung nicht benutzen. Um eine Alternative oder einen Mittelweg zu schaffen, soll eine dritte Option in Form einer temporären Zugriffsberechtigung implementiert werden.

Die folgenden Unterkapitel beinhalten die Forschungsfragen, Forschungshypothesen, die Untersuchungsvariablen sowie die Operationalisierung dieser. Abschließend erfolgt eine Beschreibung des durchgeführten Versuchs, der Methodik sowie die Vorstellung der Ergebnisse.

7.1 Forschungsfragen

In dieser Studie soll evaluiert werden, ob die Implementierung einer temporären Zugriffsberechtigung von den Nutzenden verwendet und akzeptiert wird.

Momentan steht den Nutzenden bei der Freigabe von Rechten zur Nutzung einer Applikation nur eine binäre Auswahl zur Verfügung (Akzeptieren und Ablehnen). Dabei sind die Nutzenden teilweise so konditioniert, dass sie jedes ihrer Rechte abtreten, selbst wenn sie ein Gefühl von Unbehagen überkommt (Council, 2018; Fritsch, 2017). Ferner bedarf der Widerruf des Einverständnisses der Freigabe der Rechte einigen Aufwand, technisches Verständnis sowie das Bewusstsein über die Konsequenzen, welche die Zugriffsberechtigungen mit sich bringen (Momen, 2018a). Die komplexe juristische Sprache, in der die AGBs geschrieben sind, sowie die liberalen Datenschutzvoreinstellungen erschweren es den Nutzenden die Weitergabe ihrer persönlichen Daten zu unterbinden (Fuchs, 2010). Weiterhin wird die Weitergabe der persönlichen Daten durch das Bedürfnis der Nutzung einer Applikation verstärkt, weil diese ansonsten nicht verwendet werden könnte. Es fehlt jedoch jeglicher Anreiz diese Zugriffsberechtigung nach der Abtretung erneut zu überprüfen oder zu widerrufen (Momen et al., 2019). Aus diesem Grund soll eine weitere Option bei der Anfrage der Rechte hinzugefügt werden, sodass den Nutzenden nicht nur eine binäre Auswahl zur Verfügung steht, bei der sie entweder ihre Rechte auf unbestimmte Zeit unbeschränkt freigeben, oder die Applikation nicht nutzen können. Diese zusätzliche Option soll es den Nutzenden ermöglichen, die Rechte nur temporär abzugeben. Hierbei ist es fraglich, ob diese Zugriffsberechtigung akzeptiert wird und wie benutzerfreundlich diese zusätzliche Option gestaltet werden kann, um im Alltag Verwendung zu finden. Darüber hinaus soll ermittelt werden, ob ein allgemeines Bedürfnis an einer temporären Zugriffsberechtigung besteht. Weiterhin stellt sich die Frage, ob eine wiederkehrende Anfrage der Zugriffsberechtigung die Nutzenden stört oder verärgert. So wäre es weiterhin relevant zu erfassen, ob den Nutzenden die Kontrolle über ihre Daten mit wiederholender Anfrage zur Zugriffsberechtigung oder die Bequemlichkeit mit permanenter Zugriffsberechtigung wichtiger ist. Ferner soll ermittelt werden, bei welchen Datentypen und Lebenskontexten die temporäre Zugriffsberechtigung am besten angewendet werden kann. So kann die Implementierung einer temporären Zugriffsberechtigung für die Standortdaten hilfreich erscheinen, weil die Übermittlung der Echtzeitinformation unterbrochen wird und die Nutzenden somit ihre Privatsphäre schützen können. Es ist allerdings fraglich, ob die temporäre Zugriffsberechtigung bei dem Zugriff auf die Kontakte einen Mehrwert erzielen kann, weil bei einmaliger Erteilung der Rechte bereits sämtliche Kontakte ausgelesen und weitergegeben werden können, sodass ein wiederholter Zugriff lediglich Einsicht in denselben oder nur gering erweiterten Datensatz bietet. Somit ergeben sich folgende Forschungsfragen:

a) Ist die temporäre Zugriffsberechtigung anwendbar?

b) Wird die temporäre Zugriffsberechtigung akzeptiert?

Ist die temporäre Zugriffsberechtigung erwünscht?

Hierbei soll herausgefunden werden, ob die Funktion der temporäre Zugriffsberechtigung von den Endbenutzenden erwünscht ist und somit in ihrem täglichen Leben Verwendung finden würde. Dies soll erfasst werden, indem ein Fragebogen zu alltäglicher Nutzung und Benutzerfreundlichkeit nach dem Experiment von den Teilnehmern ausgefüllt wird.

c) Werden zu eng getaktete Anfragen der Zugriffsberechtigungen als störend empfunden?

d) Wie hoch ist die Verärgerung über die wiederkehrende Anfrage für die Berechtigung eines Zugriffes durch die temporäre Zugriffsberechtigung?

e) Ist es für die Nutzenden wichtiger, die Kontrolle über ihre Daten zu haben, oder hat die Bequemlichkeit Vorrang?
Hierbei soll untersucht werden, ob die Teilnehmenden es bevorzugen, ihre Daten zeitlich unbegrenzt freizugeben, um die wiederkehrende Anfrage auf die Zugriffsberechtigung zu vermeiden.

Weiterhin soll explorativ erfasst werden, für welche Lebenskontexte und Datentypen die temporäre Zugriffsberechtigung einsetzbar ist, um persönliche Daten zu schützen.

7.2 Hypothesen

Die vorliegende Studie untersucht den Einsatz einer temporären Zugriffsberechtigung, welche in die Oberfläche einer Nachrichtenapplikation implementiert wurde. Dabei soll diese Berechtigung nur für eine bestimmte Zeit und eine bestimmte Anzahl von Zugriffen gelten (Daniel Franzen & David Aspinall, 2016; Fritsch, 2017; Momen & Fritsch, 2020). Dies soll den Endnutzenden zu einer informierteren und datenschutzfreundlicheren Entscheidung verhelfen.

In einem wissenschaftlichen Artikel von Custers (2016) verdeutlicht dieser, dass die Endnutzenden meist keinen wirklichen Entscheidungsfreiraum bezüglich der Einverständniserklärungen haben, weil diese meist akzeptiert werden müssen, wenn sie das Produkt benutzen möchten. Darüber hinaus verdeutlicht er erneut die Problematik, welche schon häufiger im Rahmen des Privacy Paradox erwähnt wurde. Dabei stellt er heraus, dass den Nutzenden ihre persönlichen Daten zwar wichtig sind, jedoch aus Bequemlichkeiten, Vergünstigungen und anderen Anregungen oder durch das mangelnde Verständnis in die Einverständniserklärungen einwilligen. Ferner kritisiert Custers das Fehlen der

erneuten Abfrage des Einverständnisses in die Erklärungen, weil vor allem im digitalen Bereich die Programme, Applikationen und Internetpräsenzen ihre Funktionen ständig ändern und erweitern, sodass die Einverständniserklärungen zwar angepasst werden, es jedoch keiner neuen Zustimmung bedarf.

Im Rahmen dieser Studie soll somit eruiert werden, ob diese temporären Zugriffsfreigaben, welche eine erneute Abfrage des Einverständnisses mit sich bringen, von den Nutzenden erwünscht und akzeptiert werden (Custers, 2016). Auf Grund der Ergebnisse des ersten Versuches, in denen bestätigt wird, dass die Endnutzenden den persönlichen Daten einen hohen Wert zuschreiben (siehe Abschnitt 5.7.7 und 5.8.2) und aufgrund der positiven Bewertung der Datenschutzskala durch die Teilnehmenden im zweiten Versuch (siehe Abschnitt 6.8.6.2 und 6.9.8) ist davon auszugehen, dass die meisten Nutzenden mobiler Endgeräte eine weitere Funktion zum Schutz ihrer persönlichen Daten ebenfalls positiv bewerten. Im Rahmen des ersten Versuches wurde das Privacy Paradox bestätigt, welches besagt, dass Nutzende stets eine Applikation nutzen würden, welche anwenderfreundlichere Datenschutzbestimmungen haben, solange keine Kompromisse in der Funktionalität gemacht werden müssen. Es ist fraglich, ob eine wiederkehrende Zugriffsberechtigung für die Nutzenden eine Beeinträchtigung der Funktionalität mit sich bringt. Ist dem so, muss damit gerechnet werden, dass die Nutzenden die temporäre Zugriffsberechtigungen nicht nutzen, um ihre persönlichen Daten zu schützen. Allerdings zeigen die Ergebnisse der zweiten Studie zum Einfluss einer Datenschutzskala auf das Auswahlverhalten, dass die Datenschutzskala durchaus genutzt wird und zu einem datenschutzfreundlichen Verhalten beigetragen hat. Aus diesem Grund wird davon ausgegangen, dass die Teilnehmenden der Studie auch diese Funktion nutzen werden, um die Zugangsberechtigung zeitlich zu begrenzen und somit ihre Daten zu schützen. Aus den eben genannten Ergebnissen der vorherigen Studien lassen sich somit folgende Hypothesen aufstellen:

- Hypothese 1. Die temporäre Zugriffsberechtigung wird von den Nutzenden angewendet.

- Hypothese 2. Die temporäre Zugriffsberechtigung wird hinsichtlich ihrer Funktionsweise von den Nutzenden positiv bewertet.

- Hypothese 3. Die Funktion der temporären Zugriffsberechtigung wird von den Nutzenden im Alltag erwünscht.

- Hypothese 4. Die Nutzenden empfinden durch die wiederkehrende Anfrage einer Berechtigung Ärgernis.

- Hypothese 5. Die Nutzenden bevorzugen die Kontrolle über ihre Daten trotz der wiederkehrenden Anfrage für die Berechtigung.

7.3 Versuchsdesign

Für den dritten empirischen Versuch wird eine Nachrichtenapplikation entwickelt, bei der die Funktion einer temporären Zugriffsberechtigung implementiert ist. Den Teilnehmenden werden anschließend Aufgaben gestellt, die Sie innerhalb der Applikation lösen müssen.

Aufgrund der zum Zeitpunkt der Durchführung herrschenden Umstände bedingt durch die „Covid-19"-Pandemie und aufgrund der Dauer von insgesamt zehn Tagen erfolgt der dritte empirische Versuch nicht im Labor, sondern ausschließlich online. Hierfür werden die Teilnehmenden gebeten, die Einverständniserklärung und einen selbstgenerierten persönlichen Code per E-Mail an den Versuchsleiter zu schicken.

Aufgrund der Tatsache, dass E-Mails abgerufen werden müssen und die Aufgaben so bald wie möglich bzw. zumindest am gleichen Tag erledigt werden sollen, wird sich dazu entschieden die Aufgaben ebenfalls per SMS zu versenden. Somit erhalten die Teilnehmenden der Studie die Aufgabe als Push-Nachricht direkt auf ihr Smartphone, auf diesem sie die Aufgaben innerhalb der Applikation lösen sollen.

Die Teilnehmenden an der Studie werden zunächst gebeten, die prototypisierte Nachrichtenapplikation herunterzuladen und auf ihrem mobilen Endgerät zu installieren. Anschließend werden sie aufgefordert dem Versuchsleiter ihre „Device ID" mitzuteilen. Diese Aufforderung wird ebenfalls über SMS und E-Mail versandt. Die Entscheidungen die Instruktionen per SMS und E-Mail zu versenden wurde gewählt, weil einige Teilnehmende die SMS nicht erhalten haben. Nach dem Erhalt der „Device ID" werden den Teilnehmenden täglich mehrere Aufgaben gestellt, welche mit der Akzeptanz von Zugriffsberechtigungen einhergeht. Darunter fällt beispielsweise das Teilen von Nachrichten, sowie die Freigabe der Positionsdaten. Die genaue Aufgabenstellung kann unter Anhang CC eingesehen werden. Bei der Anfrage für die Freigabe der Daten erscheint ein Dialogfenster, in dem die Teilnehmenden zwischen „Allow", „Maybe" und „Deny" auswählen können. Weil das Experiment auch in Schweden durchgeführt werden soll, wurde die Oberfläche auf Englisch entworfen, die temporäre Option wurde hierbei als „Maybe"-Button (Abbildung 22 a) implementiert.

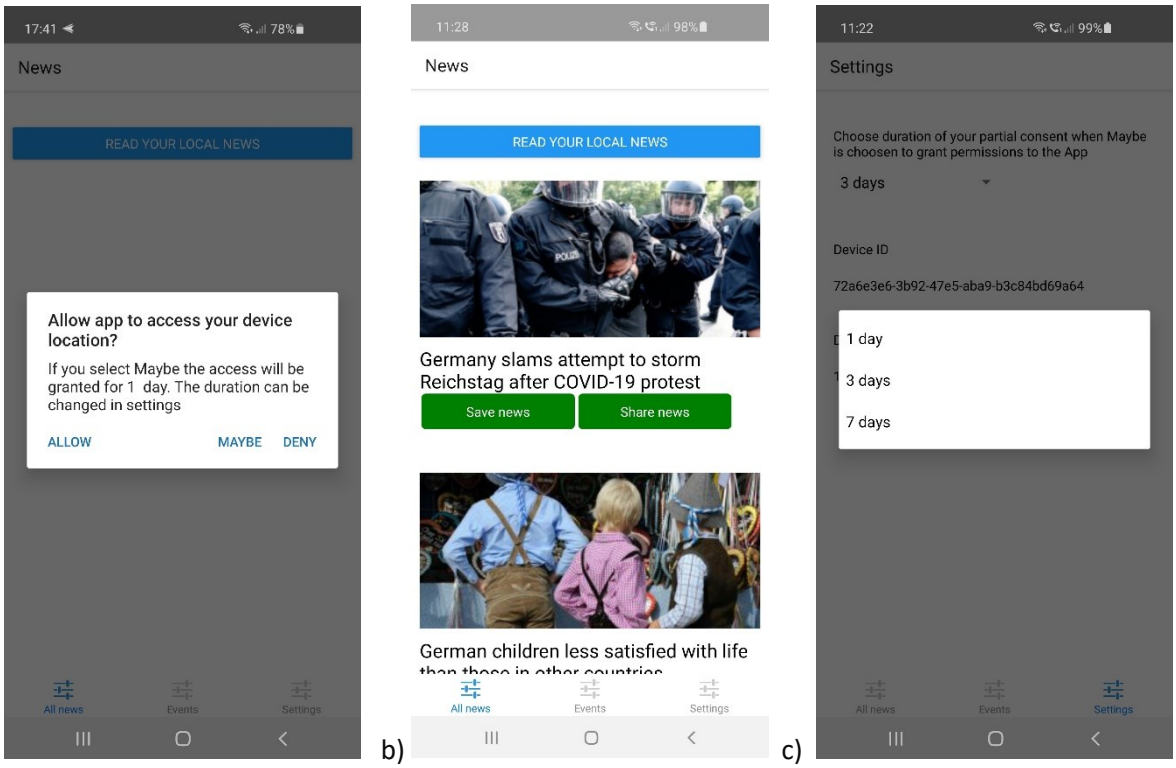


Abbildung 22. a) Bildschirmabzug des Dialogfensters zur Abfrage der Zugriffsberechtigung mit Implementierung der temporären Option, b) der Oberfläche der Nachrichtenapplikation und c) den Einstellungen zur Bestimmung der Zeitspanne für die die Zugriffsberechtigung erteilt wird.

Diese Abbildung zeigt die Nachrichtenapplikation, welche für die Studie zur Bewertung und Akzeptanz der temporären Zugriffsberechtigung entwickelt wurde. Dabei ist links (a) das Dialogfenster zu sehen, welches die Zugriffsberechtigung auf die Positionsdaten des Endgerätes anfordert, um die lokalen Nachrichten abzurufen. Mittig (b) ist die Oberfläche der Nachrichtenapplikation mit den Möglichkeiten, die Nachricht zu speichern oder diese zu teilen, abgebildet. Rechts (c) sind die Einstellungsmöglichkeiten zu sehen, welche den Nutzenden ermöglichen, Zugriffsberechtigung für einen, drei oder sieben Tage zu erteilen.

Bei der ersten Option „Allow“ sind die Teilnehmenden damit einverstanden, dass auf ihre Daten dauerhaft und ohne jegliche Begrenzung zugegriffen wird. Wird die Option „Temporär“ gewählt, so wird die Freigabe der Daten nur für eine bestimmten Zeitraum stattgegeben (s. Abbildung 22 c). Die Option „Ablehnen“ unterbindet die Freigabe der Daten. Beim Öffnen der Optionen der Anwendung wird ein Auswahlmenü angezeigt, das es den Nutzenden ermöglicht, die gewünschten Rechte für einen, drei oder sieben Tage zu erteilen, so dass die Anwendung nur für diese zeitliche Spanne auf die Daten zugreifen kann (s. Abbildung 22 c). Dies erlaubt den Nutzenden, eine fundiertere Entscheidung darüber zu treffen, welche Zugriffsberechtigungen wie lange für eine Anwendung gewährt werden sollen. Über einen Zeitraum von zehn Tagen werden die Aufgaben an die Teilnehmenden geschickt.

Insgesamt werden täglich ein bis zwei Aufgaben gestellt. Dazu gehört z.B. der Empfang von lokalen Nachrichten, das Teilen der Nachrichten und das Speichern des Nachrichtenbeitrags auf dem Gerät.

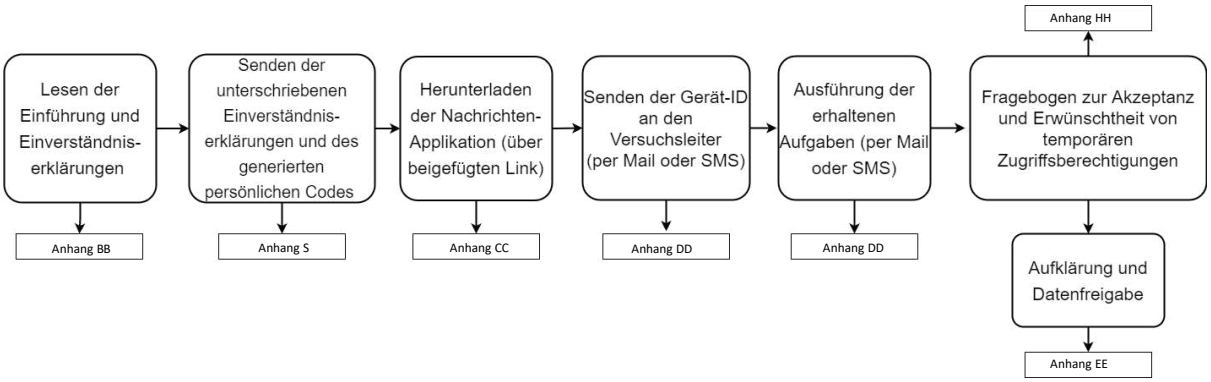


Abbildung 23. Flussdiagramm des dritten empirischen Versuchs bezüglich der Datenschutzskala.

Mit Hilfe dieser Studie soll das Bedienverhalten (Entscheidungsverhalten) der Teilnehmenden aufgenommen und analysiert werden. Für die spätere Auswertung werden lediglich der Name der Berechtigung (Speicher, Mikrophon etc.), die gewählte Option („Allow“, „Maybe“, „Deny“) und der Zeitstempel, welcher festhält, wann die Entscheidung getroffen wird, abgespeichert. Nach dem Experiment werden die Teilnehmenden gebeten, einen Online-Fragebogen zur Benutzerfreundlichkeit und zur hypothetischen Alltagsnutzung dieser Funktion zu beantworten.

7.3.1 Untersuchungsvariablen

Der dritte empirische Versuch enthält keine unabhängige Variable (UV), dazu wurde sich entschieden, weil lediglich getestet werden soll, ob die Funktion der temporären Zugriffsberechtigung benutzt und akzeptiert wird. Weil weiterhin die Optionen des üblichen Zustimmens und Ablehnens vorhanden sind, kann in derselben Stichprobe beobachtet werden, welche Optionen die Teilnehmenden vorziehen, ohne die mögliche Auswahl zu verändern.

Die abhängige Variable (AV) besteht aus der Nutzung der temporären Zugriffsberechtigung. Es wird darauf geachtet, ob die Teilnehmenden zur Erfüllung der täglichen Aufgaben diese temporäre Funktion nutzen oder sich für die bisherigen Möglichkeiten des Akzeptierens oder Ablehnens entscheiden.

7.3.2 Versuchsvorbereitung

Für die Prüfung der Hypothesen wird sich auch in diesem Fall dafür entschieden, den Teilnehmenden nicht den eigentlichen Grund der Studie mitzuteilen, bevor sie den Versuch nicht abgeschlossen haben. Den Teilnehmenden wird lediglich mitgeteilt, dass es sich um die Evaluation einer Nachrichtenapplikation handelt. Dass die Funktion der temporären Zugriffsberechtigung im Fokus des Experimentes stehen, wird den Teilnehmenden nicht explizit kommuniziert. Für die Durchführung der Studie wird in Zusammenarbeit mit der Universität Karlstad eine Applikation entwickelt, welche bereits im Abschnitt 7.3 beschrieben wurde.

Dabei soll das Experiment, vor allem die erste Hypothese, prüfen und untersuchen, ob die Funktion der temporären Zugriffsberechtigung im alltäglichen Gebrauch Anwendung finden würde. Alle weiteren Hypothesen werden mit Hilfe von anschließenden Fragebögen überprüft.

7.3.3 Implementierung der temporären Zugriffsberechtigung in eine Nachrichtenapplikation

In diesem Abschnitt soll beschrieben werden, wie in einen Prototyp einer Nachrichtenapplikation die temporäre Zugriffsberechtigung implementiert wird. Dabei soll vor allem die Entwicklung des Prototyps näher beschrieben werden. Die generische Architektur des „Access Control“-Modells von Android basiert auf den Berechtigungen, die Zugriff auf die Ressourcen und den Speicher des Gerätes ermöglichen. Seit der Einführung von Android 9.0 kann der Endnutzende eine detailliertere Kontrolle über seine Zustimmung mit den Zugriffsberechtigungen ausüben (Google Developers, 2020). Dabei ist es den Nutzenden jedoch nicht möglich einzusehen, wie häufig die Applikation auf ihre Daten zugreift. Ferner erfolgt auch kein Anreiz, das Einverständnis im Nachhinein noch einmal zu überprüfen. Neben der konventionellen Auswahl zwischen dem Akzeptieren und Ablehnen soll eine dritte Option implementiert werden, die eine temporäre Zugriffsberechtigung („Maybe“) zur Verfügung stellt. Dabei wird zunächst von der Applikation die Berechtigung angefragt. Anschließend wird geprüft, ob es sich bei dieser Berechtigung um eine gefährliche Berechtigung (siehe Abschnitt 6.5.1) handelt. Ist dem nicht so, wird der Zugriff direkt gestattet. Andernfalls wird geprüft, ob bereits eine Zugriffsberechtigung vergeben wurde. Ist dies der Fall, wird der Zugriff ebenfalls gestattet. Ansonsten erfolgt die Darstellung des bereits bekannten Dialogfensters mit den Optionen des Akzeptierens und des Ablehnens und der zusätzlichen Option der temporären Zugriffsberechtigung. Beim Akzeptieren der Berechtigung wird der Zugriff erteilt. Wird dieser abgelehnt, so wird der Zugriff unterbunden. Die Funktionsweise wird in Abbildung 24 noch einmal illustriert. Bei der Wahl der temporären Zugriffsberechtigung wird diese für einen bestimmten Zeitraum erteilt, der in den Optionen (1,3 oder 7 Tage) festgelegt werden kann. Zusätzlich wird die Device-ID des Endgerätes den Teilnehmenden unter den Optionen angezeigt.

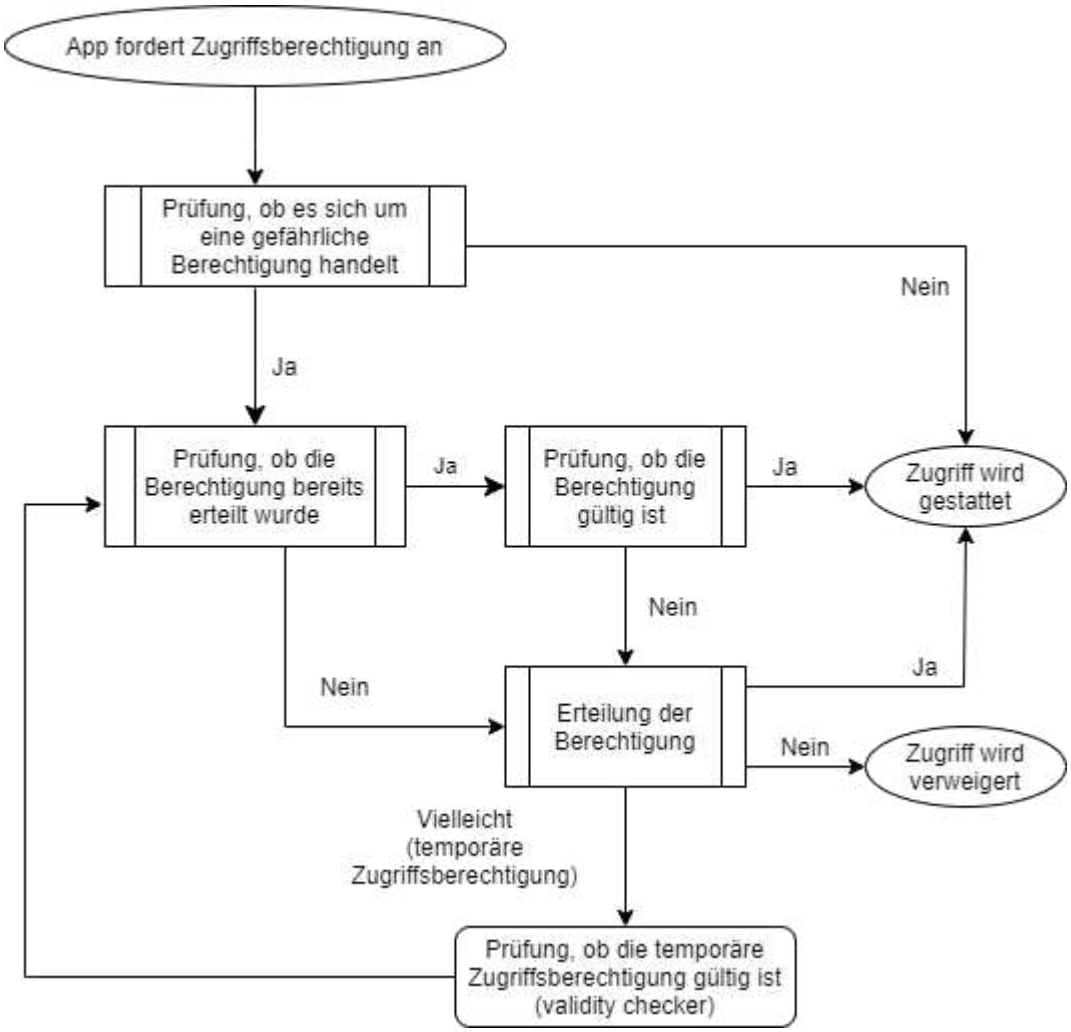


Abbildung 24. Flussdiagramm des Zugriffkontrollmodells mit Implementierung der temporären Zugriffsberechtigung, dargestellt nach Momen et al. (2020).

Diese Abbildung illustriert den bisherigen Prozess des derzeitigen Zugriffkontrollmodells mit zusätzlicher Implementierung der temporären Zugriffsberechtigung.

Beim Wählen der temporären Zugriffsberechtigung wird die Funktion des „validity-checkers“ aufgerufen. Dieser bestimmt, wie lange das Einverständnis in eine Berechtigung gültig ist, abhängig von der festgelegten Gültigkeit durch den Benutzer. Ferner gibt es auch die Möglichkeit, die Zugriffsberechtigungen nicht nur zeitlich, sondern auch basierend auf der Anzahl der Zugriffe zu beschränken. Um die temporäre Zugriffsberechtigung in eine Applikation zu implementieren, wurde wiederum die Applikation A-Ware genutzt, welche bereits in Abschnitt 6.5.1 näher beschrieben wurde. Die Applikation berechnet das Ablaufen der temporären Zugriffsberechtigung, indem sie aus dem

„system_timestamp“ die vergangene Zeit entnimmt und zum gewünschten Zeitpunkt die Zugriffsberechtigung wieder entzieht. Die Abbildung 25 veranschaulicht die Funktionsweise.

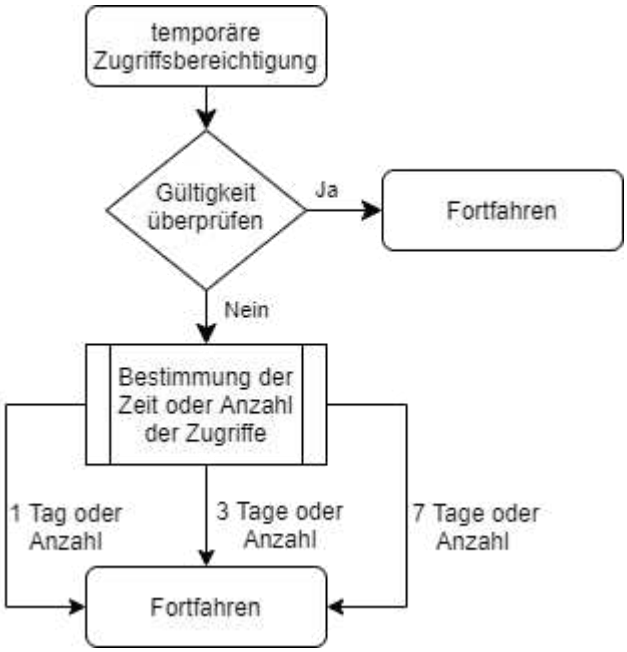


Abbildung 25. Flussdiagramm der Funktionsweise der temporären Zugriffsberechtigung, dargestellt nach Momen et al. (2020).

Diese Abbildung illustriert die Funktionsweise der temporären Zugriffsberechtigung. Dabei wird zunächst geprüft, ob eine bisherige Berechtigung bereits besteht. Ist dies nicht der Fall, obliegt es den Nutzenden zu entscheiden, wie lange sie diese Berechtigung (1, 3 oder 7 Tage) erteilen möchten.

7.3.4 Auswahl der Teilnehmenden

Im dritten Versuch wurden die Teilnehmenden für das Experiment erneut über das Online-Probandenportal „Prometei“ der Technischen Universität Berlin akquiriert. Insgesamt nahmen 32 Personen an dem Versuch teil. Im Rahmen der Probandenaquirierung wurde erneut eine möglichst heterogene Stichprobe für den Versuch angestrebt, sodass sich die demographischen Eigenschafften ausgleichen und in Summe keinen Effekt auf die Ergebnisse haben.

Den Teilnehmenden wurde im Online-Portal eine finanzielle Gegenleistung in Höhe von 10 Euro oder einer Versuchspersonenstunde für die Teilnahme angeboten. Sie konnten sich in dem Zeitraum vom 17.08.2020 bis zum 08.09.2020 für den Versuch anmelden.

7.4 Aufbau

In diesem Kapitel werden Aufbau und Ablauf des dritten Versuches im Detail erläutert. Dabei werden zunächst die Einleitung und Einverständniserklärung, welche die Teilnehmenden vor dem Versuch erhalten haben, beschrieben. Anschließend wird erläutert, wie die eindeutige Zuordnung der Fragebogendaten mit den Daten der Applikation anonym erfolgt ist. Ferner werden die den Teilnehmenden gestellten Aufgaben erläutert und beschrieben, wie diese übermittelt werden. Darüber hinaus wird kurz der Aufbau und der Inhalt des Fragebogens zur Akzeptanz und Erwünschtheit der temporären Zugriffsberechtigungen und die Aufklärung genauer erläutert.

7.4.1 Einleitung und Einverständniserklärung

Die Einverständniserklärung begann mit einer kurzen Einleitung. Ähnlich wie bei den anderen beiden Versuchen wurde den Teilnehmenden auch hier nicht das eigentliche Ziel der Studie mitgeteilt. Ihnen wurde lediglich vermittelt, dass es sich bei der Studie um die Nutzbarkeit und Handhabung einer Nachrichtenapplikation handelt. Als nächstes wurde den Teilnehmenden erläutert, dass sie die Applikation über einen Link, der ihnen per E-Mail und SMS zugesandt wurde, auf ihr Endgerät herunterladen und installieren können. Ferner wurde darauf hingewiesen, dass das Experiment über zehn Tage lang andauert und mit zehn Euro oder einer Versuchspersonenstunde vergütet wird.

Weiterhin wurde den Teilnehmenden mitgeteilt, dass sie die Studie jederzeit, ohne weitere Konsequenzen abbrechen können und dass die erhobenen Daten zur Auswertung der Studie verwendet werden. Zugleich wurde die zehnjährige Aufbewahrung der Daten und die anonymisierte Veröffentlichung der Ergebnisse im Rahmen der Doktorarbeit erwähnt. Darüber hinaus wurden die Teilnehmenden darauf hingewiesen, dass sie zwei Wochen Zeit haben, um die Löschung ihrer Daten anzufordern. Bei Fragen oder Anmerkungen wurden die Versuchspersonen darüber in Kenntnis gesetzt, dass sie jederzeit den Versuchsleiter telefonisch oder per E-Mail erreichen können.

Ähnlich wie im zweiten Versuch (s. Abschnitt 6.6.1) haben die Teilnehmenden zur Anonymisierung einen persönlichen Code nach der standardisierten Anleitung (s. Anhang S) der Ethikkommission generiert. Die Einverständniserklärung wurde den Teilnehmenden in deutscher und englischer Sprache per E-Mail übermittelt, mit der Bitte diese unterschrieben zurückzuschicken. In einer zweiten E-Mail wurde den Teilnehmenden die Anleitung zur Generierung ihres persönlichen Codes geschickt, den sie ebenfalls an den Versuchsleiter zurückschicken sollten.

7.4.2 Device-ID

Zum Zwecke der besseren Zuordnung der mit Hilfe der Applikation gesammelten Daten und des auszufüllenden Fragebogens wurden die Teilnehmenden gebeten dem Versuchsleiter ihre Device-ID zu übermitteln. Sämtliche Daten im Rahmen der Applikation wie der Name der Berechtigung, die gewählte Option und der Zeitstempel wurden unter dieser Device-ID abgespeichert. Aus diesem Grund wurde die Device-ID, wie schon in Abschnitt 7.3.3 beschrieben, in den Optionen angezeigt. Die Teilnehmenden wurden gebeten einen Bildschirmabzug von ihrem Endgerät während des Anzeigens der Device-ID zu machen (s. Anhang DD) und diesen per E-Mail an den Versuchsleiter zu schicken. Über die E-Mail-Adresse, den persönlichen Code und die Device-ID konnten anschließend die Datensätze der Applikation denen des Fragebogens zugeordnet werden.

7.4.3 Aufgaben

Um einen alltäglichen Gebrauch der Applikation zu simulieren und zu garantieren, dass die Interaktion mit der Applikation regelmäßig stattfindet, wurden einmal täglich über zehn Tage Aufgaben versandt, welche von den Teilnehmenden zu erfüllen waren. Um sicher zu stellen, dass die Aufgaben unverzüglich oder zumindest am selben Tag ausgeführt werden, wurden diese per SMS versandt, sodass die Teilnehmenden ähnlich wie bei einer Push-Nachricht den Erhalt der Aufgaben direkt wahrnehmen konnten. Zusätzlich wurde die Aufgabenstellung teilweise etwas ausführlicher über E-Mail versandt. Einige Teilnehmende mit ausländischer Handynummer erhielten somit die Aufgabenstellung ausschließlich per Mail, wobei andere Teilnehmende die Bitte geäußert haben, ausschließlich über SMS informiert zu werden.

In der ersten Nachricht an die Teilnehmenden wurden diese gebeten die Applikation von dem Server des Fachgebiets „Mensch-Maschine-Systeme“ herunterzuladen, indem Sie auf den beigefügten Link klicken. Hierbei wurden sie darauf hingewiesen, dass sie zur Installation der Applikation die Option der Zulassung von unbekannten Quellen aktivieren müssen. Weiterhin wurden sie gebeten die Aufgaben so zeitnah wie möglich zu erledigen und dem Versuchsleiter ihre Device-ID wie in Abschnitt 7.4.2 beschrieben mitzuteilen. Um zu überprüfen, ob die angegebenen Handynummern der Teilnehmenden aktuell sind, wurden sie gebeten ein X zurückzuschicken. Am darauffolgenden Tag haben sie eine SMS und E-Mail mit den ersten Aufgaben erhalten. Die Aufgaben des ersten Tages beinhalteten das Laden der lokalen Nachrichten, welches auch eine Teilaufgabe jedes weiteren Tages war. Zudem sollte die für sie wichtigste Nachricht geteilt werden. Dabei wurde immer eine kleine Anleitung beigefügt, wie die Aufgaben zu lösen sind. Zum Dialogfeld für die Erteilung der Zugriffsberechtigungen wurden keine weiteren Informationen gegeben, sodass die Teilnehmenden in ihrer Entscheidung der Wahl („Allow“,

„Deny“, „Maybe“) nicht beeinflusst wurden. Am zweiten Tag wurden die Teilnehmenden gebeten die interessanteste Nachricht abzuspeichern und eine Veranstaltung herauszusuchen, um diese im Kalender einzufügen. Die Aufgaben des dritten Tages bestanden darin eine Veranstaltung herauszusuchen, um die Push-Benachrichtigung bei dieser Veranstaltung zu aktivieren. Am vierten Tag wurden die Teilnehmenden gebeten die für sie unwichtigste Nachricht zu teilen, während am fünften Tag sie eine nicht interessante Nachricht speichern und eine nicht interessante Veranstaltung im Kalender eintragen sollten. Die Aufgaben des sechsten Tages beinhalteten wiederum das Heraussuchen einer nicht interessanten Veranstaltung und die Aktivierung der Push-Benachrichtigung. Am siebten Tag wurden die Teilnehmenden erneut gebeten eine nicht interessante Nachricht abzuspeichern und diese zu teilen, während sie am achten Tag die Push-Benachrichtigung einer nicht interessanten Veranstaltung aktivieren und diese teilen sollten. Am neunten Tag wurden die Teilnehmenden gebeten eine Veranstaltung herauszusuchen, die für ihre/ihren beste/n Freund /-in am interessantesten sein könnten zu teilen und die Push-Benachrichtigung zu aktivieren. Die Aufgaben des letzten Tages bestanden, abgesehen vom Abrufen der lokalen Nachrichten, nur darin, eine weitere interessante Nachricht zu speichern. Der genaue Wortlaut der gestellten Aufgaben ist in Anhang CC wiederzufinden.

7.4.4 Fragebogen zu Akzeptanz und Erwünschtheit der temporären Zugriffsberechtigungen

Nachdem die letzten Aufgaben an alle Teilnehmenden versandt wurden, erhielten diese eine weitere Nachricht mit der Bitte, den Fragebogen auszufüllen, dessen Link in der Nachricht enthalten war. Zu Beginn des Fragebogens wurden sie gebeten ihren persönlichen Code einzugeben, um den Datensatz mit dem Datensatz aus der Applikation verknüpfen zu können.

Der erste Block der Fragen bot als Antwortmöglichkeit eine Skala von 1 bis 10, wobei „1“ keiner Zustimmung und „10“ der vollen Zustimmung entspricht. Dabei sollte erfasst werden, ob die Option der temporären Zugriffsberechtigung den Nutzenden aufgefallen ist (Frage 1a) und die Teilnehmenden diese auf ihren privaten Geräten benutzen würden (Frage 1b). Ferner sollte mit der nächsten Unterfrage ermittelt werden, ob die wiederkehrende Anforderung die Zustimmung zu erteilen, Ärgernis in ihnen auslöst (Frage 1c). In Frage 1d werden die Teilnehmenden dazu aufgefordert, zu bewerten, wie wichtig ihnen die Kontrolle über ihre persönlichen Daten ist und in Frage 1e für wie benutzerfreundlich sie die temporäre Zugriffsberechtigung erachten. Hierbei sollte untersucht werden, ob den Teilnehmenden die Benutzerfreundlichkeit wichtiger als der Schutz ihrer Daten ist. Der letzte Unterpunkt (Frage 1f) sollte erheben, ob die Teilnehmenden Gefallen an der temporären Zugriffsberechtigung gefunden haben.

In der zweiten Aufgabe wurden die Teilnehmenden gefragt, wie lange es einer Anwendung erlaubt sein soll eine Zugriffsberechtigung zu erhalten. Als Antwortmöglichkeiten standen die Optionen von „weniger als 30 Minuten“ bis „für immer“ zur Verfügung. Diese Frage wurde ebenfalls gestellt, um zu ermitteln, ob die temporäre Zugriffsberechtigung von den Teilnehmenden erwünscht ist. Im Rahmen der dritten Frage sollten die Teilnehmenden angeben, für welche Berechtigung sie die temporären Zugriffsberechtigungen in Betracht ziehen. Hierbei standen den Teilnehmenden acht Antwortmöglichkeiten zur Verfügung, wobei sie die Möglichkeit auf Mehrfachantworten hatten (Standort, Handy-Speicher, SD-Kartenspeicher, Kontakte, Nachrichten (Messenger), Nachrichten (SMS), Kalender, Mikrofon). In der vierten Frage hatten die Teilnehmenden die Möglichkeit, Verbesserungsvorschläge bezüglich der temporären Zugriffsberechtigung in einem Freitextfeld anzugeben, während sie in der fünften Frage angeben sollten, in welchen alltäglichen Situationen sie die temporäre Zugriffsberechtigung nutzen würden. In der sechsten Frage sollte angegeben werden, was die Teilnehmenden dachten, als sie zum ersten Mal die „Maybe“-Option (der temporären Zugriffsberechtigung) gesehen haben. Mit dieser Frage sollte erfasst werden, ob die Funktionalität der temporären Option richtig interpretiert wurde oder es einer vorherigen Erläuterung bedarf, um den Sinn und Zweck dieser Option zu vermitteln. Die siebte Frage sollte lediglich erfassen, ob die temporäre Zugriffsberechtigung benutzt wurde, um zu ermitteln, ob diese Funktion im Alltag Gebrauch finden würde. In der achten Frage sollten die Teilnehmenden angeben, ob sie die Funktion der temporären Zugriffsberechtigung verstanden haben, indem sie diese kurz erläutern. Im Rahmen der neunten Frage sollten die Teilnehmenden begründen, weshalb sie die temporäre Zugriffsberechtigung benutzt haben. Die zehnte Frage sollte erfassen, ob die Teilnehmenden die vorgesehene Dauer der temporären Zugriffsberechtigung als angemessen empfunden haben oder diese zu kurz bzw. zu lang waren. Ferner wird abgefragt, ob genügend Optionen zur Auswahl verfügbar waren. Mit Hilfe der nächsten Fragegruppe sollten die demographischen Daten der Teilnehmenden erhoben werden. Dafür wurde zunächst in Frage 11 das Geschlecht, in Frage 12 das Alter und in Frage 13 der Bildungsabschluss (kein Abschluss; Sekundarschule / Oberstufe; Abitur / Allgemeine Hochschulreife; Berufsausbildung; Akademischer Abschluss) abgefragt. In Frage 14 sollten die Teilnehmenden ihre Technikaffinität angeben, um zu erfassen, wie intensiv sich mit digitalen Geräten auseinandergesetzt wird. Vor demselben Hintergrund erfasste die 15. Frage die Anzahl der Stunden pro Tag, in denen die Teilnehmenden das Smartphone nutzen (weniger als eine halbe Stunde; mehr als eine halbe Stunde, aber weniger als eine Stunde; mehr als eine Stunde, aber weniger als zwei Stunden; mehr als zwei Stunden, aber weniger als vier Stunden; mehr als vier Stunden). Die 16. Frage sollte mit Hilfe einer siebenstufigen Likert-Skala erfassen, wie wichtig den Teilnehmenden der Schutz ihrer Privatsphäre ist, während sie in der 17. Frage angeben sollten, ob sie aktiv ihre Informationen schützen (Ja; Nein; Ich habe eine Anwendung zum Datenschutz installiert.; Ich versuche, so wenig wie möglich von meinen

Daten offenzulegen.; Ich habe die Bedingungen und Konditionen gelesen, bevor ich eine Anwendung installiere.). Nach dem Beantworten der letzten Frage wurden die Teilnehmenden auf die nächste Seite geleitet, bei der Sie angeben konnten, ob und welche Aufwandentschädigung geleistet werden soll (10 Euro oder eine Versuchspersonenstunde) und wie, bei Auswahl der monetären Entschädigung, diese überwiesen werden soll (PayPal oder Banküberweisung). Der genaue Wortlaut, sowie der Aufbau des Fragebogens kann im Anhang HH eingesehen werden.

7.4.5 Aufklärung

Nach der erfolgreichen Ausführung des Fragebogens wurde die Aufklärung zur Studie an alle Teilnehmenden per E-Mail versendet. In der Aufklärung wurde verdeutlicht, dass der Fokus der Studie auf der temporären Zugriffsberechtigung liegt. Darüber hinaus wurde kurz die Funktion dieser Option erläutert, welche zum Ziel hatte, den Endnutzenden eine informiertere Entscheidung zu ermöglichen und die eingeforderten Berechtigungen nur für einen bestimmten Zeitraum zu erteilen. Außerdem wurde den Teilnehmenden erläutert, dass das Eruieren der Erwünschtheit und Akzeptanz der temporären Zugriffsberechtigungen weitere Ziele waren. Ferner werden die Teilnehmenden darüber in Kenntnis gesetzt, dass lediglich drei Arten von Daten erhoben wurden. Hierunter fallen die Namen der Berechtigungen (Speicher, Mikrophon etc.), die gewählten Optionen („Allow“, „Maybe“, „Deny“) und die Zeitstempel, welche festhalten, wann die Entscheidung getroffen wurde. Weiterhin wurde versichert, dass keine Zugriffe auf die angeforderten Berechtigungen, wie z.B. Standort oder andere sensible Daten, stattgefunden haben, sondern es sich nur um die temporäre Zugriffsberechtigung bzw. deren Akzeptanz und Angemessenheit handele. Darüber hinaus wurden die Teilnehmenden darüber informiert, dass ihnen die Möglichkeit freisteht ihre Daten, die im Rahmen der Studie erhoben wurden, binnen zwei Wochen mittels der Übermittlung ihres persönlichen Codes löschen zu lassen. Nach dem Ablaufen der Frist, können sie weiterhin die Löschung beantragen, jedoch fließen die Daten anonymisiert in die Auswertung der Ergebnisse dieser Studie mit ein. Mit der Unterschrift der Aufklärung gaben die Teilnehmenden das Herunterladen der Daten und die wissenschaftliche Auswertung dieser frei. Der genaue Wortlaut der Aufklärung ist in Anhang EE einzusehen.

7.5 Datenaufbereitung

Im folgenden Kapitel wird ähnlich wie im ersten und zweiten empirischen Versuch die Aufbereitung der Rohdaten und das weitere Vorgehen zur Analyse der Daten erläutert. Datensätze wurden wiederum in eine Tabelle bestehend aus 118 Variablen zusammengeführt und in SPSS importiert. Wie

schon im ersten Versuch ist ein Großteil der Variablen durch die Kategorisierung der Antworten entstanden.

7.5.1 Demographische Daten der Stichprobe

Wie schon in den vorherigen Versuchen wurde das Geschlecht kodiert, indem den männlichen Teilnehmern eine „1“ und den weiblichen Teilnehmern eine „2“ zugeordnet wurde. Das Alter bedurfte keiner weiteren Aufbereitung.

Die Antworten zur Frage des höchsten Bildungsabschlusses wurden umkodiert, indem der Antwort „kein Abschluss“ eine „1“, „Sekundär Stufe/Oberschule“ eine „2“, „Abitur/ Allgemeine Hochschulreife“ eine „3“, „Berufsausbildung“ eine „4“ und „akademischer Abschluss“ eine „5“ zugeordnet wurde.

Die Antworten bezüglich der Technikaffinität und der Wichtigkeit der Privatsphäre wurden auf einer zehnstufigen Skala mit den Polen „trifft überhaupt nicht zu“ und „trifft voll und ganz zu“ beantwortet. Den Antworten wurden entsprechende Werte von „1“ bis „10“ zugewiesen, um es zu ermöglichen, die Mittelwerte der verschiedenen Gruppen zu berechnen.

Bezüglich der Frage zur täglichen Handynutzung wurden die Antworten „weniger als eine halbe Stunde“ mit einer „1“, „mehr als eine halbe Stunde aber weniger als eine Stunde“ mit einer „2“, „mehr als eine Stunde aber weniger als zwei Stunden“ mit einer „3“, „mehr als zwei Stunden aber weniger als vier Stunden“ mit einer „4“ und „mehr als vier Stunden“ mit einer „5“ kodiert.

Die Antworten der Frage zu der Wichtigkeit der Privatsphäre, welche mit einer siebenstufigen Likert-Skala erfasst wurden, wurden ebenfalls in Ziffern von „1“ bis „7“ umkodiert, wobei die Antwort „trifft überhaupt nicht zu“ einer „1“ und „trifft völlig zu“ einer „7“ entsprach.

Bei der Frage, ob die Teilnehmenden aktiv tätig sind, um ihre Privatsphäre zu schützen, wurde dieselbe Kodierung wie im Abschnitt 6.7.1 angewandt, bei der jeder Antwortmöglichkeit eine neue Variable zugeordnet wurde, um somit Mehrfachantworten zu ermöglichen.

7.5.2 Fragebogen über die Akzeptanz der temporären Zugriffsberechtigung

Auch der Fragebogen des dritten Versuches wurde über das Portal LimeSurvey der Technischen Universität Berlin ausgefüllt. Dies ermöglichte den Import sämtlicher Daten in SPSS.

Zu Beginn wurde der Personencode abverlangt, welcher ohne weitere Datenaufbereitung in SPSS importiert wurde. Die erste Frage bezüglich der Bewertung der Aussagen bedurfte keiner weiteren Datenaufbereitung, weil die Teilnehmenden diese auf einer Skala von „1“ (stimmt nicht zu) bis „10“ (stimmt voll und ganz zu) bewerten sollten. Die Antworten wurden im Anhang FF unter den Nummern 9 bis 15 in SPSS eingepflegt. Weiterhin wurden die Antworten der zweiten Frage, welche erfassen sollte wie lange eine Anwendung auf eine Zugriffsberechtigung zugreifen darf, wie folgt kodiert: die Antwort „weniger als 30 Minuten“ wurde mit einer „1“, „30 Minuten“ mit einer „2“, „1 Stunde“ mit einer „3“, „6 Stunden“ mit einer „4“, „12 Stunden“ mit einer „5“, „1 Tag“ mit einer „6“, „2 Tage“ mit einer „7“, „1 Woche“ mit einer „8“, „2 Wochen“ mit einer „9“, „1 Monat“ mit einer „10“, „6 Monate“ mit einer „11“, „1 Jahr“ mit einer „12“ und „für immer“ mit einer „13“ kodiert (s. Anhang FF Nr. 13). Die dritte Frage sollte erfassen, welche Berechtigungen die Teilnehmenden für die temporäre Zugriffsberechtigung in Betracht ziehen. Hierbei waren Mehrfachantworten möglich, deshalb wurde aus jeder Antwort eine Variable generiert (s. Anhang FF Nr. 16-23) und diese bei der Auswahl mit einer „1“ und bei Nichtauswahl mit einer „2“ versehen.

Die vierte Frage, bei der die Teilnehmenden gebeten wurden, Verbesserungsvorschläge zu nennen, bedurfte einer etwas umfangreicheren Datenaufbereitung, weil die Antworten in ein Freitextfeld eingegeben wurden. Für die Auswertung wurden die Antworten nach ihrem Inhalt kategorisiert und diese Kategorien als neue Variablen in SPSS eingepflegt. Aufgrund der Tatsache, dass viele Verbesserungsvorschläge nur einmalig von einzelnen Personen genannt wurden, diese jedoch trotzdem aufgezeigt werden sollten, wurden auch Kategorien für Verbesserungsvorschläge gebildet, die nur einmal genannt wurden. Anschließend wurde in den neu gebildeten Variablen eine „1“ eingetragen, wenn die Versuchsperson diese Kategorie inhaltlich als Verbesserungsvorschlag erwähnte. Insgesamt wurden 13 Variablen eingefügt, welche im Anhang FF unter den Nummern 25 bis 37 wiederzufinden sind.

Das gleiche Verfahren der Kategorisierung wurde bei der fünften (s. Anhang FF Nr. 39-47), sechsten (s. Anhang FF Nr. 49-53), achten (s. Anhang GG Nr. 56-58), neunten (s. Anhang FF Nr. 60-65) und elften Frage (s. Anhang FF Nr. 67, 69, 71, 73, 75) angewandt.

Für die siebte Frage, welche erfassen sollte, ob die Teilnehmenden auf die Optionen der temporären Zugriffsberechtigung geklickt haben, wurde die bejahende Antwort mit „1“ und die verneinende Antwort mit „2“ kodiert (s. Anhang FF Nr. 54). Für die zehnte Frage, in der die Teilnehmenden angeben sollten, ob die vorgegebene Dauer der temporären Zugriffsberechtigung angemessen war, wurden mehrere Variablen erstellt (s. Anhang FF Nr. 66-75).

7.5.3 Device ID

Die Device ID, welche in der Applikation unter den Einstellungen angezeigt wurde, sollte von den Teilnehmenden durch die Erzeugung eines Bildschirmfotos, welches anschließend per E-Mail an den Versuchsleiter gesandt wurde, übermittelt werden. Anschließend wurde die Device ID mit dem Personencode verknüpft. Somit lassen sich die Daten des Fragebogens mit denen der Applikation verbinden.

7.5.4 Applikationsdaten

Die Applikationsdaten, welche aus den Namen der Berechtigung, der gewählten Option und dem Zeitstempel besteht, wurden von der Nachrichtenapplikation in eine SQL-Datenbank eingespeist. Dabei wurde bei jeder Zugriffsanfrage die Device ID neu aufgeführt. Die SQL-Datenbank wurde in eine Excel-Datei konvertiert, wobei diese bereinigt wurde, indem der Kopf und das Ende entfernt wurden. Insgesamt wurden 219 Zugriffsanfragen aufgelistet. Um die Anfragen mit Hilfe der Device ID und des Personencodes zu verknüpfen und die Daten personengebunden in SPSS einzufügen, wurden alle Anfragen einer Device ID in einer Zeile zusammengefügt, indem insgesamt 23 neue Variablen gebildet wurden. Die erste Gruppe der Variablen setzt sich aus der Zugriffsanfrage und der Zugriffsberechtigung zusammen (z.B. APP_accept). Die Variablen sind im Anhang FF unter Nummer 93 bis 107 einzusehen.

Die eingetragenen Werte in diesen Variablen entsprechen der Häufigkeit wie oft die Zugriffsberechtigung für die Zugriffsanfrage unter dieser Device ID erteilt wurde. Ferner wurden drei Variablen erstellt (s. Anhang FF Nr. 108-110), um festzuhalten wie oft die entsprechende Device ID insgesamt die Optionen „Allow“, „Maybe“ und „Deny“ verwendet hat. In fünf weiteren Variablen (s. Anhang FF Nr. 11-115) wurde festgehalten, wie lange eine Device ID die temporären Zugriffsberechtigungen stattgegeben hat. Wurde beispielsweise während des gesamten Versuchszeitraumes zweimal die temporäre Zugriffsberechtigung jeweils mit einem und mit drei Tagen erteilt, so summieren sich diese Berechtigungszeiträume zu einer vier zusammen.

Weiterhin wurde in den Variablen von Nummer 116 bis 118 (s. Anhang FF) festgehalten, wie oft ein Teilnehmer eine gewisse Dauer von einen, drei oder sieben Tagen gewählt hat.

7.6 Ergebnisse

Das folgende Kapitel beinhaltet die Ergebnisse der durchgeführten Studie zur Akzeptanz und Verwendung einer temporären Zugriffsberechtigung. Das erste Kapitel beinhaltet die demografischen Daten der Teilnehmenden, während das zweite Kapitel die Ergebnisse des Fragebogens näher betrachtet. Das dritte Kapitel stellt die Ergebnisse der Applikationsdaten vor, welche über den Zeitraum von zehn Tagen erfasst wurden.

7.6.1 Demographische Daten der Stichprobe

An der Onlinestudie nahmen insgesamt 32 deutschsprachige Personen teil. Die Alterspanne liegt bei der Stichprobe zwischen 20 und 64 Jahren mit einem Durchschnitt von 29,68 Jahren und einer Standardabweichung von 9,18. Darüber hinaus sind elf Teilnehmer männlich und 20 Teilnehmerinnen weiblich (s. Tabelle 178, Anhang GG). Ihr Bildungshintergrund variiert von der Mittelschule bis zu höheren akademischen Graden: 14 von ihnen haben ein Abitur, zwei haben eine Berufsausbildung abgeschlossen und 15 besitzen höhere akademische Abschlüsse von Universitäten (s. Tabelle 179, Anhang GG). Dabei verbringt eine Person mehr als 30 Minuten, sieben Personen mehr als eine Stunde, 14 Personen mehr als zwei Stunden und neun Personen mehr als fünf Stunden mit ihrem Smartphone (s. Tabelle 180, Anhang GG). Die Verteilungen der Daten, sind zur besseren Veranschaulichung in Abbildung 26 illustriert.

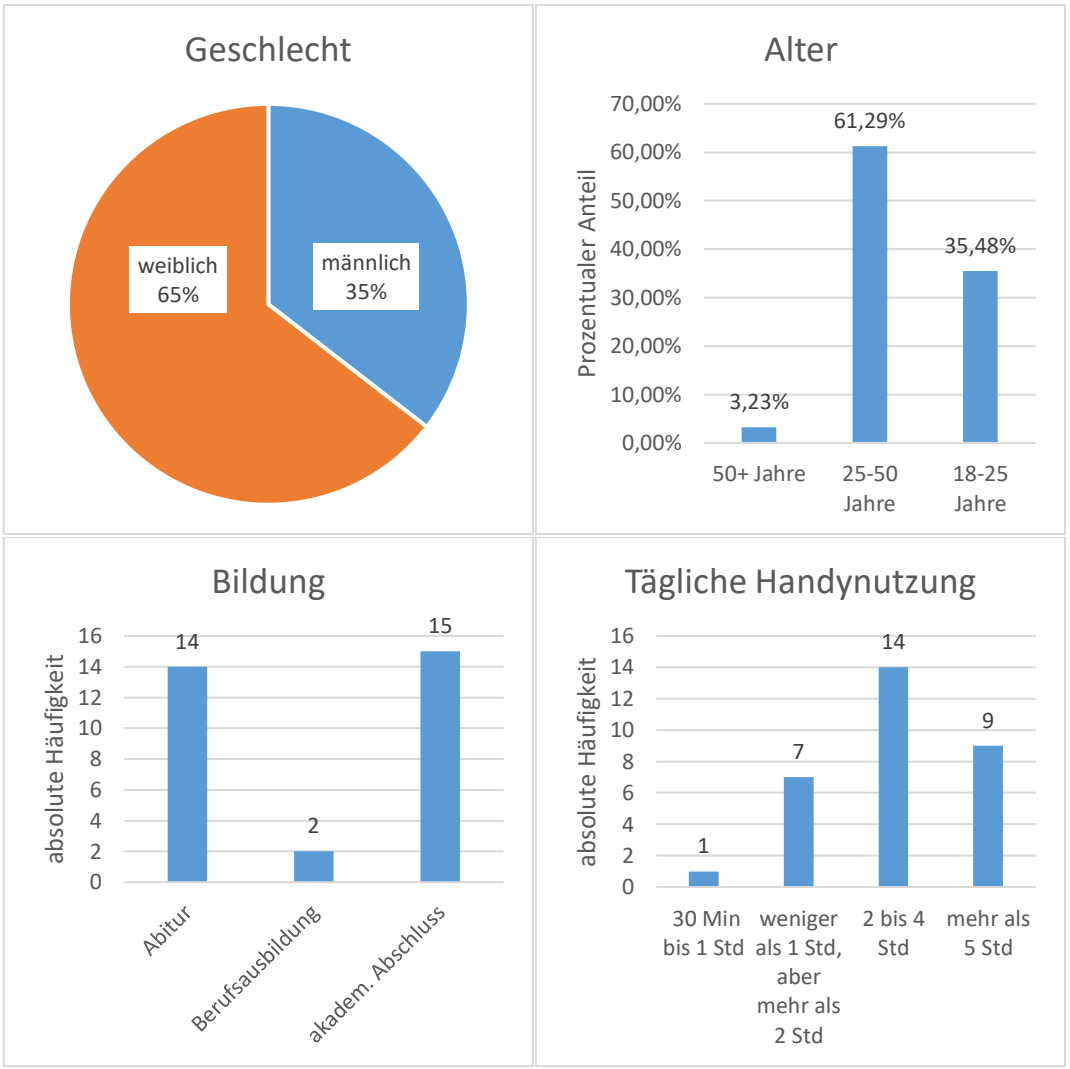


Abbildung 26. Verteilung des Geschlechtes, des Alters, der Bildung und der Handynutzung der Stichprobe.

Der Aussage „Ich habe eine große Affinität zur Technik“ beantworteten zwölf Personen (38,7 %) mit einer „7“ auf einer Skala von „1“ bis „10“. Weitere zwölf (38,7 %) Personen bewerteten ihre technische Affinität besser als eine „7“, während weitere sieben (22,58 %) Personen ihre technische Affinität mit schlechter als „7“ bewerteten (s. Tabelle 181, Anhang GG).

Bei der Frage nach der Wichtigkeit des Schutzes der Privatsphäre, welche auf einer Likert-Skala von „trifft überhaupt nicht zu“ (1) bis „trifft völlig zu“ (7) dargestellt wurde, resultierte ein Mittelwert von 5,97 (*SD* = 0,91) (s. Tabelle 182, Anhang GG).

Bei der Frage, ob die Teilnehmenden aktiv sind, um ihre Daten zu schützen, haben insgesamt 22 Personen (70,97 %) angegeben dies zu tun, während neun Personen (29,03 %) angaben, den aktiven Schutz der Daten zu unterlassen. Fünf Personen (16,13 %) gaben an, eine Applikation zum Schutz ihrer Daten installiert zu haben, während 13 Personen (41,94 %) angaben, so wenige Daten wie möglich von

ihrer Person preiszugeben. Die AGBs zu lesen, bevor eine Applikation installiert wird, gaben sechs Personen (19,36 %) an (s. Tabelle 183, Anhang GG).

7.6.2 Fragebogen über die Akzeptanz der vorübergehenden Datenfreigabe

In den folgenden Kapiteln werden die Angaben der Teilnehmenden, die sie im Fragenbogen getätigt haben, aufgezeigt und analysiert.

In der ersten Frage des Fragebogens sollen die Teilnehmenden auf einer Skala von „1“ („stimmt nicht zu“) bis „10“ („stimmt voll und ganz zu“) angeben, ob sie den vorgegebenen Aussagen zustimmen oder nicht zustimmen.

Bezüglich der Aussage, dass die Option der temporären Zugriffsberechtigung aufgefallen sei, wird ein Mittelwert von 5,1 (*SD* = 3,6) errechnet. Dabei haben die Teilnehmenden vor allem die Skalenwerte an den beiden Polen gewählt. So wurde die „1“ von neun Teilnehmenden (29,03 %) und die „10“ von acht Teilnehmenden (25,81 %) gewählt. Der am dritthäufigsten gewählte Skalenwert belegt die „5“, welche von sechs Teilnehmenden (19,35 %) gewählt wurde. Alle weiteren Skalenwerte wurden von zwei Teilnehmenden (6,45 %) oder weniger gewählt. Nach dem Teilen der Stichprobe in zwei Gruppen resultieren 20 Teilnehmende (64,52 %), die der Aussage (mit einem Wert von ≤ 5) nicht zustimmen und elf Teilnehmende (35,48 %), die der Aussage (mit einem Wert von ≥ 6) zustimmen.

Bei der Aussage, dass die Teilnehmenden die temporäre Zugriffsberechtigung auf ihrem privaten Gerät benutzen würden, wird ein Mittelwert von 5,35 (*SD* = 3,03) errechnet. Bei Betrachtung der Häufigkeit der Auswahl der Skalenwerte fällt hierbei auf, dass am häufigsten die „5“ von sieben Teilnehmenden (22,6 %) und am zweithäufigsten die „1“ von sechs Teilnehmenden (19,4 %) gewählt wurde. Die „6“ und die „9“ wurden von vier Teilnehmenden (12,9 %) gewählt, während alle weiteren Werte von zwei Teilnehmenden (6,5 %) oder weniger gewählt wurden. Nach dem Teilen der Stichprobe in zwei Gruppen resultieren 17 Teilnehmende (54,9 %), die der Aussage nicht zustimmten und 14 Teilnehmende (45,1 %), die der Aussage zustimmten.

Die Aussage, dass die immer wiederkehrende Aufforderung die Zustimmung zu erteilen Ärgernis auslöst, erlangt einen Mittelwert von 4,32 (*SD* = 2,87). Am häufigsten wurde hierbei die „1“ von sieben Teilnehmenden (22,6 %) gewählt, während die zweithäufigsten Werte von „2“ und „5“ von jeweils fünf Teilnehmenden (16,1 %) gewählt wurden. Mit Ausnahme der „8“ (3 Teilnehmende; 9,7 %) wurden alle weiteren Skalenwerte von zwei Teilnehmenden (6,5 %) oder weniger gewählt. Nach dem Teilen der

Stichprobe in zwei Gruppen resultieren 21 Teilnehmende (67,8 %), die der Aussage nicht zustimmten und zehn Teilnehmende (32,4 %), die der Aussage zustimmten.

Die Aussage, dass die Kontrolle der persönlichen Daten wichtig sei, erreicht den höchsten Mittelwert von 8,19 (*SD* = 1,94) und wurde von elf Teilnehmenden (35,5 %) mit einem Skalenwert von „10“ bestätigt und von sechs Teilnehmenden (19,4 %) mit einem Skalenwert von „9“ bestätigt. Am dritthäufigsten wurden die Skalenwerte „7“ und „8“ von jeweils vier Teilnehmenden (12,9 %) gewählt. Alle weiteren Skalenwerte wurden von drei Teilnehmenden (9,7 %) oder weniger gewählt, wobei die Skalenwerte „1“, „2“ und „4“ nicht gewählt wurden. Nach dem Teilen der Stichprobe in zwei Gruppen resultieren vier Teilnehmende (12,9 %), die der Aussage nicht zustimmten und 27 Teilnehmende (87,2 %), die der Aussage zustimmten.

Bezüglich der Aussage, dass die Benutzerfreundlichkeit wichtiger sei als der Schutz persönlicher Daten ist ein Mittelwert von 4 (*SD* = 2,7) zu verzeichnen. Dabei wurden am häufigsten die Skalenwerte „1“ und „3“ von jeweils sieben Teilnehmenden (22,6 %) gewählt. Der dritthäufigste Skalenwert „6“ wurde von fünf Teilnehmenden gewählt. Alle anderen Werte wurden von drei (9,7 %) oder weniger Teilnehmenden gewählt, während die „7“ nicht gewählt wurde. Nach dem Teilen der Stichprobe in zwei Gruppen resultieren 22 Teilnehmende (71,1 %), die der Aussage nicht zustimmten und neun Teilnehmende (29 %), die der Aussage zustimmten.

Bezüglich der Aussage, ob die Option der temporären Zugriffsberechtigung Gefallen findet, kann ein Mittelwert von 5,87 (*SD* = 2,33) verzeichnet werden. Am häufigsten wurde hierbei der Skalenwert „5“ von insgesamt zwölf Teilnehmenden (38,7 %), während die Skalenwerte von „7“ und „9“ mit jeweils vier Teilnehmenden (12,9 %) am zweithäufigsten und die Skalenwerte „1“, „6“ und „8“ am dritthäufigsten von drei Teilnehmenden (9,7 %) gewählt wurden. Alle weiteren Skalenwerte wurden seltener gewählt, wobei die Skalenwerte „2“ und „4“ nicht gewählt wurden. Nach dem Teilen der Stichprobe in zwei Gruppen resultieren 16 Teilnehmende (51,6 %), die der Aussage nicht zustimmten und 15 Teilnehmende (48,4 %), die der Aussage zustimmten. Zur besseren Übersicht befindet sich die Tabelle 184 mit den Ergebnissen in Anhang GG.

Die zweite Frage, welche erfassen soll, wie lange eine Anwendung auf eine Zugriffsberechtigung zugreifen darf, wurde von fünf Teilnehmenden (16,1 %) mit „weniger als 30 Minuten“ beantwortet. Vier Teilnehmende (12,9 %) gaben jeweils an, dass eine Zeitspanne von „1 Tag“, „1 Woche“ und „1 Monat“ angemessen wäre. Jeweils drei Teilnehmende (9,7 %) gaben an, dass eine Dauer von „1 Stunde“, „2 Wochen“ und „6 Monate“ adäquat wäre. Jeweils zwei Teilnehmende gaben an, dass eine Zeitspanne von „12 Stunden“ und die dauerhafte Zugriffsberechtigung angemessen wären. Lediglich eine Person empfand, dass eine Zeitspanne von zwei Tagen genüge. Zur besseren Veranschaulichung

wurden die Ergebnisse in ein Balkendiagramm implementiert (s. Abbildung 26). Eine Übersicht der Ergebnisse befindet sich in Tabelle 185 im Anhang GG.

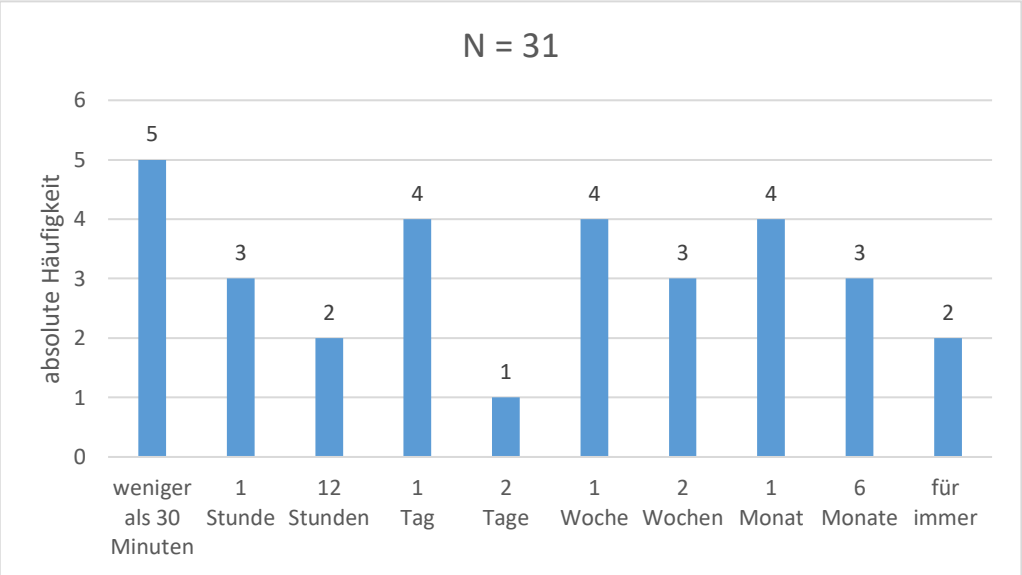


Abbildung 27. Verteilung der gewünschten Dauer der temporären Zugriffsberechtigung.

Diese Abbildung illustriert die Häufigkeit der ausgewählten Zeitspannen, welche die Teilnehmenden als angemessen für die temporäre Zugriffsberechtigung ansehen.

Bei der dritten Frage, welche gestellt wurde, um zu erfassen für welche Berechtigungen die temporäre Zugriffsberechtigung in Betracht gezogen wird, stimmten 25 Teilnehmende (80,6 %) für die Implementierung dieser Funktion bei dem Standort. Bei allen anderen Berechtigungen stimmte die Mehrheit der Teilnehmenden gegen die Implementierung der temporären Zugriffsberechtigung (Nachrichten (SMS): 41,9 %; Kalender: 41,9 %; Handy-Speicher: 35,5 %; Kontakte: 35,5 %; Nachrichten (Messenger): 29 %; Mikrofon: 29 %; SD-Kartenspeicher: 19,4 %). Eine Übersicht der Ergebnisse ist in Tabelle 187 im Anhang GG zu finden.

Nach der Auswertung der vierten Frage, bei der die Teilnehmenden die Möglichkeit hatten, Verbesserungsvorschläge bezüglich der Option der temporären Rechtefreigabe einzugeben, wird ersichtlich, dass neun Teilnehmende (29,03 %) keine Verbesserungsvorschläge vorwiesen. Fünf Teilnehmende gaben an, sich die Option einer beliebigen Zeit zu wünschen, für die die temporäre Zugriffsberechtigung erteilt wird. Vier der Teilnehmenden (12,9 %) wünschten sich Verbesserung bezüglich der Sichtbarkeit der temporären Zugriffsberechtigung, also der „Maybe“-Schaltfläche. Jeweils drei Teilnehmende wünschten sich längere Intervalle für die temporäre Zugriffsberechtigung und Verbesserungen hinsichtlich des Designs, sodass es beispielsweise besser einprägsam sein sollte.

Darüber hinaus gibt es jeweils einzelne Verbesserungsvorschläge (3,23 %) bezüglich längerer Zeitintervalle für die temporäre Zugriffsberechtigung. Zudem wurde sich eine Übersicht oder ein Berechtigungskonzept gewünscht, welches anzeigt, wer auf welche Daten zugreifen darf. Es wurde ebenfalls vorgeschlagen eine Zeiterfassung zu implementieren, welche illustriert, wie lange eine Applikation eine bestimmte Zugriffsberechtigung erteilt bekommen hat. Ferner wurde als Verbesserung genannt, die Zugriffsberechtigung nur zu erteilen, wenn die Applikation aktiv genutzt wird und nicht im Hintergrund läuft. Ein weiterer Vorschlag ist es, die Zugriffsberechtigung nur für eine bestimmte Anzahl an Zugriffen zu erteilen und den temporären Aspekt somit auszuschließen. Weiterhin wurde sich eine Erläuterung gewünscht, wofür die angeforderten Zugriffsberechtigungen von Nöten sind. Ein weiterer Wunsch war die Übersetzung der Oberfläche auf die Muttersprache der Endnutzenden und eine Erläuterung der Funktion, z.B. in Form einer Infobox (s. Tabelle 188, Anhang GG).

Die Auswertung der fünften Frage, die erfassen soll, in welchen alltäglichen Situationen die temporäre Zugriffsberechtigung genutzt werden würde, verdeutlicht, dass die Funktion besonders erwünscht ist, wenn die Endnutzenden ihren Standort ändern oder diesen mit Freunden teilen möchten. Insgesamt gaben neun Teilnehmende (29,03 %) an, die Funktion beim Wechseln ihres Standortes zu nutzen. Drei Teilnehmende (9,68 %) gaben an, die Funktion bei Applikationen nutzen zu wollen, die nur kurz für eine bestimmte Aufgabe auf dem Endgerät installiert und anschließend wieder gelöscht wurde. Drei weitere Teilnehmende würden die Funktion bei Applikationen nutzen, die über einen Zugriff auf persönliche Daten verfügen, wie z.B. Nachrichten und Bilder. Zwei der Teilnehmenden (6,45 %) gaben an, die Funktion niemals nutzen zu wollen. Ferner haben vier weitere Teilnehmende jeweils eine alltägliche Situation genannt, worunter das Installieren von neuen Applikationen, das Aufhalten am Arbeitsplatz, das seltene Nutzen von installierten Applikationen und die Terminplanung fällt (s. Tabelle 192, Anhang GG).

Die sechste Frage, mit welcher der erste Eindruck der Teilnehmenden festgehalten werden soll, ergab, dass acht Teilnehmende (25,81 %) die Schaltfläche („Maybe“-Option) der temporären Zugriffsberechtigung zwar bemerkt haben, sich jedoch keine weiteren Gedanken darüber gemacht haben. Fünf Teilnehmende (16,13 %) haben positive Bemerkungen über die temporäre Zugriffsberechtigung geäußert. Die Funktion wurde dabei als „gut“ und „interessant“ beschrieben. Jeweils vier Teilnehmende (12,90 %) gaben an, die Schaltfläche nicht wahrgenommen zu haben oder die Funktion nicht verstanden zu haben. Lediglich zwei Teilnehmende (6,45 %) äußerten sich negativ über die Funktion und bemängelten die fehlende Erläuterung über die Funktionsweise (s. Tabelle 190, Anhang GG).

Die siebte Frage, welche lediglich erfassen soll, ob die „Maybe“-Funktion genutzt wurde, ergab, dass insgesamt 32,3 % der Teilnehmenden die temporäre Zugriffsberechtigung verwendet haben (s. Tabelle 191 , Anhang GG).

Die achte Frage soll erheben, ob die Teilnehmenden die Funktion der temporären Zugriffsberechtigung richtig verstanden haben. Hierbei ist zu erwähnen, dass die Frage nur angezeigt wurde, wenn in der vorherigen Frage die Nutzung der „Maybe“-Funktion bestätigt wurde. Von diesen zehn Teilnehmenden, welche die Nutzung bestätigt haben, gaben sieben (70 %) eine richtige Erläuterung der Funktion ab. Eine Person gab zwar an, die Funktionsweise verstanden zu haben, unterließ jedoch die Erläuterung der Funktion. Eine weitere Person gab eine falsche Erläuterung der Funktion an, während eine Testperson eine Antwort abgegeben hat, die eher die sechste Frage bezüglich des ersten Eindrucks beantwortet als das Verständnis der Funktion wiedergibt (s. Tabelle 192, Anhang GG).

Die neunte Frage soll die Motive der Teilnehmenden erfassen, die dazu geführt haben, dass sie die Option der temporären Zugriffsberechtigung genutzt haben. Dabei haben acht Teilnehmende (25,81 %) angegeben, die Funktion nicht genutzt zu haben, während sechs Teilnehmende (19,35 %) keinen Grund für die Nutzung dieser Funktion angaben. Der temporäre Gebrauch der Applikation wurde von fünf Teilnehmenden (16,13 %) als Grund für die Funktion genannt. Jeweils drei Teilnehmende (9,68 %) gaben an, die Funktion genutzt zu haben, um mehr Kontrolle über ihre Daten und Privatsphäre zu erlangen sowie den Datenschutz zu steigern. Zwei Teilnehmende (6,45 %) gaben an, die temporäre Zugriffsberechtigung genutzt zu haben, weil sie der Applikation misstrauten (s. Tabelle 193, Tabelle 189, Anhang GG).

In der zehnten Frage wird erfasst, ob die vorgegebene Auswahl der Dauer von einem, drei und sieben Tagen für die temporäre Zugriffsberechtigung angemessen war. Insgesamt 19 Teilnehmende (61,3 %) sind mit der Dauer der temporären Zugriffsberechtigung zufrieden, wobei jeweils vier Teilnehmende angaben, dass die Intervalle zu kurz waren und zu wenige Optionen bezüglich der Intervallslänge vorhanden waren. Zwei Teilnehmende (6,5 %) gaben an, dass die Intervalle zu lang waren. Insgesamt gaben fünf Teilnehmende sonstige Gründe an. Vier Teilnehmende gaben als Grund an, die Option der temporären Zugriffsberechtigung nicht bemerkt zu haben oder sich nicht an die Intervallslänge erinnern zu können. Eine Person brachte den Vorschlag, davor eine Option einzubauen, welche es der Applikation erlaubt, nur auf die Berechtigung zuzugreifen, solange die Applikation geöffnet und im Vordergrund ist (s. Tabelle 194, Anhang GG).

In dem folgenden Abschnitt werden einige Korrelationen und Signifikanztests zwischen den Antworten, die von den Teilnehmenden innerhalb des Fragebogens gegeben wurden, näher betrachtet. Zunächst soll erfasst werden, ob ein Zusammenhang zwischen dem Auffallen der „Maybe“-

Option (Frage 1 Aussage 1) und dem Gefallen (Frage 1 Aussage 6) dieser zu finden ist. Aufgrund der Abwesenheit einer Normalverteilung bei beiden Datensätze wird der Spearman-Rho-Test durchgeführt. Hierbei kann ein positiver Zusammenhang (r = 0,105) festgestellt werden, der jedoch mit p < .575 als nicht signifikant resultiert. Anschließend wird geprüft, ob ein Zusammenhang zwischen dem Auffallen der „Maybe"-Option und der Kontrolle der persönlichen Daten (Frage 1 Aussage 4) vorhanden ist. Hierbei wird erneut ein Spearman-Rho-Test durchgeführt, welcher mit r = -261 und p < .041 einen signifikanten negativen Zusammenhang mittlerer Effektstärke ergibt (s. Tabelle 195, Anhang GG).

Als nächstes wird geprüft, ob die Wichtigkeit des Schutzes der Privatsphäre mit den Aussagen aus der ersten Frage korreliert. Hierzu wird ebenfalls ein Spearman-Rho-Test durchgeführt, weil der Datensatz zur Wichtigkeit des Schutzes der Privatsphäre keine Normalverteilung aufweist. Hierbei kann lediglich ein positiver (r = 0,72) signifikanter (p < .000) Zusammenhang mit großer Effektstärke zwischen der Wichtigkeit der Kontrolle der persönlichen Daten (Frage 1 Aussage 4) erfasst werden. Alle weiteren Korrelationen ergeben keine Signifikanz (s. Tabelle 196, Anhang GG).

In einem weiteren Schritt wird geprüft, ob die Antworten der zweiten Frage, welche die präferierte Dauer der Teilnehmenden für die temporäre Zugriffsberechtigung festhalten soll, mit den Aussagen der ersten Frage korrelieren. Hierbei kann nur ein signifikanter (p < .043) negativer Zusammenhang (r = -0,37) einer mittleren Effektstärke ebenfalls mit der Wichtigkeit der Kontrolle der persönlichen Daten gefunden werden (s. Tabelle 197, Anhang GG).

Ferner wird die technische Affinität mit den Aussagen der ersten Frage korreliert, wobei sich lediglich ein positiver und signifikanter Zusammenhang eines mittleren Effekts zwischen der technischen Affinität und des Ärgernisses über die sich wiederholenden Berechtigungsanfragen ergibt (s. Tabelle 198, Anhang GG).

Beim Korrelieren der täglichen Handynutzung (Frage 15) und des Alters (Frage 12) mit den Aussagen aus Frage 1 können keine signifikanten Zusammenhänge gefunden werden (s. Tabelle 199, Tabelle 200, Anhang GG). Ebenso ergibt die Korrelation zwischen der technischen Affinität und die tägliche Dauer des Gebrauches des mobilen Endgerätes keinen signifikanten Zusammenhang (s. Tabelle 201, Anhang GG).

7.6.3 Applikationsdaten

Nach der Aufbereitung der Applikationsdaten kann eingesehen werden, welche Optionen bei den einzelnen Zugriffsberechtigungen gewählt wurden. Über die Dauer von zehn Tagen und der Stellung von insgesamt 24 Aufgaben wurden vier Aufgaben bezüglich der Aktivierung der Push-Benachrichtigung gestellt. Dabei haben fünf Teilnehmende (16,1 %) nicht einmal die Zugriffsberechtigung akzeptiert, während 26 Personen (83,9 %) die Berechtigung einmalig erteilt („Allow“) haben. Die Zugriffsberechtigung wurde von 30 Personen (96,8 %) nicht einmal, jedoch von einer Person (3,2 %) zweimal abgelehnt („Deny“). Die temporäre Zugriffsberechtigung haben zwei Teilnehmende (6,5 %) dreimal, zwei weitere (6,5 %) zweimal und eine einzelne Person (3,2 %) einmal gewählt. Somit haben insgesamt 26 Teilnehmende (83,9 %) die Option bei dieser Zugriffsberechtigung nicht gewählt. Insgesamt wurde ungeachtet, wie oft eine Person eine Option gewählt hat, sich 26-mal (66,7 %) für die Option „Allow“, zweimal (5,1 %) für die Option „Deny“ und elfmal (28,2 %) für die temporäre Zugriffsberechtigung „Maybe“ entschieden.

Insgesamt wurden zehn Aufgaben bezüglich der Freigabe der Positionsdaten (Location) gestellt. Dabei haben zwei Teilnehmende (6,5 %) nicht einmal die Zugriffsberechtigung akzeptiert, während 29 Personen (93,5 %) die Berechtigung einmal erteilt („Allow“) haben. Die Zugriffsberechtigung wurde von 27 Personen (87,1 %) nicht einmal, jedoch von drei Personen (9,7 %) einmal und von einer Person (3,2 %) zweimal abgelehnt („Deny“). Die temporäre Zugriffsberechtigung haben zwei Teilnehmende (6,5 %) sechsmal gewählt. Somit haben insgesamt 29 Teilnehmende (93,5 %) die temporäre Option bei der Freigabe der Positionsdaten nicht gewählt. Insgesamt wurde 29-mal (74,4 %) die Option „Allow“, fünfmal (12,8 %) die Option „Deny“ und zwölfmal (30,8 %) die temporäre Zugriffsberechtigung „Maybe“ gewählt.

Bezüglich der Freigabe der Kontaktdaten (Contacts) wurden fünf Aufgaben gestellt. Dabei haben sechs Teilnehmende (19,4 %) nicht einmal die Zugriffsberechtigung akzeptiert, während 25 Personen (80,6 %) die Berechtigung einmal erteilt („Allow“) haben. Die Zugriffsberechtigung wurde von 28 Personen (90,3 %) nicht einmal, jedoch von zwei Personen (6,5 %) einmal und von einer Person (3,2 %) zweimal abgelehnt („Deny“). Die temporäre Zugriffsberechtigung haben zwei Teilnehmende (6,5 %) viermal, zwei weitere Teilnehmende (6,5 %) dreimal und ein Einzelner (3,2 %) zweimal gewählt. Somit haben insgesamt 26 Teilnehmende (83,9 %) die Option bei dieser Zugriffsberechtigung nicht gewählt. Insgesamt wurde 25-mal (64,1 %) die Option „Allow“, viermal (10,3 %) die Option „Deny“ und 16-mal (41 %) die temporäre Zugriffsberechtigung „Maybe“ gewählt.

Weitere vier Aufgaben wurden bezüglich der Freigabe des Gerätespeichers (Device Storage) gestellt. Dabei haben vier Teilnehmende (12,9 %) nicht einmal die Zugriffsberechtigung akzeptiert, während 27

Personen (87,1 %) die Berechtigung einmalig erteilt („Allow“) haben. Die Zugriffsberechtigung wurde von 30 Personen (96,8 %) nicht einmal, jedoch von einer Person (3,2 %) dreimal abgelehnt („Deny“). Die temporäre Zugriffsberechtigung haben drei Teilnehmende (9,7 %) viermal, eine Person (3,2 %) dreimal und eine weitere Person (3,2 %) zweimal gewählt. Somit haben insgesamt 26 Teilnehmende (83,9 %) die Option bei dieser Zugriffsberechtigung nicht gewählt. Insgesamt wurde 27-mal (69,2 %) die Option „Allow“, dreimal (7,7 %) die Option „Deny“ und 17-mal (43,6 %) die temporäre Zugriffsberechtigung „Maybe“ gewählt.

Lediglich zwei Aufgaben wurden bezüglich der Freigabe des Kalenders (Calender) gestellt. Dabei haben sechs Teilnehmende (19,4 %) nicht einmal die Zugriffsberechtigung akzeptiert, während 25 Personen (80,6 %) die Berechtigung einmal erteilt („Allow“) haben. Die Zugriffsberechtigung wurde von 30 Personen (96,8 %) nicht einmal, jedoch von einer Person (3,2 %) zweimal abgelehnt („Deny“). Die temporäre Zugriffsberechtigung haben vier Teilnehmende (12,9 %) zweimal, eine Person (3,2 %) einmal gewählt. Somit haben insgesamt 26 Teilnehmende (83,9 %) die Option bei dieser Zugriffsberechtigung nicht gewählt. Insgesamt wurde von 25 Teilnehmenden (64,1 %) die Option „Allow“, von zwei Teilnehmenden (5,1 %) die Option „Deny“ und von neun Teilnehmenden (23,1 %) die temporäre Zugriffsberechtigung „Maybe“ gewählt.

Eine Übersicht von den Häufigkeiten sowie die gesamten Anzahlen der Häufigkeiten der gewählten Option, getrennt nach der Berechtigungsart, sind in Tabelle 202 im Anhang GG wiederzufinden.

Unabhängig von den Aufgaben wurde von zwei Personen (6,5 %) nicht einmal eine angeforderte Zugriffsberechtigung akzeptiert, während von zwei Personen (6,5 %) einmal, von einer Person (3,2 %) zweimal, von zwei weiteren Personen (6,5 %) viermal und von 24 Personen (77,4 %) fünfmal zugestimmt („Allow“) wurde. Insgesamt wurde von 25 Teilnehmenden (80,6 %) die Zugriffsberechtigungen nicht einmal abgelehnt, während vier Personen (12,9 %) diese einmal, eine Person (3,2 %) diese dreimal und eine weitere Person (3,2 %) diese neunmal abgelehnt hat. Die temporäre Zugriffsberechtigung wurde von 25 Teilnehmenden (80,6 %) nicht einmal und jeweils von einer Person (3,2 %) ein-, zwei-, vier- und fünfmal gewählt. Zwei weitere Personen (6,5 %) wählten die temporäre Zugriffsberechtigung 17-mal.

Hieraus kann errechnet werden, dass von den insgesamt 213 eingeforderten Zugriffsberechtigungen 132 (62 %) akzeptiert und nur 16 (7,5 %) abgelehnt wurden. Die restlichen 65 Berechtigungen (30,5 %) wurden temporär gewährt, indem die „Maybe“-Option gewählt wurde.

Insgesamt haben von den 31 Teilnehmenden 29 (93,5 %) die Option „Allow“ und jeweils sechs Teilnehmende (19,4 %) die Option „Maybe“ und „Deny“ genutzt (s. Tabelle 203, Anhang GG). Ferner

konnte ermittelt werden, dass lediglich eine Person nach Anwendung der temporären Zugriffsberechtigung das endgültige Einverständnis durch die „Allow"- Option gewählt hat. Die fünf anderen Teilnehmenden haben sich immer wieder für die temporäre Zugriffsberechtigung entschieden, ohne das endgültige Einverständnis zu erteilen.

Nach der Auswertung der Dauer, die bei Anwenden der temporäreren Zugriffsberechtigung gewählt wurde, konnte verzeichnet werden, dass zwei Teilnehmende (6,5 %) zweimal einen Tag für die Dauer des Zugriffs und jeweils eine Person (3,2 %) den Zugriff für einen Tag siebenmal, zwölfmal, 13-mal und 16-mal erteilte. Lediglich eine Person wählte eine Dauer von drei Tagen und diese zehnmal in Folge. Eine weitere Person wählte die Dauer von sieben Tagen und dies dreimal in Folge. Somit wurde die Option von einem Tag 52-mal (80 %), die von drei Tagen zehnmal (15,38 %) und die von sieben Tagen dreimal (4,62 %) gewählt (s. Tabelle 204, Anhang GG).

Die kürzeste Dauer der erteilten Zugriffsberechtigung ist bei den Push-Benachrichtigungen mit *M* = 3,5 (*SD* = 1,73) wiederzufinden. Aufsteigend lassen sich bei den Zugriffsberechtigungen des Kalenders ein Mittelwert von 3,6 (*SD* = 2,61), des Gerätespeichers von *M* = 4,2 (*SD* = 2,78), der Kontakte von *M* = 5,2 (*SD* = 2,17) und der Positionsdaten von *M* = 6,33 (*SD* = 5,51) verzeichnen. Dabei kann lediglich bei der Dauer der Zugriffsberechtigung auf die Kontakte eine Normalverteilung gefunden werden. Die restlichen Datensätze sind entweder nicht normalverteilt oder es kann aufgrund der geringen Daten keine Verteilung berechnet werden. Insgesamt ergab sich eine durchschnittliche Dauer der erteilten temporären Zugriffsberechtigung von 4,57 Tagen (s. Tabelle 205, Anhang GG).

Über die deskriptiven Daten hinaus soll erfasst werden, ob ein Zusammenhang zwischen der Wichtigkeit des Schutzes der Privatsphäre und der insgesamten Häufigkeit beim Wählen der Option „Allow", „Maybe" und „Deny" besteht. Der Spearman-Rho-Test ergibt jedoch keine Signifikanz bei allen dreien Korrelationen (s. Tabelle 206, Anhang GG).

Insgesamt wird durchschnittlich *M* = 4,6-mal (*SD* = 1,59) „Allow", *M* = 2,1-mal (*SD* = 0,54) „Maybe" und *M* = 0,52-mal (*SD* = 1,69) „Deny" gewählt (s. Tabelle 207, Anhang GG).

In einem weiteren Schritt soll das Verhalten der Gruppe, welche angegeben hat, die temporäre Zugriffsberechtigung genutzt zu haben, mit der Gruppe verglichen werden, welche angegeben hat, diese nicht genutzt zu haben. Die erste Gruppe hat durchschnittlich *M* = 2,9-mal (*SD* = 2,28) „Allow" , *M* = 6,3-mal (*SD* = 7,42) „Maybe" und *M* = 1,2-mal (*SD* = 2,90) „Deny" gewählt, während die zweite Gruppe durchschnittlich *M* = 4,9-mal (*SD* = 0,3) „Allow", *M* = 0,1-mal (*SD* = 0,44) „Maybe" und *M* = 0,19-mal (*SD* = 0,4) „Deny" gewählt hat (s. Tabelle 208, Anhang GG). Alle Datensätze weisen hierbei die Abwesenheit einer Normalverteilung auf. Aus diesem Grund wird sich dazu entschieden den Mann-

Whitney-U-Test durchzuführen, welcher ein signifikantes Ergebnis zwischen den Gruppen bezüglich der Option „Allow“ (U = 57,5; z = -2,74; p < .043; r = 0,49) und „Maybe“ (U = 55; z = -3,06; p < .035; r = 0,55) ergibt (s. Tabelle 209, Anhang GG).

7.7 Diskussion

In dem folgenden Kapitel werden die Ergebnisse nach Hypothesen geordnet diskutiert. Hierbei wird zunächst diskutiert, ob die temporäre Zugriffsberechtigung von den Nutzenden angewendet wird. Ferner werden die Bewertung und die Erwünschtheit der temporären Zugriffsberechtigung näher betrachtet. Darüber hinaus wird in einem weiteren Kapitel das Ärgernis durch die wiederkehrende Anfrage einer Berechtigung diskutiert und abgewogen, ob die Kontrolle der Daten der Nutzenden diesen wichtiger ist als der Aufwand, den sie betreiben müssen, um nach Ablauf der temporären Zugriffsberechtigung diese erneut zu erteilen. Abschließend werden explorative Ergebnisse vorgestellt, wobei einzelne Attribute untereinander korreliert und auf Signifikanz geprüft werden.

7.7.1 Zur Hypothese 1: Diskussion über die Anwendung der temporären Zugriffsberechtigung

Hypothese 1:

Die temporäre Zugriffsberechtigung wird von den Nutzenden angewendet (Aufzeichnung der Benutzung)

In Abschnitt 7.2 wurde das Privacy Paradox erneut erwähnt, welches besagt, dass sich die Nutzenden stets für eine Applikation entscheiden würden, welche anwenderfreundlichere Datenschutzbestimmungen hat, solange keine Kompromisse in der Funktionalität und Benutzerfreundlichkeit gemacht werden müssen. Andererseits haben die Ergebnisse der zweiten Studie gezeigt, dass die Datenschutzskala durchaus genutzt wird und zu einem datenschutzfreundlichen Verhalten beigetragen hat. Aus diesem Grund wird davon ausgegangen, dass die temporäre Zugriffsberechtigung genutzt wird.

Bei dem Vergleich der insgesamten Häufigkeiten, bei der Wahl der drei Optionen „Allow“, „Maybe“ und „Deny“ werden 30,5 Prozent der Zugriffsberechtigungsanfragen mit „Maybe“, also temporär, gewährt. Darüber hinaus wird die „Maybe“ Funktion von insgesamt sechs von 31 Personen (19,4 %) genutzt, wobei jedoch insgesamt zehn Personen (32,3 %) angaben, auf die „Maybe“-Option geklickt zu haben. Hierbei könnte ebenfalls der moralische Druck einen Einfluss auf die Angaben im Fragebogen

gehabt haben, wobei die Teilnehmenden angaben, die Funktion, die bei diesem Laborversuch im Fokus steht, genutzt zu haben, obwohl es nicht der Fall war.

Die Hypothese kann somit nur teilweise bestätigt werden, weil 80,6 % der Teilnehmenden die Funktion nicht genutzt haben.

Ferner gaben von diesen zehn Personen neun Teilnehmende an, die Funktion der „Maybe“-Option richtig verstanden zu haben. Sieben Personen haben hierbei eine korrekte Erläuterung der „Maybe“-Option angegeben. Somit kann davon ausgegangen werden, dass die Mehrheit der Teilnehmenden, welche die temporäre Zugriffsberechtigung benutzten, die Funktionsweise dieser Option verstanden haben. Die Frage wurde allerdings nur den Teilnehmenden gestellt, die auch bestätigten, auf die „Maybe“-Option geklickt zu haben. Im Nachhinein wäre es ebenfalls interessant gewesen, ob die Teilnehmenden, die sich gegen den Gebrauch der temporären Zugriffsberechtigung entschieden haben, die Funktionsweise dieser richtig verstanden haben.

Hierbei ist jedoch zu berücksichtigen, dass die Teilnehmenden keine weitere Erläuterung zu der Funktion der temporären Zugriffsberechtigung erhalten haben und sie trotzdem von ca. einem Fünftel genutzt wird. Darüber hinaus ist zu erwähnen, dass lediglich eine Person nach wiederholter Anwendung der temporären Zugriffsberechtigung in die Berechtigungsanfrage endgültig mit „Allow“ eingewilligt hat. Die anderen Teilnehmenden haben die temporäre Zugriffsberechtigung durchgängig benutzt und sich dagegen entscheiden, eine permanente Einwilligung für den Zugriff zu erteilen. Die temporäre Zugriffsberechtigung wird überwiegend (zu 80 %) für einen Tag vergeben. Dieses Phänomen kann einerseits aufgrund der Standardeinstellung der temporären Zugriffsberechtigung, welche auf einen Tag eingestellt war, auftreten, andererseits könnte dieses Verhalten auch den Wunsch der Teilnehmenden widerspiegeln, die Berechtigung nur für eine kurze Zeitspanne freigeben zu wollen.

Werden die einzelnen Typen der Zugriffsanfrage untereinander verglichen, so fällt auf, dass die temporäre Zugriffsberechtigung am häufigsten beim Gerätespeicher und den Kontakten verwendet wird. Deshalb ist davon auszugehen, dass die temporäre Zugriffsberechtigung besonders in diesen beiden Kategorien Anwendung finden könnte. Diese Ergebnisse widersprechen jedoch teilweise der Aussage, welche aus den Ergebnissen der dritten Frage des Fragebogens zu entnehmen ist. Dort wird mit über 80 % angegeben, dass die Anwendung der temporäre Zugriffsberechtigung am meisten bei den Standortdaten erwünscht ist. Dieses Verhalten ist damit zu erklären, dass die Teilnehmenden einem gewissen moralischen Druck unterliegen, die gestellten Aufgaben zu erfüllen und deshalb bei den Zugriffsanfragen, denen sie im Alltag nicht stattgeben würden, innerhalb dieses Versuches eine temporäre Berechtigung erteilt haben. Ferner ist davon auszugehen, dass die Teilnehmenden sich der Problematik, die schon in Abschnitt 7.1 erläutert wurde, bewusst sind, dass die einmalige temporäre

Zugriffsberechtigung auf z.B. Kontakte oder den Speicher bereits die komplette Weitergabe der Daten ermöglicht, während eine zeitliche Begrenzung der Freigabe von Positionsdaten nur einen auf die Dauer der Freigabe der Daten bezogenen Ausschnitt der Daten zur Verfügung stellt. Eine weitere Erläuterung für dieses Verhalten ist die Häufigkeit und der Zeitpunkt, an dem die Berechtigung abgefragt wird. Aufgrund der Tatsache, dass die Teilnehmenden die lokalen Nachrichten täglich und somit auch am Anfang und am Ende des Experimentes abrufen sollten und dafür die Berechtigung auf den Zugriff der Standortdaten eingeholt wurde, könnte es sein, dass der Primacy und Recency Effekt, wie er in der Studie von Steiner und Rain (1989) beschrieben wird, Auswirkungen auf das Gedächtnis der Teilnehmenden hat. Dabei könnte davon ausgegangen werden, dass bezüglich der Gedächtnisleistung eine sogenannte „Badewannenkurve“ vorliegt, in der die Berechtigungen zu Beginn und zum Ende am besten erinnert werden, wobei die Berechtigungen, welche eher in der Mitte des Experiments abgefragt wurden, in Vergessenheit geraten. Somit könnte es sein, dass die gewünschte Anwendung der temporären Zugriffsberechtigung mit der eigentlichen Nutzung dieser nicht übereinstimmt.

7.7.2 Zur Hypothese 2: Diskussion über die Bewertung der temporären Zugriffsberechtigung

Hypothese 2:

Die temporäre Zugriffsberechtigung wird hinsichtlich ihrer Funktionsweise von den Nutzenden positiv bewertet.

Im zweiten Versuch wird den persönlichen Daten ein hoher Wert zugeschrieben (siehe Abschnitt 5.7.7 und 5.8.2), weshalb davon ausgegangen wird, dass die meisten Nutzenden eine weitere Funktion zum Schutz ihrer persönlichen Daten positiv bewerten.

Aus der fünften Aussage der ersten Frage ist zu entnehmen, dass die temporäre Zugriffsberechtigung durchschnittlich mit einem Wert von 5,87 auf der Skala eher gefallen hat. Beim Teilen der Stichprobe in zwei Gruppen resultiert jedoch, dass eine knappe Mehrheit die temporäre Zugriffsberechtigung nicht mag. Hierbei ist jedoch zu beachten, dass über ein Drittel der Stichprobe die Aussage mit einer „5“ bewertet hat. Lediglich vier Teilnehmende (12,9 %) widersprachen dieser Aussage mit einem niedrigeren Wert auf der Skala von 1 bis 10. Aufgrund des großen Anteils der Teilnehmenden, welche die Aussage mit einer „5“ bewertet haben, also knapp an der Schwelle zur Zustimmung waren, wäre hier zu überlegen, ob diesem leichten Missfallen durch eine vorherige Erläuterung, wie diese z.B. im zweiten Versuch in Gruppe A präsentiert wurde, entgegenzuwirken wäre.

Ferner geht aus der zehnten Frage hervor, dass knapp zwei Drittel die vorgegebene Dauer der temporären Zugriffsberechtigung als adäquat bewertet haben. Nur zwei Teilnehmende wünschen sich eine kürzere und vier Teilnehmende eine längere Zeitspanne. Vier weitere Teilnehmende bestätigen den Wunsch nach der Auswahl von mehr Zeitspannen. Auf diese Anregungen könnte eingegangen werden, indem den Verbesserungsvorschlägen aus Frage vier Folge geleistet wird. Dort gaben über 16 % der Teilnehmenden an, sich eine Option zu wünschen, bei der eine beliebige Zeit für die temporäre Zugriffsfreigabe angegeben werden kann. So könnte die Implementierung dieser variablen Zeitangabe das Gefallen dieser Funktion eventuell noch etwas steigern. Es ist jedoch zu betonen, dass die meisten Teilnehmenden mit dem Zeitintervall der Zugriffberechtigung zufrieden sind und den vorgegebenen negativen Aussagen meist zu etwa 90 % widersprechen. Darüber hinaus ist zu vermerken, dass vier Fünftel der Teilnehmenden die Zugriffsberechtigung überwiegend bei der Zugriffsberechtigung der Positionsdaten benutzen würden.

Auf Grundlage der vorliegenden Ergebnisse ist es in diesem Fall schwer zu beurteilen, ob die Hypothese weiterhin aufrechterhalten werden kann. Die Angaben der Teilnehmenden lassen weder auf eine eindeutige Ablehnung noch Annahme der temporären Zugriffsberechtigung schließen. Es besteht jedoch die Möglichkeit, dass wenn diese Funktion bei der Hälfte der Stichprobe Gefallen findet, die Anwendung der temporären Zugriffsberechtigung nach einer vorherigen Erläuterung von etwa 50 % auf 90 % gesteigert werden könnte.

7.7.3 Zur Hypothese 3: Diskussion über die Erwünschtheit der temporären Zugriffsberechtigung

Hypothese 3:

Die Funktion der temporären Zugriffsberechtigung wird von den Nutzenden im Alltag erwünscht.

Nach der Studie von Custers (2016) ist eine erneute Einforderung des Einverständnisses nach einiger Zeit sinnvoll und zeitgemäß. Hierbei verdeutlicht Custers das Interesse der Endnutzenden, die persönlichen Daten schützen zu wollen. Deshalb wird davon ausgegangen, dass eine weitere Funktion zum Schutz der Daten auf dem Endgerät der Nutzenden erwünscht ist.

Wie schon im vorherigen Abschnitt erwähnt, würden vier Fünftel der Teilnehmenden die Funktion der temporären Zugriffsberechtigung bei den Positionsdaten nutzen, während bei allen anderen Berechtigungen der Gebrauch der temporären Zugriffsberechtigung eher abgelehnt wird.

Dies könnte wiederum mit der Problematik zusammenhängen, welche bereits in der Diskussion der ersten Hypothese (Abschnitt 7.7.1) besprochen wurde. Die Problematik betrifft das einmalige Aushändigen von Daten und Kontakten für eine vollständige Erfassung dieser Daten. Ein wiederholter Zugriff auf diese Daten führt nach einer kurzen Zeitspanne meist nicht zu einem Gewinn neuer Daten.

Anders verhält es sich bei den Positionsdaten, bei denen bei dauerhaftem Zugriff ein Bewegungsprofil erstellt werden kann und es Zeitpunkte gibt, an denen es nicht gewollt ist, dass Dritte die aktuelle Position der Endnutzenden orten können. Dies könnte auch der Grund dafür sein, weshalb die Teilnehmenden bei allen anderen Berechtigungen eher dazu neigen, die temporäre Zugriffsberechtigung nicht anwenden zu wollen. Verwunderlich ist jedoch, dass die höchsten Prozentsätze neben den Positionsdaten bezüglich der potenziellen Anwendung bei den Berechtigungen auf den Zugriff der SMS-Nachrichten und des Kalenders wiederzufinden sind, obwohl während der Studie die Optionen der temporären Zugriffsberechtigung am meisten bei dem Gerätespeicher und den Kontakten mit jeweils über 40 % von fünf Teilnehmenden genutzt wurden.

Die große Erwünschtheit der temporären Zugriffsberechtigung bei den Berechtigungen auf die SMS-Nachrichten und den Kalender könnte mit einem gewissen Grad der Privatsphäre zusammenhängen. Bei Einsicht in die Nachrichten oder den Kalender könnte ein Dritter nachverfolgen, wann die Endnutzenden welche Tätigkeit ausführen. Die Diskrepanz zwischen der Erwünschtheit und der Nutzung der temporären Zugriffsberechtigung ist einerseits damit zu erklären, dass innerhalb der Studie keine Berechtigung auf den Zugriff der SMS-Nachrichten stattgefunden hat, weshalb die eigentliche Nutzung bei dieser Berechtigung nicht festgehalten werden konnte. Andererseits könnte hier wiederum der Recency und Primacy Effekt, welcher bereits in Abschnitt 7.7.1 erläutert wurde, dazu führen, dass einige Berechtigungen besser erinnert werden als andere. Der wichtigste Punkt, der jedoch berücksichtigt werden muss, ist, dass die Berechtigungsanfrage nach dem Zugriff auf den Kalender nur zweimal stattgefunden hat, während die auf den Kontakten fünfmal und den Speicher viermal stattgefunden hat.

Ferner geht aus der zweiten Aussage der ersten Frage hervor, dass über 45 % der Teilnehmenden die temporäre Zugriffsberechtigung auf ihrem privaten Endgerät nutzen würden. Auch hier ist eine ähnliche Verteilung wie bei dem Gefallen der temporären Zugriffsberechtigung in Hypothese 2 wiederzufinden, sodass über 22 % der Teilnehmenden diese Aussage mit einer 5 bewertet haben und wiederum sich somit knapp gegen den privaten Gebrauch entschieden haben. Insgesamt ist jedoch ein Durchschnitt von 5,35 auf einer Skala von 1 bis 10 zu beobachten, sodass eine leichte Zustimmung bezüglich des privaten Gebrauches erfasst werden kann.

Wird nun die Verwendung der temporären Zugriffsberechtigung von 19,4 % der Teilnehmenden mit dem Anteil von 45 %, die nach dem Experiment die temporäre Zugriffsberechtigung auf ihrem privaten Endgerät nutzen würden, verglichen, so fällt auf, dass durch das Hervorheben der Funktion eine Steigerung der Nutzenden auf mehr als das Doppelte erfolgen könnte.

Bei der Betrachtung der Ergebnisse kann auch diese Hypothese nur teilweise aufrechterhalten werden, weil lediglich knapp die Hälfte der Teilnehmenden angab, die temporäre Zugriffsberechtigung auf ihrem privaten Gerät im Alltag nutzen zu wollen.

7.7.4 Zur Hypothese 4: Diskussion über das Ärgernis durch die wiederkehrende Anfrage einer Berechtigung

Hypothese 4:

Die Nutzenden empfinden durch die wiederkehrende Anfrage einer Berechtigung Ärgernis.

Aus den Ergebnissen der dritten Aussage der ersten Frage geht hervor, dass über zwei Drittel der Teilnehmenden die wiederkehrende Anfrage für die Zugriffsberechtigung als nicht störend empfinden. Auch durchschnittlich wird ein Mittelwert von 4,3 auf einer Skala von 1 bis 10 erreicht, welcher bestätigt, dass die Mehrheit der Teilnehmenden der Aussage, dass die immer wiederkehrende Anforderung, die Zustimmung zu erteilen, sie verärgert hätten, widersprochen haben. Ein weiteres Indiz dafür, dass die temporäre Zugriffsberechtigung als nicht störend empfunden wird, ist die wiederholte Anwendung der Option bei fast allen Teilnehmenden, welche die temporäre Zugriffsberechtigung genutzt haben. Wie schon in Abschnitt 7.7.1 zu Hypothese 1 erwähnt, hat lediglich eine Person nach Anwendung der temporären Zugriffsberechtigung die Berechtigung anschließend endgültig erteilt. Somit kann davon ausgegangen werden, dass zumindest bei den Teilnehmenden, welche die temporäre Zugriffsberechtigung genutzt haben, das wiederholte Erscheinen der Berechtigungsanfrage kein Ärgernis hervorgerufen hat.

Aus diesem Grund kann die vierte Hypothese nicht aufrechterhalten werden.

7.7.5 Zur Hypothese 5: Diskussion über die Abwägung zwischen der Kontrolle der Daten und dem wiederkehrenden Anfragen für die Berechtigung

Hypothese 5:

Die Nutzenden bevorzugen die Kontrolle über ihre Daten trotz der wiederkehrenden Anfrage für die Berechtigungen.

Die nähere Betrachtung der Ergebnisse der vierten Aussage der ersten Frage ergibt, dass knapp neun Zehnteln der Teilnehmenden die Kontrolle ihrer Daten wichtig ist. Insgesamt wird ein Mittelwert von 8,19 (SD = 1,94) erreicht. Somit kann der Schluss gezogen werden, dass den Teilnehmenden die Kontrolle ihrer Daten durchaus wichtig ist. Wird diese Erkenntnis nun mit den Beobachtungen aus Hypothese 4, dass die wiederkehrenden Anfragen der temporären Zugriffsberechtigung kein Ärgernis hervorrufen, und mit Hypothese 3, dass die Funktion der temporären Zugriffsberechtigung erwünscht ist, verbunden, so könnte darauf geschlossen werden, dass die Nutzenden die Kontrolle über ihre Daten trotz der wiederkehrenden Anfrage für die Zugriffsberechtigung bevorzugen. Mit Hilfe der 16. Frage aus dem Fragebogen kann ermittelt werden, dass der Schutz der Privatsphäre auf einer Skala von 1 bis 7 bei einem Mittelwert von 5,97 (SD = 0,91) liegt. Somit ist davon auszugehen, dass der Schutz der Privatsphäre einen hohen Stellenwert bei den Teilnehmenden einnimmt. Darüber hinaus bestätigt die fünfte Aussage der ersten Frage, dass mehr als zwei Drittel der Teilnehmenden der Aussage widersprechen, dass die Benutzerfreundlichkeit wichtiger sei als die Kontrolle ihrer Daten. Dies bestätigt der Mittelwert, welcher bei dieser Aussage lediglich bei 4,0 (SD = 2,70) liegt. Somit kann davon ausgegangen werden, dass die Teilnehmenden die Kontrolle über ihre Daten trotz der wiederkehrenden Anfrage für die Zugriffsberechtigung bevorzugen und somit kann die fünfte Hypothese aufrechterhalten werden.

7.7.6 Diskussion der explorativen Ergebnisse

In einem weiteren Schritt soll untersucht werden, ob das Auffallen der temporären Zugriffsberechtigung bzw. der Schaltfläche „Maybe“ mit der Wichtigkeit der Kontrolle der Daten korreliert. Diese Vermutung bestätigt sich mit einer Signifikanz mittlerer Effektstärke. Hierbei könnte angenommen werden, dass die Teilnehmenden, denen die Kontrolle ihrer persönlichen Daten wichtig ist, eher auf Einstellungen achten, welche den Schutz ihrer persönlichen Daten steigern können. Deshalb ist davon auszugehen, dass bei jenen Teilnehmenden die Wahrscheinlichkeit größer ist, neue Funktionen wie beispielsweise die temporäre Zugriffsberechtigung zu nutzen.

Beim Korrelieren der Wichtigkeit des Schutzes der Privatsphäre mit den Aussagen der ersten Frage ergibt sich lediglich ein signifikantes Ergebnis mit einer großen Effektstärke bezüglich der Wichtigkeit der Kontrolle der persönlichen Daten. Aus diesem Zusammenhang kann vermutet werden, dass die Teilnehmenden den Fragebogen mit Bedacht ausgefüllt haben, sodass die Personen, denen der Schutz ihrer persönlichen Daten wichtig ist, auch viel Wert auf die Kontrolle ihrer persönlichen Daten legen.

Ferner ergibt sich bei der Korrelation zwischen den Aussagen der ersten Frage mit der von den Teilnehmenden ausgewählten Dauer der Zugriffsberechtigung und der Wichtigkeit der Kontrolle der persönlichen Daten ein negativer und signifikanten Zusammenhang. Somit kann davon ausgegangen werden, dass die Personen, denen die Kontrolle ihrer persönlichen Daten wichtig ist, eine kürzere Dauer bei der Vergabe der temporären Zugriffsberechtigung wählen.

Die Korrelation zwischen der technischen Affinität und der Aussagen der ersten Frage ergibt lediglich einen Zusammenhang mit dem Ärgernis über die wiederkehrende Berechtigungsanfrage. Dabei ist davon auszugehen, dass bei denen Personen, welche angaben, eine hohe Affinität zur Technik zu haben, eher ein Ärgernis über die wiederkehrenden Berechtigungsanfragen hervorgerufen wird als bei denen, die angaben, eine niedrigere Affinität zu Technik zu haben. Dies könnte damit zusammenhängen, dass die Person mit einer höheren Affinität zur Technik öfter und länger mit ihrem mobilen Endgerät arbeiten und somit häufiger die temporäre Zugriffsberechtigung angezeigt bekommen.

Beim Korrelieren des Alters und der täglichen Dauer der Nutzung des mobilen Endgeräts seitens der Teilnehmenden mit den Aussagen der ersten Frage ergeben sich keine signifikanten Zusammenhänge, aus diesem Grund kann angenommen werden, dass sowohl die Smartphone Nutzung sowie auch das Alter keinen Einfluss auf das Mögen und Nutzen der temporären Zugriffsberechtigung haben. Es konnte lediglich ein negativer Zusammenhang mit einem kleinen Effekt zwischen der Nutzung des Smartphones und der Wichtigkeit der Kontrolle der Daten gefunden werden, der jedoch nicht signifikant ist. Hierbei besteht die Vermutung, dass der Effekt eher klein ausgefallen ist, weil die Teilnahme an dem Experiment gewisse Kenntnisse im Bereich der mobilen Endgeräte voraussetzt. So mussten die Teilnehmenden vor Beginn der Studie einige Dokumente einscannen und per Mail versenden, sowie auf Textnachrichten antworten (siehe Abschnitt 7.4.1, 7.4.2 und 7.4.5). Deshalb ist davon auszugehen, dass die Teilnehmenden, welche über diese Kenntnisse verfügen auch eine gewisse Zeit mit der Bedienung ihres mobilen Endgerätes aufwenden. Allerdings konnte beim Korrelieren der technischen Affinität mit der täglichen Dauer der Nutzung des Mobiltelefons kein Zusammenhang festgestellt werden, weshalb die eben genannte Vermutung wieder verworfen werden muss.

Bei näherer Betrachtung der Mittelwerte zwischen der Gruppe, welche angab, die temporäre Zugriffsberechtigung genutzt zu haben und der, die angab, diese nicht genutzt zu haben, ist zu sehen, dass deutlich weniger Teilnehmende der erstgenannten Gruppe die Berechtigung akzeptiert haben als die Teilnehmenden der Gruppe, die angab, die „Maybe“-Option nicht genutzt zu haben.

Die Mittelwerte der Wahl der „Maybe“-Option stimmen mit den Angaben seitens der Teilnehmenden überein. Dabei liegt der Mittelwert der Gruppe, die angegeben hat, die „Maybe“-Option genutzt zu haben, bei M = 6,3, während der Mittelwert der Gruppe, die angegeben hat, die „Maybe“-Option nicht genutzt zu haben bei *M* = 0,1 liegt, was wahrscheinlich auf das versehentliche Tippen auf die Schaltfläche der „Maybe“-Option zurückzuführen ist.

Bezüglich des Ablehnens der Berechtigung ist der höhere Mittelwert in der Gruppe wiederzufinden, welche die temporäre Zugriffsberechtigung genutzt hat.

Beim Betrachten der eben genannten Ergebnisse liegt die Vermutung nah, dass die Teilnehmenden, die angegeben haben, die temporäre Zugriffsberechtigung genutzt zu haben, generell kritischer bezüglich der Erteilung von Berechtigungen waren. Diese kritische Haltung könnte zur Folge haben die Berechtigung seltener endgültig zu erteilen („Allow“ zu wählen) und häufiger die Berechtigung zu verweigern („Decline“ zu wählen).

Durch den moralischen Druck die Aufgaben zu erfüllen, welche im Rahmen der teilgenommenen Studie gestellt wurden, könnten sich die Teilnehmenden dazu entschlossen haben, einen Kompromiss zwischen dem Verlangen die Berechtigung zu verweigern und dem Wunsch zur Teilnahme der Studie bzw. zum Erhalt der finanziellen Gegenleistung zu wählen. In diesem Fall wäre der Kompromiss die temporäre Zugriffsberechtigung. Diese Vermutung wird ebenfalls mit Hilfe eines Signifikanztestes bestätigt, bei dem sich die Mittelwerte zwischen den Gruppen der Teilnehmenden, welche die temporäre Zugriffsberechtigung benutzt bzw. nicht benutzt haben signifikant bezüglich des Akzeptierens („Allow“) und bezüglich der „Maybe“-Option abweichen.

Lediglich bei der Auswahl des Ablehnens der Berechtigung („Decline“) kann kein signifikanter Unterschied zwischen den Gruppen festgestellt werden, vermutlich weil beide Gruppen, wie bereits erwähnt, befürchtet haben durch das Ablehnen der Berechtigung und dem damit verbundenen Versäumnis der Aufgabe aus der Studie ausgeschlossen zu werden. Diese Situation lässt sich in den Alltag übertragen, indem davon ausgegangen wird, dass eine Person eine gewisse Aufgabe mit Hilfe einer Applikation erfüllen möchte. Um diese zu erfüllen, ist die Person gezwungen meist alle von der Applikation angeforderten Berechtigungen zu akzeptieren. Aus den eben diskutierten Ergebnissen lässt sich schließen, dass Endnutzende, die Wert auf den Schutz ihrer Privatsphäre und die Kontrolle

ihrer persönlichen Daten legen, die temporäre Zugriffsberechtigung nutzen würden, um einen Kompromiss zwischen dem Nutzen der Applikation und dem Erteilen endgültiger Zugriffsberechtigungen einzugehen.

7.8 Probleme und Ausblick

Während der Durchführung der Studie, bei der die Teilnehmenden nicht vor Ort erscheinen konnten, ergab sich das Problem, den Teilnehmenden die Einverständniserklärung und den persönlichen Code zukommen zu lassen. Es bedurfte einiger Erinnerungs-E-Mails, um überhaupt einen Teil der potenziellen Stichprobe dazu zu bewegen, die erforderten Dokumente zu übersenden. Darüber hinaus ergaben sich technische Schwierigkeiten beim Versenden von langen SMS-Nachrichten, die verwendet wurden, um den Teilnehmenden erste Instruktionen und Aufgabenstellungen zu übermitteln. Ab einer bestimmten Länge von über 450 Zeichen wurde die Nachricht in eine kostenpflichtige MMS umgewandelt. Aus diesem Grund mussten die Nachrichten kürzer formuliert werden oder aufgeteilt versendet werden. Ferner verfügt das Android-Betriebssystem über einen Schutz, der es unterbindet, eine große Menge an SMS-Nachrichten zu versenden. Deshalb musste jede SMS-Nachricht einzeln bestätigt werden.

Eine weitere Störvariable könnte die Positionierung der „Maybe“-Schaltfläche sein, welche eher auf der Seite des Ablehnens war und Auswirkung auf die Entscheidung der Teilnehmenden haben könnte. Dabei wäre es denkbar, dass die Nutzenden durch die Positionierung dazu verleitet wurden, anzunehmen, dass die „Maybe“-Option ebenfalls eine Form des Ablehnens ist und sie die Applikation anschließend nicht nutzen werden können bzw. die Aufgabe nicht erfüllen können. Diesem Problem könnte entgegengewirkt werden, indem bei der Einführung dieser Option eine kurze Erläuterung über deren Funktion mit Hilfe eines Dialogfensters präsentiert würde.

Ferner ist es fraglich, ob der Name „Maybe“ auf der Schaltfläche der temporären Zugriffsberechtigung angemessen ist und bei den Nutzenden als die Funktion wahrgenommen wird, die es ist oder ob es nicht besser gewesen wäre, die Schaltfläche mit den Wörtern „temporär“ oder „temporary“ zu versehen.

Allerdings konnte aus der ersten Frage des Fragebogens entnommen werden, dass die Mehrheit der Teilnehmenden, die die temporäre Zugriffsberechtigung benutzt haben, diese auch verstanden haben. Leider wurde die Frage nicht allen Teilnehmenden gestellt, sodass nicht in Erfahrung gebracht werden konnte, ob die Funktion der „Maybe“-Option bei der Mehrheit der Teilnehmenden richtig interpretiert worden ist.

Eine weitere Störvariable, die dazu geführt haben könnte, dass die Teilnehmenden sich während der Studie nicht wie im alltäglichen Umgang mit ihrem mobilen Endgerät verhalten haben, war die Tatsache, dass ihnen bewusst war, dass das Experiment nach zehn Tagen endete und sie anschließend die Applikationen von ihren Mobiltelefonen deinstallieren konnten. Somit wäre es denkbar, dass eine gewisse Gleichgültigkeit bei der Auswahl der Erteilung der Zugriffsberechtigung mit einfloss.

Ferner beeinflusst auch der subjektive Nutzen der Applikation den Umgang mit den Zugriffsberechtigungen. Somit ist denkbar, dass die Teilnehmenden bei einer Applikation, die sie täglich gebrauchen, um Nachrichten zu versenden, auch freizügiger bezüglich der Erteilung von Zugriffsberechtigungen entscheiden als bei einer Applikation, von der sie nur einen geringen Nutzen ziehen, wie z.B. eine Taschenlampenapplikation. Auch der Nutzen einer Nachrichtenapplikation ist hierbei fraglich, weil bereits aus der zweiten Studie hervorging, dass die meisten Nutzenden Nachrichten in ihrem Internetbrowser öffnen und keine separate Applikation dafür herunterladen.

Die temporäre Zugriffsberechtigung an sich ist eine weitere Möglichkeit für die Endnutzenden eine gewisse Kontrolle über ihre privaten Daten zu erlangen. Allerdings sollten die Endnutzenden in der Lage sein zu überprüfen wie häufig eine Applikation welche Daten übermittelt. In dem wissenschaftlichen Artikel von Momen et al. (2020) wird darüber diskutiert den Endnutzenden eine temporäre Zugriffsberechtigung anzubieten. Während dieser Zeit soll es ihnen ermöglicht werden Einblick in die Art und Häufigkeit der weitergegebenen Daten zu erhalten, sodass sie sich während der temporären Zugriffsberechtigung ein Bild von der Applikation machen können. Nach dieser Zeitspanne sollen die Endnutzenden im Stande sein auf Grundlage der ihnen dargebotenen Übersicht von Art und Häufigkeit der weitergegebenen Daten zu entscheiden, ob sie die Applikation weiterhin nutzen möchten oder eine weitere Applikation mit ähnlicher Funktion wählen.

7.9 Fazit

Das Ziel dieser Studie ist die Erfassung der Akzeptanz und Verwendung einer temporären Zugriffsberechtigung. Hierfür wird bei dem Dialogfenster zur Erteilung der Berechtigungen neben der „Allow“- und „Deny“-Option, welche eine endgültige Annahme oder Ablehnung der angefragten Berechtigung erteilt, eine zusätzliche „Maybe“-Option implementiert. Diese ermöglicht es den Nutzenden, die Berechtigung temporär für 1, 3 oder 7 Tage, je nach eingestellter Dauer, zu erteilen. Anschließend erfolgt eine erneute Berechtigungsanfrage. Diese temporäre Zugriffsberechtigung wurde in einer Nachrichtenapplikation implementiert. Mit Hilfe von SMS und E-Mail-Nachrichten wurden den Teilnehmenden der Studie über einen Zeitraum von zehn Tagen täglich zwei bis drei

Aufgaben gestellt. Bei dem Erfüllen der Aufgaben wurden den Teilnehmenden Berechtigungsanfragen, z.B. auf dem Speicher des Endgerätes, gestellt, um eine Nachricht auf dem Endgerät zu speichern. Diese Berechtigungsanfragen waren jedoch nur vorgetäuscht, sodass auf die Daten der Teilnehmenden nicht zugegriffen wurde. Die Applikation übermittelte lediglich, bei welcher Berechtigung welche gewählte Option („Allow“, „Maybe“, „Deny“) zu welchem Zeitpunkt gewählt wurde.

Die wichtigsten Erkenntnisse aus den gesammelten Daten und der statistischen Analyse dieser Studie sind folgende:

a. Die temporäre Zugriffsberechtigung wird lediglich von einem Fünftel der Teilnehmenden angewandt.

b. Nahezu alle Teilnehmenden, welche die temporäre Zugriffsberechtigung genutzt haben, haben auch deren Funktion richtig verstanden.

c. Bei Anwendung der temporären Zugriffsberechtigung wird diese nach Ablauf der ausgewählten Zeitspanne wiederholt gewählt, sodass meistens keine endgültige Einwilligung in die Berechtigung stattfindet.

d. Die temporäre Zugriffsberechtigung wird überwiegend für eine Zeitspanne von einem Tag vergeben.

e. Am häufigsten wird die temporäre Zugriffsberechtigung für Zugriffe auf den Gerätespeicher und auf die Kontakte genutzt.

f. Aus den Fragebögen geht hervor, dass die temporäre Zugriffsberechtigung am meisten bei den Standortdaten erwünscht ist.

g. Die knappe Mehrheit der Teilnehmenden gibt an, keinen Gefallen an der temporären Zugriffsberechtigung zu haben, wobei jedoch mit Hilfe einer vorherigen Erläuterung der Funktion eine höhere Akzeptanz erzielt werden könnte.

h. Die Mehrheit der Teilnehmenden ist mit der vorgegebenen Zeitspanne der temporären Zugriffsberechtigung zufrieden, nur vereinzelnd wird sich eine variable selberdefinierte Zeitspanne gewünscht.

i. Knapp die Hälfte der Teilnehmenden gibt nach Ausfüllung des Fragebogens an, die temporäre Zugriffsberechtigung auf ihrem privaten Endgerät nutzen zu wollen.

j. Die wiederkehrende Anfrage einer Berechtigung hat bei den meisten Teilnehmenden keine Ärgernis hervorgerufen.

k. Die meisten Teilnehmenden bevorzugen die Kontrolle ihre Daten trotz der wiederkehrenden Anfragen der Zugriffsberechtigung.

l. Teilnehmende, die angeben, dass ihnen die Kontrolle ihre persönlichen Daten wichtig sei, wählen eine kürzere Dauer bei der Vergabe der temporären Zugriffsberechtigung.

8 Versuchsübergreifendes Fazit

Die Digitalisierung ist auch während der Verfassung dieser Dissertation weit vorangeschritten. Alleine im Jahr 2019 wurden knapp 147 Millionen Smart Speaker, also Lautsprecher mit Sprach Assistent vertrieben, welche die Möglichkeit haben, dauerhaft Gespräche und andere Geräusche aufzuzeichnen (Tenzer, 2020b). In Deutschland steigerte sich die Anzahl der Smartphone-Nutzenden von 45,6 Millionen im Jahre 2015 auf 57,7 Millionen im Jahr 2019 um 26,5 % (Tenzer, 2020a). Doch auch in dem Bereich der Automobilität ist der Fortschritt der Digitalisierung offensichtlich. Allein in Europa steigerte sich das Marktvolumen der ConnectedCars von 1,2 auf 2,5 Milliarden US-Dollar, wobei eine Steigerung auf 8,2 Milliarden im Jahre 2025 und 14 Milliarden im Jahre 2030 prognostiziert wird (Kords, 2019). Somit werden immer mehr persönliche Daten von den Konsumenten gesammelt, abgespeichert und gegebenenfalls an Dritte ausgehändigt. Andererseits kommt es immer häufiger zu Datenmissbräuchen wie z.B. dem Datenskandal von Facebook und Cambridge Analytica, die bis zu 87 Millionen Konten von Nutzenden auswerteten, um durch individuell zugeschnittene Botschaften das Wahlverhalten zu beeinflussen (Rosenberg, 2018). Darüber hinaus hat Facebook mit mehr als 150 Firmen Datenvereinbarungen abgeschlossen, durch die beispielsweise Spotify und Netflix private Daten und Nachrichten von den Facebook-Konten der Nutzenden einsehen konnten, ohne dass eine Einwilligung eingeholt wurde (Dance et al., 2018). Sowohl das Ausmaß der Erfassung persönlicher Daten von Konsumenten als auch der Umgang mit diesen Daten zeigen die Dringlichkeit eines umfangreichen Datenschutzes, der am besten direkt bei den Konsumenten beginnen sollte. Aus diesen Gründen ist das Ziel dieser Dissertation zunächst den Umgang der Endnutzenden mobiler Endgeräte mit ihren persönlichen Daten zu erfassen, um anschließend Methoden zu entwickeln, die es den Endnutzenden ermöglichen Kontrolle über ihre privaten Daten zu erlangen.

Hierfür wurde zunächst eine Studie durchgeführt, welche untersuchen sollte, ob und mit welcher Gründlichkeit die AGBs durchgelesen werden und wie freizügig die Teilnehmenden mit ihren persönlichen Daten umgehen. Ferner sollte untersucht werden, ob die Präsentationsform, digital als Dialogfenster oder ausgedruckt als Papierform, einen Einfluss auf das Verhalten der Endnutzenden hat. Hierfür wurde ein Täuschungsexperiment durchgeführt, in welchem die Teilnehmenden in dem Glauben gelassen wurden, dass es sich um einen Persönlichkeitstest handele. Zunächst wurden die Teilnehmenden in zwei Stichproben geteilt, wobei die eine Stichprobe die Teilnahmevereinbarung für das Experiment in schriftlicher Form und die andere Gruppe diese in digitaler Form präsentiert bekommen hat. Hierbei wurde gemessen, wie viel Zeit in das Lesen der Vereinbarung investiert wurde. Anschließend wurden allen Teilnehmenden Begriffspaare präsentiert, wobei der favorisierte Begriff gewählt werden sollte. Daraufhin konnten die Teilnehmenden entscheiden, an welche Institutionen

ihre Daten weitergegeben werden sollten. Mit der Anzahl der Institutionen stieg auch die finanzielle Gegenleistung.

Aus den Ergebnissen der Studie lässt sich aufzeigen, dass der Großteil der Teilnehmenden nicht genügend Zeit für das vollständige Lesen der Teilnahmevereinbarung aufwand, jedoch etwas weniger als die Hälfte der Teilnehmenden angab, die Vereinbarung vollständig gelesen zu haben. Ein Grund für dieses Phänomen könnte die Lesedauer sein, welche von den Teilnehmenden deutlich länger eingeschätzt wurde, als sie wirklich war. Somit kann davon ausgegangen werden, dass die Teilnehmenden zwar der Überzeugung sind in Kenntnis über den Inhalt der Vereinbarung zu sein, was jedoch nicht der Wahrheit entspricht. Dies könnte auch begründen, weshalb die Teilnehmenden sich weniger über die langfristigen Konsequenzen bei der Weitergabe ihrer persönlichen Daten bewusst sind, obwohl sie diesen einen hohen Stellenwert zuschreiben.

Ferner waren die Teilnehmenden bereit für eine geringe finanzielle Gegenleistung ihre Daten an sämtliche Institutionen und Unternehmen auszuhändigen, obwohl sie diesen einen hohen monetären Wert zugeschrieben haben. Die Präsentationsform der Teilnahmevereinbarung hatte keinen Einfluss auf den Umgang mit der Einverständniserklärung, in welche meistens ohne Zögern eingewilligt wurde.

Als hauptsächliche Ursache für das Unterlassen, des Lesens der Teilnahmevereinbarung gaben die Teilnehmenden an, dass sie diese als „zu lang“ und „zu zeitaufwendig“ erachten und für die Nutzung des Produktes ohnehin ein Einverständnis erfolgen muss. Aus diesem Grund wurden in der zweiten Studie Methoden entwickelt und untersucht, die es ermöglichen eine einfache und selbsterklärende Form der Weitergabe von persönlichen Daten darzustellen. In der dritten Studie wurde eine temporäre Zugriffsberechtigung entwickelt und evaluiert, welche es den Endnutzenden ermöglicht die Berechtigungen zeitlich begrenzt zu erteilen.

Das Ziel der zweiten Studie war es den Endnutzenden einen möglichst intuitiven Überblick von dem Zugriff und der Weitergabe persönlicher Daten durch Applikationen auf dem mobilen Endgerät zu schaffen. Hierfür wurden verschiedene Datenschutzskalen entwickelt und in einer Onlinevorstudie bewertet. Dabei wurde eine fünfstufige farbkodierte Skala mit zusätzlicher Beschriftung favorisiert, welche anzeigen sollte wie häufig Applikationen, die im Hintergrund laufen auf die Daten der Nutzenden zugreifen. Die Skala wurde anschließend in einem App-Markt implementiert, wobei 80 Applikationen in unterschiedlichen Kategorien von „sehr sicher“ bis „sehr kritisch“ eingeordnet wurden. Anschließend wurden die Teilnehmenden der Studie gebeten, verschiedene Aufgaben mit verschiedenen Applikationen, die sie stets neu herunterladen mussten, zu erfüllen. Dabei wurde ihnen nicht das tatsächliche Ziel der Studie genannt, welches hauptsächlich die Auswirkung der Datenschutzskala auf das Auswahlverhalten der Teilnehmenden war, sondern es wurde ihnen

mitgeteilt, dass es sich lediglich um die Benutzerfreundlichkeit eines neuen App-Marktes handele. Neben einem Fragebogen zum alltäglichen Verhalten bezüglich des Datenschutzes wurde eine Videokonfrontation durchgeführt, in der die Teilnehmenden ihr Verhalten erläutern sollen.

Aus den Ergebnissen konnte ermittelt werden, dass eine farbkodierte Datenschutzskala zu einer besseren Beurteilung der Vertrauenswürdigkeit der Applikationen führt und dies eine adäquatere Entscheidung bezüglich der Wahrung der Privatsphäre mit sich bringt. Ferner wurde die Datenschutzskala als geeignetes Instrument bewertet, um die Transparenz der Daten zu steigern, als auch die Privatsphäre zu schützen. Weiterhin konnte aus dem Fragebogen entnommen werden, dass die Bedenken über den Schutz der privaten Daten seitens der Teilnehmenden meist sehr hoch sind. Darüber hinaus hatte die Datenschutzskala keinen Einfluss auf Entscheidungs- oder Fixationszeiten, weshalb von einer effizienten und informierteren Entscheidung auszugehen ist. Ferner konnte ermittelt werden, dass bekannte Applikationen deutlich schneller ausgewählt werden als unbekannte. Die meisten Teilnehmenden werteten die Datenschutzskala als relevanteste Methode zur Bewertung einer Applikation.

Die Datenschutzskala könnte somit ein geeignetes Instrument sein, um bei den Nutzenden mobiler Endgeräte ein datenschutzfreundlicheres Verhalten zur Applikationsauswahl zu ermöglichen und hervorzurufen. Ferner ist auch damit zu rechnen, dass bei Einführung einer solchen Bewertung Applikationen, die derzeit viele Daten sammeln und weiterleiten versuchen werden dies zu minimieren, um eine bessere Bewertung innerhalb der Datenschutzskala zu erlangen.

Allerdings gibt es im Alltag auch Situationen, bei denen Endnutzende auf eine bestimmte Applikation angewiesen sind, jedoch nicht mit deren Verhalten bezüglich des Umganges mit den privaten Daten einverstanden sind. Deshalb wurde nach einer Lösung gesucht, die es den Nutzenden ermöglicht eine temporäre Zugriffsberechtigung zu erteilen, sodass eine endgültige Einwilligung nicht von Nöten ist.

In der dritten Studie wurde somit eine Applikation entwickelt, bei der es möglich war, neben dem endgültigen Akzeptieren und dem Ablehnen eine temporäre Zugriffsberechtigung über wahlweise einen, drei oder sieben Tagen zu erteilen. Ziel der Studie war es zu eruieren, ob diese temporäre Zugriffsberechtigung akzeptiert und genutzt wird, wobei den Teilnehmenden erneut vermittelt wurde, dass es sich um die Bewertung der Benutzerfreundlichkeit einer Nachrichtenapplikation handele. Nach dem Herunterladen der Applikation wurden den Teilnehmenden täglich verschiedene Aufgaben gestellt, wobei vor allem darauf geachtet wurde, ob die Funktion der temporären Zugriffsberechtigung genutzt wird. Anschließend wurde ein Fragebogen bezüglich der Akzeptanz und Erwünschtheit dieser Funktionen von den Teilnehmenden ausgefüllt.

Nach dem Auswerten der Ergebnisse dieser Studie stellt sich heraus, dass die temporäre Zugriffsberechtigung nur von einem Fünftel der Teilnehmenden genutzt wurde und die knappe Mehrheit die Funktion nicht mochte. Die Teilnehmenden, welche die Funktion genutzt haben, verstanden diese und vergaben die Zugriffsberechtigung meist für eine Zeitspanne von einem Tag. Am häufigsten wurde die Funktion für die Zugriffe auf den Gerätespeicher und die Kontakte genutzt, wobei aus dem Fragebogen hervorging, dass die Funktion vor allem für die Beschränkung des Zugriffes auf die Positionsdaten erwünscht ist. Darüber hinaus gab knapp die Hälfte der Teilnehmenden an, die Funktion im Alltag auf ihrem privaten Endgerät nutzen zu wollen. Hierbei ist davon auszugehen, dass eine vorherige Erläuterung der Funktion zu einer höheren Annahme und verbreiteteren Nutzung der Funktion führen würde.

Zusammenfassend kann in dieser Dissertation eruiert werden, dass den Endnutzenden mobiler Endgeräte ihre persönlichen Daten wichtig sind, jedoch derzeit die Möglichkeiten ihre Daten, zumindest im Bereich der mobilen Endgeräte zu schützen, sehr begrenzt sind. Darüber hinaus ist es von Nöten, den Nutzenden eine möglichst intuitive Methode mit wenig kognitivem Aufwand darzubieten, um sicher zu stellen, dass diese Anklang findet. Durch die Entwicklung und Implementierung einer Datenschutzskala in den App-Markt kann ein datenschutzfreundlicheres Verhalten bezüglich der Applikationsauswahl erzielt werden. Dabei wurde diese Methode als überwiegend positiv bewertet, sodass die Mehrheit der Teilnehmenden sich die Verwirklichung der Datenschutzskala für den alltäglichen Gebrauch wünscht. Die Implementierung einer temporären Zugriffsberechtigung, um das kontinuierliche Sammeln von privaten Daten zu unterbinden, stößt dabei auf weniger Akzeptanz bei den Teilnehmenden, wobei nur etwas weniger als die Hälfte sich für diese Funktion aussprach. Hierbei ist jedoch zu berücksichtigen, dass die Teilnehmenden keine Erläuterung der Funktion hatten und somit die Erfüllung der Aufgaben und nicht der Datenschutz im Fokus der Teilnehmenden lag. Eine zusätzliche Beschreibung der Funktion als auch die Sensibilisierung der Nutzenden bezüglich des Datenschutzes könnte eine deutlich höhere Anwendung dieser Funktion mit sich bringen. Ferner ist es jedoch, auch wenn diese Funktion nur bei knapp der Hälfte der Teilnehmenden Anwendung finden würde, erstrebenswert den Endnutzenden die Möglichkeit zu bieten über ihre eigenen Daten und deren Weitergabe walten und endscheiden zu können. Somit wäre die Implementierung beider Methoden empfehlenswert und würde zum Datenschutz von Endnutzenden mobiler Endgeräte erheblich beitragen. Zur besseren Übersicht der Forschungsfragen und den daraus aufgestellten Hypothesen wurde ein Diagramm erstellt, welches im Anhang II zu finden ist. Darüber hinaus kann diesem Diagramm entnommen werden, ob die entsprechenden Hypothesen aufrechterhalten (grün markiert) werden können, abgelehnt (rot markiert) werden müssen oder nur teilweise bestätigt (orange markiert) werden können. Bei explorativen Forschungsfragen ohne

postulierte Hypothese wurden die Erkenntnisse aus der Forschung (blau markiert) in dem Diagramm implementiert.

Nach diesen Erkenntnissen lassen sich die versuchsübergreifenden Fragen ebenfalls beantworten. Bezüglich der Frage "**Im welchen Umfang schützen die Endnutzenden mobiler Endgeräte ihre persönlichen Daten?"** konnte ermittelt werden, dass der Schutz der persönlichen Daten besonders im privaten Bereich sehr gering ist. Hierbei ist anzumerken, dass die Endnutzenden ihren persönlichen Daten zwar einen recht hohen Stellenwert zuordnen, jedoch nicht bereit sind, einen höheren Aufwand zum Schutz dieser Daten aufzubringen.

Die Erkenntnisse der Vorstudie des zweiten Versuches eruierten bezüglich der Frage „**Welche Illustrationsform einer Datenschutzskala ist die adäquateste, um die Aggressivität einer Applikation darzustellen?**", dass eine farbkodierte mehrfarbige Skala mit fünf verschiedenen Farbabschnitten zu einem Verständnis über die Skala mit geringem kognitivem Aufwand führt. Weiterhin wurde die Label-Scale, welche zusätzlich zur Farbkodierung eine Beschriftung der entsprechenden Kategorien enthält, als geeignetste bewertet.

Nach der Auswertung der zweiten Studie kann folgende Frage beantwortet werden „**Wird durch die Implementierung einer Datenschutzskala in den App-Markt ein datenschutzfreundlicheres Auswahlverhalten bezüglich der Applikationen hervorgerufen?**". Hierbei wurde bei den Stichproben, die eine Datenschutzskala zur Verfügung hatten, ein Auswahlverhalten beobachtet, bei dem als datenschutzfreundlich markierte Applikationen bevorzugt wurden.

Mit Hilfe der dritten Studie ist es möglich, die Frage „**Wird bei der Verfügbarkeit einer Funktion der temporären Zugriffberechtigung diese von den Endnutzenden mobiler Endgeräte verwendet, um ihre Daten zu schützen?**" zu beantworten. Die Funktion der temporären Zugriffsberechtigung wurde lediglich von einem Fünftel der Teilnehmenden angewandt, wobei knapp die Hälfte der Teilnehmenden nach Ausfüllen des Fragenbogens angab, die temporäre Zugriffsberechtigung auf ihrem privaten Endgerät nutzen zu wollen.

9 Literaturverzeichnis

1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83 (Volkszählungsurteil) (BVerfG 15. Dezember 1983).

Acquisti, A [Alessandro], Brandimarte, L. & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514.

Alexander Kunst (Hrsg.). (2019). *Welche Arten von Smartphone-Apps nutzen Sie regelmäßig?* https://de.statista.com/prognosen/999785/umfrage-in-deutschland-zu-beliebten-arten-von-smartphone-apps

AppBrain. (2020a). *Anzahl der kostenlosen Apps im Google Play Store nach Kategorien weltweit im Oktober 2020 (in 1.000)*. https://de.statista.com/statistik/daten/studie/928056/umfrage/anzahl-der-kostenlosen-apps-im-google-play-store-nach-kategorien-weltweit/

AppBrain. (2020b). *Anzahl der verfügbaren Apps im Google Play Store von April 2018 bis November 2020 (in 1.000)*. https://de.statista.com/statistik/daten/studie/74368/umfrage/anzahl-der-verfuegbaren-apps-im-google-play-store/

Appfigures. (2019). *Anzahl der verfügbaren Apps in den Top App-Stores im 2. Quartal 2019*. https://de.statista.com/statistik/daten/studie/208599/umfrage/anzahl-der-apps-in-den-top-app-stores/

Apple. (o.D.). *Kumulierte Anzahl der weltweit heruntergeladenen Apps aus dem Apple App Store von Januar 2011 bis Juni 2017 (in Milliarden)*. https://de.statista.com/statistik/daten/studie/20149/umfrage/anzahl-der-getaetigten-downloads-aus-dem-apple-app-store/

Apple. (2016). *App Store Review Guidelines - Apple Developer*. https://developer.apple.com/app-store/review/guidelines/

Apple. (2017). *Apple Guidelines*. https://developer.apple.com/app-store/review/guidelines/

Au, K. W. Y., Zhou, Y. F., Huang, Z. & Lie, D. (2012). PScout. In T. Yu, G. Danezis & V. Gligor (Hrsg.), *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12* (S. 217). ACM Press. https://doi.org/10.1145/2382196.2382222

Baeriswyl, B. (2000). Data Mining und Data Warehousing: Kundendaten als Ware oder geschütztes Gut. *Recht der Datenverarbeitung*, *1*, 6–11.

Bakos, Y., Marotta-Wurgler, F. & Trossen, D. R. (2014). Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts. *The Journal of Legal Studies*, *43*(1), 1–35. https://doi.org/10.1086/674424

Barrera, D., Kayacik, H. G. ü. ş., van Oorschot, P. C. & Somayaji, A. (2010). A methodology for empirical analysis of permission-based security models and its application to android. In E. Al-Shaer, A. D. Keromytis & V. Shmatikov (Hrsg.), *Proceedings of the 17th ACM conference on Computer and communications security* (S. 73–84). ACM. https://doi.org/10.1145/1866307.1866317

Bartelt, J. & Rieger, B. (2015). IT-Sicherheit im Mittelstand. In *Mittelstand-Motor und Zukunft der deutschen Wirtschaft* (S. 557–569). Springer.

Barton, T., Herrmann, F., Meister, V. G., Müller, C. & Seel, C. (Hrsg.). (2017). *Prozesse, Technologie, Anwendungen, Systeme und Management 2017: Angewandte Forschung in der Wirtschaftsinformatik : Tagungsband zur 30. AKWI-Jahrestagung vom 17.09.2017 bis 20.09.2017 an der Hochschule Aschaffenburg*. Hochschule Aschaffenburg; mana-Buch.

Begole, J. (2007). *CHI 2007: Reach beyond conference proceedings Conference on Human Factors in Computing Systems, San Jose, California, USA, April 28-May 3, 2007*. Association for Computing Machinery.

Benbasat, I., Dexter, A. S. & Todd, P. (1986). An experimental program investigating color-enhanced and graphical information presentation: an integration of the findings. *Communications of the ACM*, *29*(11), 1094–1105.

Benesty, J., Chen, J., Huang, Y. & Cohen, I. (2009). Pearson correlation coefficient. In *Noise reduction in speech processing* (S. 1–4). Springer.

Birbaumer, N. & Schmidt, R. F [R. F.]. (2000). Lernen und Gedächtnis. In R. F. Schmidt, G. Thews & F. Lang (Hrsg.), *Springer-Lehrbuch. Physiologie des Menschen* (S. 154–166). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-09346-7_8

Bitkom. (o.D.). *Schadenssummen durch Computerkriminalität in Unternehmen in Deutschland im Jahr 2018 (in Milliarden Euro).* Bitkom. https://de.statista.com/statistik/daten/studie/444719/umfrage/schaeden-durch-computerkriminalitaet-in-deutschen-unternehmen/

Bitkom. (2016). *Anteil der Smartphone- und Tablet-Nutzer in Deutschland in den Jahren 2012 bis 2015*. https://de.statista.com/statistik/daten/studie/161914/umfrage/anteil-der-smartphone-und-tablet-besitzer-in-deutschland/

Bitkom. (2019). *Anteil der Smartphone-Nutzer in Deutschland in den Jahren 2012 bis 2018*. https://de.statista.com/statistik/daten/studie/585883/umfrage/anteil-der-smartphone-nutzer-in-deutschland/

Bitkom. (2020, 21. Januar). *Anteil der Tablet-Nutzer in Deutschland in den Jahren 2012 bis 2020*.

BMWi. (o.D.). *Ausgaben für Datensicherheit im Bereich B2B-E-Commerce von 2003 bis 2008 nach Regionen in Milliarden Euro*. https://de.statista.com/statistik/daten/studie/29157/umfrage/ausgaben-fuer-datensicherheit-im-bereich-b2b-e-commerce-nach-regionen/.

Book, T., Pridgen, A. & Wallach, D. S. (2013). Longitudinal analysis of android ad library permissions. *arXiv preprint arXiv:1303.0857*.

Born, C. (2001). *Schadensersatz bei Datenschutzverstößen: Ein ökonomisches Instrument des Datenschutzes und seine präventive Wirkung*. *Schriften zum Informations-, Telekommunikations- und Medienrecht.*

Bundeszentrale für politische Bildung (Hrsg.). (2020). *Bevölkerung nach Altersgruppen und Geschlecht*.

C. I.O. (2019). *Winter 2019: State of the CIO*. https://www.cio.com/article/3335497/winter-2019-state-of-the-cio.html

Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M. & & de Oliveira, R. (2013). Your browsing behavior for a big mac: Economics of personal information online. *Proceedings of the 22nd international conference on World Wide Web*, 189–200.

Child, J. T., Pearson, J. C. & Petronio, S. (2009). Blogging, communication, and privacy management: Development of the Blogging Privacy Management Measure. *Journal of the American Society for Information Science and Technology*, *60*(10), 2079–2094. https://doi.org/10.1002/asi.21122

Chin, E [E.], Felt, A. P [A. P.], Sekar, V. & Wagner, D [D.] (Hrsg.) (2012). *Measuring user confidence in smartphone security and privacy*. ACM.

Christ, R. E. (1975). Review and analysis of color coding research for visual displays. *Human factors*, *17*(6), 542–570.

Cimbalo, R. S., Beck, K. L. & Sendziak, D. S. (1978). Emotionally Toned Pictures and Color Selection for Children and College Students. *The Journal of Genetic Psychology*, *133*(2), 303–304. https://doi.org/10.1080/00221325.1978.10533389

Conover, W. J. & Iman, R. L. (1981). Rank transformations as a bridge between parametric and nonparametric statistics. *The American Statistician*, *35*(3), 124–129.

Conti, M., Nguyen, V. T. N. & Crispo, B. (2011). CRePE: Context-Related Policy Enforcement for Android. In M. Burmester, G. Tsudik, S. Magliveras & I. Ilić (Hrsg.), *Lecture Notes in Computer Science: Bd. 6531. Information security: 13th international conference, ISC 2010, Boca Raton, FL, USA, October 25 - 28, 2010 ; revised selected papers* (Bd. 6531, S. 331–345). Springer. https://doi.org/10.1007/978-3-642-18178-8_29

Council, N. C. (2018). Deceived by design, How tech companies use dark patterns to discourage us from exercising our rights to privacy. *Norwegian Consumer Council Report*.

Coy, W. (1988). *Aufbau und Arbeitsweise von Rechenanlagen*. Vieweg+Teubner Verlag. https://doi.org/10.1007/978-3-322-83896-4

Culnan, M. J. & Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. *MIS Quarterly*, *33*(4), 673–687.

Custers, B. (2016). Click here to consent forever: Expiry dates for informed consent. *Big Data & Society*, *3*(1), 2053951715624935.

Dance, G. J., Laforgia, M. & Confessore, N. (2018, 18. Dezember). *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*. https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html

Daniel Franzen & David Aspinall (Hrsg.) (2016). *PhoneWrap-Injecting the" How Often" into Mobile Apps.*

Dedić, N. & Stanier, C. (2016). An Evaluation of the Challenges of Multilingualism in Data Warehouse Development. In *18th International Conference on Enterprise Information Systems,* Rome, Italy.

Distimo. (2014). *Apple App Store - Verteilung der Apps nach Geschäftsmodell weltweit 2014 | Statistik*. https://de.statista.com/statistik/daten/studie/321738/umfrage/anteil-der-kostenlosen-und-kostenpflichtigen-apps-im-apple-app-store-weltweit/

Documentation, A. D. (2019). Dangerous permissions. *Accessed on: Jan*, *27*.

Doolaard, F. T., Lelieveld, G.-J., Noordewier, M. K., van Beest, I. & van Dijk, E. (2020). Get out or stay out: How the social exclusion process affects actors, but not targets. *Journal of Experimental Social Psychology*, *88*, 103946. https://doi.org/10.1016/j.jesp.2019.103946

Dresing, T. & Pehl, T. (2020). Transkription. In *Handbuch qualitative Forschung in der Psychologie* (S. 835–854). Springer.

DSGVO. (2018). *EU-Datenschutz-Grundverordnung: Neue Fassung der EU-Datenschutz-Grundverordnung Mit Geltung Ab 25. Mai 2018*.

Eco. (o.D.). *Werden die Ausgaben für IT-Sicherheit in absehbarer Zeit Ihrer Meinung nach steigen oder sinken?* Eco. https://de.statista.com/statistik/daten/studie/384506/umfrage/umfrage-unter-it-experten-zur-entwicklung-der-ausgaben-fuer-it-sicherheit/.

Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P. & Sheth, A. N. (2014). TaintDroid. *ACM Transactions on Computer Systems*, *32*(2), 1–29. https://doi.org/10.1145/2619091

Enck, W., Ongtang, M. & McDaniel, P. (2009). On lightweight mobile phone application certification. *Proceedings of the 16th ACM Conference on Computer and Communications Security*.

Epstein, R. (2006). Contract, not Regulation: UCITA and High-Tech Consumers Meet Their Consumer Protection Critics. *Consumer Protection in the Age of the 'Information Economy'*, 205. http://chicagounbound.uchicago.edu/book_chapters/107

Richtlinie 95/46/EG Art. 15 Abs. 1 des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. EG (Amtsblatt der Europäischen Gemeinschaft) S. 31-50 (1995).

Eurostat. (2016). *Anteil der Haushalte in Deutschland mit Internetzugang von 2002 bis 2015.* https://de.statista.com/statistik/daten/studie/153257/umfrage/haushalte-mit-internetzugang-in-deutschland-seit-2002/

EY. (o.D.). *Wie hoch war ungefähr der durchschnittliche Schaden pro Datendiebstahl in Ihrem Unternehmen?* EY. https://de.statista.com/statistik/daten/studie/758758/umfrage/finanzielle-schaeden-durch-datendiebstahl-in-unternehmen-in-oesterreich/

Fayyad, U., Piatetsky-Shapiro, G. & Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI magazine*, *17*(3), 37.

Felt, A. P [Adrienne Porter], Egelman, S [Serge], Finifter, M., Akhawe, D. & Wagner, D. A. (2012). How to Ask for Permission. *HotSec*. https://www.usenix.org/conference/hotsec12/workshop-program/presentation/felt

Felt, A. P [Adrienne Porter], Ha, E., Egelman, S [Serge], Haney, A., Chin, E [Erika] & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. In L. F. Cranor (Hrsg.), *Proceedings of the Eighth Symposium on Usable Privacy and Security.* ACM. https://doi.org/10.1145/2335356.2335360

FireEye, I. (2015). *Out of Pocket: A Comprehensive Mobile Threat Assessment of 7 Million iOS and Android Apps.*

Fix, E. & Hodges Jr, J. L. (1955). Significance probabilities of the Wilcoxon test. *The Annals of Mathematical Statistics*, 301–312.

Forbrukerrådet. (2016). *Appfail Report: Threats to Consumers in Mobile Apps*. https://fil.forbrukerradet.no/wp-content/uploads/2016/03/Appfail-Report-2016.pdf

Fritsch, L. (2017). *Partial commitment–"Try before you buy" and "Buyer's remorse" for personal data in Big Data & Machine learning*.

Fuchs, C. (2010). Facebook, Web 2.0 und ökonomische Überwachung. *Datenschutz und Datensicherheit - DuD*, *34*(7), 453–458. https://doi.org/10.1007/s11623-010-0128-x

Gillette, C. P. (2004). *Rolling Contracts as an Agency Problem.*

Good, N [Nathaniel], Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D. & Konstan, J. (Hrsg.) (2005). *Stopping spyware at the gate: a user study of privacy, notice and spyware*. ACM.

Google. (2017). *Monetarisierung und Werbung*. https://play.google.com/intl/de/about/monetization-ads/

Google Developers. (2020). https://developer.android.com/guide/topics/permissions/overview

Griesenbrock, S. (2014). *Der Milliardenmarkt mit Apps: Studie zur globalen Entwicklung mobiler Applikationen*. Diplomica-Verl.

Gross, R. & Acquisti, A [A.] (Hrsg.) (2005). *Information revelation and privacy in online social networks.*

Grossklags, J. & Good, N [Nathan] (Hrsg.) (2007). *Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers*. *Financial Cryptography and Data Security*. Springer Berlin Heidelberg.

Gu, J., Xu, Y., Xu, H., Zhang, C. & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94*, 19–28. https://doi.org/10.1016/j.dss.2016.10.002

Guan, Z., Lee, S., Cuddihy, E. & Ramey, J. (Hrsg.) (2006). *The validity of the stimulated retrospective think-aloud method as measured by eye tracking.*

Guide, C. (2019). IT Security. *Huawei Technologies Co., Ltd.-2012*.

Hammad, M., Bagheri, H. & Malek, S. (2017). Determination and Enforcement of Least-Privilege Architecture in Android. In *ICSA 2017: 2017 IEEE International Conference on Software Architecture : proceedings : 3-7 April 2017, Gothenburg, Sweden* (S. 59–68). IEEE. https://doi.org/10.1109/ICSA.2017.18

Hartley, J. (2008). Legal ease and 'Legalese'. *Psychology, Crime & Law*, *6*(1), 1–20. https://doi.org/10.1080/10683160008410828

Hatamian, M., Serna, J. & Rannenberg, K. (2019). Revealing the unrevealed: Mining smartphone users privacy perception on app markets. *Computers & Security*, *83*, 332–353.

Hatamian, M., Serna, J., Rannenberg, K. & Igler, B. (Hrsg.) (2017). *Fair: Fuzzy alarming index rule for privacy analysis in smartphone apps*. Springer.

Hermann, E., Volker, C. & Schwill, A. (1993). *Duden Informatik: Ein Sachlexikon für Studium und Praxis* (2. Aufl.). Dudenverlag.

Hibbard, J. H. & Peters, E. (2003). Supporting informed consumer health care decisions: data presentation approaches that facilitate the use of information in choice. *Annual review of public health*, *24*(1), 413–433.

Hillebrand, A., Niederprüm, A., Schäfer, S., Thiele, S. & Henseler-Unger, I. (2017). Aktuelle Lage der IT-Sicherheit in KMU. *Projekt im Rahmen der BMWi-Initiative „IT-Sicherheit in der Wirtschaft ", Langfassung und Kurzfassung zum Download unter www. wik. org. Kurzfassung kann als Broschüre angefordert werden*.

Hiscox. (o.D.a). *Haben sie aktuell eine Cyber-Versicherung?* Hiscox. https://de.statista.com/statistik/daten/studie/695209/umfrage/inanspruchnahme-von-cyber-versicherungen-durch-unternehmen-im-vereinigten-koenigreich/

Hiscox. (o.D.b). *Was hat sich in den letzten zwölf Monaten aufgrund von Cybercrime-Vorfällen in Ihrem Unternehmen geändert?* Forrester Research. https://de.statista.com/statistik/daten/studie/693068/umfrage/reaktionen-der-unternehmen-auf-cybercrime-vorfaelle/.

Hoepman, J. H. (2014). Privacy Design Strategies. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, T. Sans & J.-H. Hoepman (Hrsg.), *Privacy Design Strategies: ICT Systems Security and Privacy Protection* (Vol. 428). Springer Berlin Heidelberg.

Hofmann, D. A., Jacobs, R. & Landy, F. (1995). High reliability process industries: Individual, micro, and macro organizational influences on safety performance. *Journal of Safety Research*, *26*(3), 131–149. https://doi.org/10.1016/0022-4375(95)00011-E

Holdampf-Wendel, A., SHAHD, M. & HAMPE, K. (2014). Jung und vernetzt–Kinder und Jugendliche in der digitalen Gesellschaft. *Studie der Bitkom Research GmbH.[online] https://www. bitkom. org/Publikationen/2014/Studien/Jung-und-vernetzt-Kinder-und-Jugendliche-in-der-digitalen-Gesellschaft/BITKOM_Studie_Jung_und_vernetzt_2014. pdf [17-11-2015]*.

Holland, P. C. (1984). Origins of behavior in Pavlovian conditioning. In *Psychology of Learning and Motivation* (Bd. 18, S. 129–174). Elsevier.

Hubmann, H. (1953). *Das Persönlichkeitsrecht*. Böhlau.

Hugl, U. (2012). Privacy Management in Progress: Balanceakte zwischen Öffnung und Schließung personenbezogener Daten. In Rußmann, U., Beinsteiner, A., Ortner, H., & Hug, T (Hrsg.), *Grenzenlose Enthüllungen? Medien zwischen Öffnung und Schließung* (S. 125–142). Innsbruck University Press.

IFH Köln. (2015). *Perspektiven für den Datenschutz in Europa aus Sicht der Verbraucher und des (elektronischen) Handels*.

Inmon, W. H. (1992). *Building the Data Warehouse*. John Wiley & Sons, Inc.

Jaeyeon, J., Han, S. & Wetherall, D. (Hrsg.) (2012). *Short paper: enhancing mobile application permissions with runtime feedback and constraints.*

Kabakus, A. T. & Dogru, I. A. (2018). An in-depth analysis of Android malware using hybrid techniques. *Digital Investigation*, *24*, 25–33. https://doi.org/10.1016/j.diin.2018.01.001

Kantar. (2020). *Vergleich der Marktanteile von Android und iOS am Absatz von Smartphones in Deutschland von Januar 2012 bis Juni 2020 [Graph].* https://de.statista.com/statistik/daten/studie/256790/umfrage/marktanteile-von-android-und-ios-am-smartphone-absatz-in-deutschland/

Keith-Lucas, T. & Guttman, N. (1975). Robust-single-trial delayed backward conditioning. *Journal of Comparative and Physiological Psychology*, *88*(1), 468–476.

Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N. & Wetherall, D. (Hrsg.). (2012). *A Conundrum of Permissions: Installing Applications on an Android Smartphone* (Bd. 7398). https://doi.org/10.1007/978-3-642-34638-5_6

Kelley, P. G., Cranor, L. F. & Sadeh, N. (2013). Privacy as part of the app decision-making process. In W. E. Mackay, S. Brewster & S. Bødker (Hrsg.), *CHI 2013: Changing perspectives ; the 31st Annual CHI Conference on Human Factors in Computing Systems, conference proceedings, 27 April - 2 May 2013, Paris, France* (S. 3393). ACM. https://doi.org/10.1145/2470654.2466466

Kitchener, R. F. (1977). Behavior and behaviorism. *Behaviorism*, *5*(2), 11–71.

Konrad, K. (2020). Lautes Denken. In *Handbuch qualitative Forschung in der Psychologie* (S. 373–393). Springer.

Kords, M. (2019, 4. Dezember). *PwC. (17. Oktober, 2019). Prognose des Marktvolumens von fahrzeugbasierten Connected Services nach weltweiten Regionen in den Jahre 2018 bis 2030 (in Milliarden US-Dollar)*. https://de.statista.com/statistik/daten/studie/984961/umfrage/prognose-des-marktvolumens-von-connected-car-services-nach-weltweiten-regionen/

Kraus, L., Ina Wechsung & Sebastian Möller (Hrsg.) (2014). *Using statistical information to communicate android permission risks to users*. IEEE.

Krüger, D. & Riemeier, T. (2014). Die qualitative Inhaltsanalyse–eine Methode zur Auswertung von Interviews. In *Methoden in der naturwissenschaftsdidaktischen Forschung* (S. 133–145). Springer.

Krunz, M. (2012). *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*. ACM. http://www4.ncsu.edu/~mcgrace/WISEC12_ADRISK.pdf

Kruskal, W. H. & Wallis, W. A. (1952). Use of ranks in one-criterion variance analysis. *Journal of the American statistical Association*, *47*(260), 583–621.

Lefrancois, G. R. (2013). *Psychologie des Lernens*. Springer-Verlag.

Lilliefors, H. W. (1967). On the Kolmogorov-Smirnov test for normality with mean and variance unknown. *Journal of the American statistical Association*, *62*(318), 399–402.

Malhotra, N. K., Kim, S. S. & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.

Manar Alohaly & Hassan Takabi (Hrsg.) (2016). *Better privacy indicators: a new approach to quantification of privacy policies.*

Maske, P. (2012). *Mobile Applikationen*. Springer.

Mayerhofer, J. (2012). *Apps erfolgreich verkaufen: Vermarktungsstrategien für Apps auf iPhone, iPad, Android und Co*. Hanser. http://dx.doi.org/10.3139/9783446431607 https://doi.org/10.3139/9783446431607

Mayring, P. (2015). *Qualitative Inhaltsanalyse. 12., überarb. Aufl*. Weinheim: Beltz.

McAfee Labs. (2016). *McAfee Labs 2016 Threats Predictions Report*. https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/rp-threats-predictions-2016.pdf

McKnight, P. E. & Najab, J. (2010). Mann-Whitney U Test. *The Corsini encyclopedia of psychology*, 1.

Meier, R. (2006). *Praxis E-Learning: Grundlagen, Didaktik, Rahmenanalyse, Medienauswahl, Qualifizierungskonzept, Betreuungskonzept, Einführungsstrategie, Erfolgssicherung ; mit CD-ROM*. *Professional Training*. GABAL-Verl. http://deposit.ddb.de/cgi-bin/dokserv?id=2689670&prov=M&dok_var=1&dok_ext=htm

Mester, B. A. (2014). Tagungsbericht von der DSRI-Herbstakademie 2013, Berlin 11.—14. September ‚Law as a Service (LaaS)—Recht im Internet-und Cloud-Zeitalter'. *Datenschutz und Datensicherheit - DuD*, *38*(1), 64.

Midha, V. (2012). Impact of consumer empowerment on online trust: An examination across genders. *Decision Support Systems*, *54*(1), 198–205. https://doi.org/10.1016/j.dss.2012.05.005

Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological review*, *63*(2), 81.

Milne, G. R. & Rohm, A. J. (2000). Consumer Privacy and Name Removal across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives. *Journal of Public Policy & Marketing*, *19*(2), 238–249. https://doi.org/10.1509/jppm.19.2.238.17136

Momen, N. (2018a). *Towards Measuring Apps' Privacy-Friendliness (licentiate thesis)*.

Momen, N. (2018b). *Turning the Table Around: Monitoring App Behavior*.

Momen, N., Bock, S. & Fritsch, L. (2020). *Accept-Maybe-Decline: Introducing Partial Consent for the Permission-based Access Control Model of Android*.

Momen, N. & Fritsch, L. (2020). App-generated digital identities extracted through Android permission-based data access-a survey of app privacy. *SICHERHEIT 2020*.

Momen, N., Hatamian, M. & Fritsch, L. (2019). Did App Privacy Improve After the GDPR? *IEEE Security and Privacy Magazine*, *17*(6), 10–20.

Nauman, M., Khan, S. & Zhang, X. (2010). Apex: Extending android permission model and enforcement with user-defined runtime constraints. *Proceedings of the 5th ACM Symposium on*, 328–332.

Office for National Statistics (UK). (2019). *Anteil der mobilen Internetnutzer nach Endgeräten in Großbritannien im Jahr 2019.* https://de.statista.com/statistik/daten/studie/898162/umfrage/nutzung-des-internets-unterwegs-nach-endgeraeten-in-grossbritannien/

Olson, G. M. & Olson, J. S. (2003). Human-computer interaction: psychological aspects of the human use of computing. *Annual review of psychology*, *54*, 491–516. https://doi.org/10.1146/annurev.psych.54.101601.145044

Ongtang, M., McLaughlin, S., Enck, W. & McDaniel, P. (2012). Semantically rich application-centric security in Android. *Security and Communication Networks*, *5*(6), 658–673. https://doi.org/10.1002/sec.360

Pagano, R. R. (2010). *Understanding statistics in the behavioral sciences (9th ed.).* CA: Thomson Wadsworth.

Pavlov, I. P. (1927). Conditional reflexes: an investigation of the physiological activity of the cerebral cortex.

Payne, M. (2017). *An overview of the cyber insurance industry: Challenges for insurers and insureds in quantifying and mitigating cyber risk.*

Peng, H., Gates, C., Sarma, B., Li, N., Qi, Y., Potharaju, R., Nita-Rotaru, C. & Molloy, I. (2012). Using probabilistic generative models for ranking risks of Android apps. In T. Yu, G. Danezis & V. Gligor (Hrsg.), *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12* (S. 241). ACM Press. https://doi.org/10.1145/2382196.2382224

Perez, S. (2015). *App Submissions On Google Play Now Reviewed By Staff, Will Include Age-Based Ratings*. https://techcrunch.com/2015/03/17/app-submissions-on-google-play-now-reviewed-by-staff-will-include-age-based-ratings/

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Suny Press.

Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation? *Journal of family theory & review*, *2*(3), 175–196.

Plaut, V. C. & Bartlett, R. P. (2012). Blind consent? A social psychological investigation of non-readership of click-through agreements. *Law and human behavior*, *36*(4), 293–311. https://doi.org/10.1037/h0093969

Pommerening, K. (1991). *Datenschutz und Datensicherheit*. BI-Wiss.-Verlag.

Priori Data. (2017). *Number of app downloads on the App Store and Play Store in the UK, Germany and France in 2016 (in billions)*. https://www.statista.com/statistics/764692/downloads-d-applications-kingdom-united-germany-and-la-france/

Puth, M.-T., Neuhäuser, M. & Ruxton, G. D. (2015). Effective use of Spearman's and Kendall's correlation coefficients for association between two measured traits. *Animal Behaviour*, *102*, 77–84.

Qiao, M., Sung, A. H. & Liu, Q. (2016). Merging Permission and API Features for Android Malware Detection. In T. Matsuo, A. Kanzaki, N. Komoda & A. Hiramatsu (Hrsg.), *2016 5th IIAI International Congress on Advanced Applied Informatics - IIAI-AAI 2016: Kumamoto, Japan, 10-14 July 2016 : proceedings* (S. 566–571). IEEE. https://doi.org/10.1109/IIAI-AAI.2016.237

Radner, W., Willinger, U., Obermayer, W., Mudrich, C., Velikay-Parel, M. & Eisenwort, B. (1998). Eine neue Lesetafel zur gleichzeitigen Bestimmung von Lesevisus und Lesegeschwindigkeit [A new reading chart for simultaneous determination of reading vision and reading speed]. *Klinische Monatsblatter fur Augenheilkunde*, *213*(3), 174–181. https://doi.org/10.1055/s-2008-1034969

Rajivan, P. & Jean, C. (Hrsg.) (2016). *Influence of privacy attitude and privacy cue framing on android app choices.*

Rakoff, T. D. (1983). Contracts of Adhesion: An Essay in Reconstruction. *Harvard Law Review*, *96*(6), 1173. https://doi.org/10.2307/1341009

Ramey, J., Boren, T., Cuddihy, E., Dumas, J., Guan, Z., van den Haak, M. J. & Jong, M. D. de (Hrsg.) (2006). *Does think aloud work? How do we know?*

Reidenberg, J. R. (1997). Lex informatica: The formulation of information policy rules through technology. *Tex. L. Rev.*, *76*, 553.

Robertson, J. (2012). Android apps collect too much user data. *The Sydney Morning Herald*. http://www.smh.com.au/digital-life/digital-life-news/android-apps-collect-too-much-user-data-researcher-says-20121102-28oie.html/

Rodríguez-Aranda, C. (2003). Reduced writing and reading speed and age-related changes in verbal fluency tasks. *The Clinical neuropsychologist*, *17*(2), 203–215. https://doi.org/10.1076/clin.17.2.203.16508

Rosen Sanae, Zhiyun Qian & Z. Morely Mao (Hrsg.) (2013). *Appprofiler: a flexible method of exposing privacy-related behavior in android applications to end users.*

Rosenberg, M. (2018, 23. März). *Bolton Was Early Beneficiary of Cambridge Analytica's Facebook Data*. https://www.nytimes.com/2018/03/23/us/politics/bolton-cambridge-analyticas-facebook-data.html

Salkind, N. J. (2010). *Encyclopedia of research design*. Sage.

Sandmann, A. (2014). Lautes Denken–die Analyse von Denk-, Lern-und Problemlöseprozessen. In *Methoden in der naturwissenschaftsdidaktischen Forschung* (S. 179–188). Springer.

Schaper, N. (2011). Psychologie der Arbeitssicherheit. In F. W. Nerdinger, G. Blickle & N. Schaper (Hrsg.), *Springer-Lehrbuch. Arbeits- und Organisationspsychologie* (S. 451–474). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-16972-4_27

Schmidt, M. (2015). *Mehrheit gegen Vorratsdatenspeicherung – selbst, wenn sie hilft*. https://yougov.de/news/2015/06/30/mehrheit-gegen-vorratsdatenspeicherung-selbst-wenn/

Schober Information Group GmbH. (2017). *Schober Adressen*. http://shop.schober.com/index.php?EVENT=home&PHPSESSID=rh3hrlqqesvhoi9ig18fbrkjq7

Schwabe, A., Brandl, L., Boomgaarden, H. G. & Stocker, G. (2020). Literatur am Bildschirm: Zum Stand der empirischen Leseforschung. *Orbis Litterarum*, *75*(5), 213–229.

Sedgwick, P. (2012). Multiple significance tests: the Bonferroni correction. *Bmj*, *344*, e509.

Shklovski I., Mainwaring S. D., Skúladóttir H. H. & Borgthorsson, H. (Hrsg.) (2014). *Leakiness and creepiness in app space: Perceptions of privacy and mobile app use.*

Skinner, B. F. (1948). Superstition in the pigeon. *Journal of experimental psychology*, *38*(2), 168–172.

Skinner, B. F. (1984). An operant analysis of problem solving. *Behavioral and Brain Sciences*, *7*(04), 583. https://doi.org/10.1017/S0140525X00027412

Smith, H. J., Milberg, S. J. & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, *20*(2), 167–196. https://pdfs.semanticscholar.org/57fc/4b0249ee98e7370c7718d3dc7880571664c8.pdf

Snethlage, J. L. (1929). Der Behaviorismus. *Kant-Studien*, *34*(1-4), 167–175.

Solove, D. J. (2006). A taxonomy of privacy. *U. Pa. L. Rev.*, *154*, 477–560.

Spencer, G. (2016). *Exploring the App Store's Top Grossing Chart*. https://www.macstories.net/stories/exploring-the-app-stores-top-grossing-chart/

Staiano, J., Oliver, N., Lepri, B., Oliveira, R. de, Caraviello, M. & Sebe, N. (2014). Money walks. *UbiComp '14 Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 583–594. https://doi.org/10.1145/2632048.2632074

Stanley, M. (2010). *Internet Trends*. https://de.slideshare.net/blueeyepathrec/internet-trends-ri041210-3723169

Statista. (o.D.). *Umsatz im Apple App Store und Google Play Store weltweit in den Jahren 2014 bis 2016 (in Milliarden US-Dollar).* https://de.statista.com/statistik/daten/studie/180896/umfrage/apple-app-store-vs-google-playstore-umsatz/

Statista Research Department (Hrsg.). (2020). *Wie hören Sie zu Hause am liebsten Musik?*

Statistisches Bundesamt. (2020). *Anteil der privaten Haushalte in Deutschland mit Personal Computern von 2000 bis 2020*. https://de.statista.com/statistik/daten/studie/2596/umfrage/ausstattungsgrad-privater-haushalte-mit-einem-pc-seit-1998/

Steiner, D. D. & Rain, J. S. (1989). Immediate and delayed primacy and recency effects in performance evaluation. *Journal of Applied Psychology*, *74*(1), 136.

Suhr, F. (2020). *Die größten Risiken für mittelständische Unternehmen*. https://de.statista.com/infografik/20895/groesste-risiken-fuer-mittelstaendische-unternehmen/

Tekfi, C. (1987). Readability formulas: An overview. *Journal of documentation*, *43*(3), 261–273.

Tenzer, F. (2020a, 13. August). *VuMA. (13. November, 2019). Anzahl der Smartphone-Nutzer in Deutschland in den Jahren 2009 bis 2019 (in Millionen)*. https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/

Tenzer, F. (2020b, 20. August). *Strategy Analytics. (11. August, 2020). Absatz von intelligenten Lautsprechern weltweit vom 3. Quartal 2016 bis zum 2. Quartal 2020 (in Millionen Stück)*. https://de.statista.com/statistik/daten/studie/818982/umfrage/absatz-von-intelligenten-lautsprechern-weltweit-pro-quartal/

Tenzer, F. (2020c, 6. Oktober). *Ausgaben für IT-Sicherheit in Deutschland nach Segment in den Jahren 2017 bis 2019 und Prognose bis 2021 (in Milliarden Euro)*. https://de.statista.com/statistik/daten/studie/151727/umfrage/ausgaben-fuer-it-sicherheit-in-deutschland/

Thompson C., Johnson M., Egelman, S [S.], Wagner, D [D.] & King, J. (Hrsg.) (2013). *When it's better to ask forgiveness than get permission: attribution mechanisms for smartphone resources.*

Thurm, S. & Kane, Y. I. (2010). Your apps are watching you. *The Wall Street Journal*, *17*, 1. http://www.wsj.com/articles/SB10001424052748704694004576020083703574602

Todd, P. & Benbasat, I. (1992). The Use of Information in Decision Making: An Experimental Investigation of the Impact of Computer-Based Decision Aids. *MIS Quarterly*, *16*(3), 373–393. https://doi.org/10.2307/249534

Trefis.com. (o.D.). *Schätzung des durchschnittlichen Preises kostenpflichtiger Apps für das iPhone und iPad weltweit in den Jahren 2009 bis 2023 (in US-Dollar)*. https://de.statista.com/statistik/daten/studie/170003/umfrage/preisentwicklung-von-apps-in-den-fuehrenden-app-stores-weltweit

Tsai, J. Y., Egelman, S [Serge], Cranor, L. & Acquisti, A [Alessandro] (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*(2), 254–268.

TUI Stiftung (Hrsg.). (2018). *Wie sehr vertrauen Sie den folgenden Organisationen und Gruppen?*

VentureBeat. (o.D.). *Anzahl der Apps, die im Google Play Store heruntergeladen wurden in den Jahren 2014 bis 2017 (in Milliarden)*. https://de.statista.com/statistik/daten/studie/243412/umfrage/anzahl-von-downloads-im-google-play-store/

Wächter, M. (2016). *Mobile Strategy: Marken- und Unternehmensführung im Angesicht des Mobile Tsunami*. *#RideTheMobileTsunami*. Springer Gabler. http://dx.doi.org/10.1007/978-3-658-06011-4 https://doi.org/10.1007/978-3-658-06011-4

Wade Morris, J. & Elkins, E. (2015). FCJ-181 There's a History for That: Apps and Mundane Software as Commodity. *The Fibreculture Journal*(25), 63–88. https://doi.org/10.15307/fcj.25.181.2015

Watson, J., Lipford, H. R. & Besmer, A. (2015). Mapping user preference to privacy default settings. *ACM Transactions on Computer-Human Interaction (TOCHI)*, *22*(6), 1–20.

Watson, J. B. (1998). *Behaviorism*. Routledge.

Wijesekera, P., Baokar, A., Hosseini, A., Egelman, S [Serge], Wagner, D. & Beznosov, K. (2015). Android Permissions Remystified: A Field Study on Contextual Integrity.

Wilcox, R. R. (2011). *Introduction to robust estimation and hypothesis testing*. Academic press.

Witt, B. C. (2008). *Datenschutz kompakt und verständlich*. Vieweg. https://doi.org/10.1007/978-3-8348-9442-7

Xu, H., Gupta, S., Rosson, M. B. & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy.

Zhauniarovich, Y. & Gadyatskaya, O. (2016). Small Changes, Big Changes: An Updated View on the Android Permission System. In F. Monrose, M. Dacier, G. Blanc & J. Garcia-Alfaro (Hrsg.), *Lecture Notes in Computer Science: Bd. 9854. Research in Attacks, Intrusions, and Defenses: 19th International Symposium, RAID 2016, Paris, France, September 19-21, 2016, Proceedings* (Bd. 9854, S. 346–367). Springer International Publishing. https://doi.org/10.1007/978-3-319-45719-2_16

Anhang

Anhang A. Measuring mobile users' concerns for information privacy (MUIPC)

Research Constructs and Measures

Perceived surveillance (self-developed) (Xu et al., 2012)

(1) I believe that the location of my mobile device is monitored at least part of the time.

(2) I am concerned that mobile apps are collecting too much information about me.

(3) I am concerned that mobile apps may monitor my activities on my mobile device.

Perceived intrusion (Xu et al. 2008)

(1) I feel that as a result of my using mobile apps, others know about me more than I am comfortable with.

(2) I believe that as a result of my using mobile apps, information about me that I consider private is now more readily available to others than I would want.

(3) I feel that as a result of my using mobile apps, information about me is out there that, if used, will invade my privacy.

Secondary use of personal information (Smith et al. 1996)

(1) I am concerned that mobile apps may use my personal information for other purposes without notifying me or getting my authorization.

(2) When I give personal information to use mobile apps, I am concerned that apps may use my information for other purposes.

(3) I am concerned that mobile apps may share my personal information with other entities without getting my authorization.

Prior Privacy Experience (Smith et al. 1996)

(1) How often have you personally experienced incidents whereby your personal information was used by some company or e-commerce web site without your authorization?

(2) How much have you heard or read during the last year about the use and potential misuse of the information collected from the Internet?

(3) How often have you personally been the victim of what you felt was an improper invasion of privacy?

Behavioral Intention (Xu et al. 2004)

(1) I am likely to disclose my personal information to use mobile apps in the next 12 months.

(2) I predict I would use mobile apps in the next 12 months.

(3) I intend to use mobile apps in the next 12 months.

Anhang B. Fragebogen zur Erfassung der Einstellung gegenüber der Weitergabe der Daten und Rechte

Teilnehmer-Nr: _____

(Die in dieser Untersuchung erhobenen Daten werden anonym behandelt und nicht an Dritte weitergegeben. Bei Fragen oder Unklarheiten wenden Sie sich bitte an den Versuchsleiter.)

1. **Geschlecht:**

☐ männlich ☐ weiblich

2. **Alter:** _____
3. **Welche Betriebssysteme nutzen Sie auf ihren mobilen Endgeräten?** (mehrfach Antwort möglich)

☐ IOs

☐ Android

☐ Windows

☐ Andere / Unbekannt

4. **Welche App nutzen Sie am meisten?**

_____

5. **Nennen Sie diejenige der von ihnen genutzten Apps, der Sie am wenigsten vertrauen.**

_____

6. **Wie oft installieren Sie neue Software auf ihren mobilen Endgeräten?**

☐ täglich

☐ wöchentlich

☐ monatlich

☐ nie

(? Hierbei ist die Neuinstallation von Applikationen gemeint und nicht das Durchführen von Updates.)

7. **Wie oft lesen Sie sich vor dem Installieren einer Software die AGBs bzw. EULAs durch?** *(bitte ankreuzen)*

   ☐ in 81% zu 100 % der Fälle

   ☐ in 61% bis 80% der Fälle

   ☐ in 41% bis 60% der Fälle

   ☐ in 21% bis 40% der Fälle

   ☐ in 1% bis 20% der Fälle

   ☐ seltener

( In diesen Fall wird unter AGBs der Text verstanden, der den Nutzer vor der Installation über die Rechte und Pflichten des Herausgebers der Applikation informiert.)

8. **Begründen Sie ihre Auswahl zu Frage 7:**

_____

9. **Im Folgenden finden Sie Gründe für nicht Befassung mit AGBs/EULAs. Bitte kreuzen Sie an, ob diese auf Sie zutreffen.**

	Trifft zu	**Trifft eher zu**	**Weder noch**	**Trifft eher nicht zu**	**Trifft nicht zu**
AGBs sind lang und zeitaufwendig	☐	☐	☐	☐	☐
AGBs sind in einer schwer verständlichen Juristensprache formuliert	☐	☐	☐	☐	☐
Die AGB muss akzeptiert werden, wenn das zugehörige Produkt benutzt werden möchte	☐	☐	☐	☐	☐
Die AGBs haben allesamt den gleichen Inhalt	☐	☐	☐	☐	☐
Vor Gericht werden erdrückende Bedingungen im Nachhinein für ungültig erklärt	☐	☐	☐	☐	☐
Die Bedingungen der Anbieter in den AGBs sind generell fair und vernünftig	☐	☐	☐	☐	☐
Ich nutze nur Apps von seriösen Anbietern, diese haben keine ökonomischen Gründe, unvernünftige oder unfaire Bedingungen anzubieten bzw. zu erzwingen	☐	☐	☐	☐	☐
Niemand liest die AGBs	☐	☐	☐	☐	☐
Ich informiere mich aus anderen Quellen (Freundeskreis, Fachzeitschriften, Blogs) über die von mir verwendeten Apps	☐	☐	☐	☐	☐

10. **Wenn Sie die AGBs näher betrachten, wie viel Zeit wenden Sie dafür auf (in Minuten)?**

10. **Wenn Sie die AGBs näher betrachten, wie viel Zeit wenden Sie dafür auf (in Minuten)?**

_____ Stunden _____ Minuten _____ Sekunden

11. **Falls Frage 7 nicht mit „nie“ beantwortet wurde. Lesen Sie die den gesamten Text oder nur bestimmte Abschnitte?**

☐ vollständig ☐ In Auszügen

12. **Begründen Sie ihre Antwort auf Frage 8:**

_____

13. **Einige Applikationen und Plattformen zeigen eine kurze Zusammenfassung der für die Applikation freigegebenen Daten und Rechte. Hat die Darstellung einer solchen Zusammenfassung Einfluss auf die Beachtung der AGBs?**

	Ja	**Nein**
Ich kenne die oben beschriebenen Zusammenfassungen.	☐	☐
Die Darbietung einer solchen Zusammenfassung hat mich dazu bewogen die jeweiligen AGBs näher zu betrachten.	☐	☐
Der Inhalt einer solchen Zusammenfassung hat mich dazu bewogen eine Applikation nicht zu installieren.	☐	☐

14. **Welche Konsequenzen könnte die Weitergabe Ihrer Daten für Sie haben?**

_____

15. **Haben Sie aufgrund der AGBs schon einmal das Installieren von Software unterlassen?**

☐ ja ☐ nein

16. **Nennen Sie bitte sinngemäße Inhalte von AGBs, die bei Ihnen bereits zu einer Unterlassung der Installation einer Applikation geführt hat.**

_____

17. **Haben Sie Bedenken, dass gewisse Applikationen bzw. deren Anbieter Ihre persönlichen Daten speichern und an Dritte weitergeben?** (mehrfach Antwort möglich)

☐ Nein

☐ Am Speichern

☐ An der Weitergabe

18. **Welche Art von persönlichen Daten auf Ihren/m mobilen Endgerät/en werden Ihrer Meinung nach weitergegeben?**

_____

_____

19. **Schätzen Sie, was für einen monetären Wert Ihre persönlichen Daten für ein Unternehmen haben.**

Alter	_____ €
Geschlecht	_____ €
Adresse	_____ €
Standortdaten	_____ €
Kontaktdaten aus dem Adressbuch	_____ €
Persönliche Bilder	_____ €
Browserchronik	_____ €

20. **Welchen Stellenwert nimmt für Sie der Schutz persönlicher Daten ein?** *(Bitte in den Leerräumen ankreuzen)*



Niedrig **Hoch**

21. **Wieviel geben Sie durchschnittlich im Monat für Applikationen für mobile Endgeräte aus?**

_____ € ☐ Keine Angabe

Anhang C. Quellcode zum Programm zur Entscheidungsfindung

```
/*
 * To change this license header, choose License Headers in Project Properties.
 * To change this template file, choose Tools | Templates
 * and open the template in the editor.
 */
package entscheidungsrs;

import ClickTroughAgreement.ClickTroughAgreement;
import java.awt.Color;
import java.awt.event.KeyEvent;
import java.util.Date;
import javax.swing.Timer;
import java.awt.event.ActionListener;
import java.awt.event.ActionEvent;
import java.io.BufferedReader;
import java.io.FileReader;
import java.io.IOException;
import java.util.ArrayList;
import java.util.Random;
import java.io.PrintWriter;
import java.io.File;

import entscheidungsrs.BegriffsPaar;
import entscheidungsrs.Result;
import entscheidungsrs.BegriffHäufigkeit;
//import ClickTroughAgreement.ClickTroughAgreement;
import java.io.FileInputStream;
import java.io.InputStreamReader;

import Config.Config;
/**
 *
 * @author Sven_ThinkPad
 */
public class EntscheidungsrsGui extends javax.swing.JFrame {
Config mConfig;
    /**
     * Creates new form EntscheidungsrsGui
     */
    public EntscheidungsrsGui() {
        initComponents();
        mConfig = new Config();
        CountdownCounter = mConfig.Countdown;
        LoadBegriffe();
    }

    int counter = 0;
    boolean countdown = false;
    int KeyPressed = 2;
    int BegriffsAnzahl;
```

```
    private Timer mTimer;
    private Timer mTimer2;
    int CountdownCounter = 10;
    long StartTime;
    //ArrayList, da diese keine festgelgete groesse bei intitalisierung brauch
    ArrayList<BegriffsPaar> BegriffsArray = new ArrayList<BegriffsPaar>();
    //ArrayList zum speichern der ergebnisse, zeit und auswahl
    ArrayList<Result> ResultArray = new ArrayList<Result>();
    //ArrayList zum speichern der Häufigkeit der Begriffsauswahl
    ArrayList<BegriffHäufigkeit> BegriffsHäufigkeitArray = new ArrayList<BegriffHäufigkeit>();
    //fonts

    /**
     * This method is called from within the constructor to initialize the form.
     * WARNING: Do NOT modify this code. The content of this method is always
     * regenerated by the Form Editor.
     */
    @SuppressWarnings("unchecked")
    // <editor-fold defaultstate="collapsed" desc="Generated Code">
    private void initComponents() {

        jPanel1 = new javax.swing.JPanel();
        lblB = new javax.swing.JLabel();
        lblA = new javax.swing.JLabel();
        jScrollPane1 = new javax.swing.JScrollPane();
        jTextArea1 = new javax.swing.JTextArea();
        lblCountdown = new javax.swing.JLabel();

        setDefaultCloseOperation(javax.swing.WindowConstants.EXIT_ON_CLOSE);
        setBackground(new java.awt.Color(0, 0, 0));
        setLocation(new java.awt.Point(0, 0));
        setSize(new java.awt.Dimension(800, 600));
        getContentPane().setLayout(new javax.swing.BoxLayout(getContentPane(),
javax.swing.BoxLayout.LINE_AXIS));

        jPanel1.setBackground(new java.awt.Color(0, 0, 0));
        jPanel1.setPreferredSize(new java.awt.Dimension(800, 600));
        jPanel1.addKeyListener(new java.awt.event.KeyAdapter() {
            public void keyPressed(java.awt.event.KeyEvent evt) {
                jPanel1KeyPressed(evt);
            }
        });

        lblB.setFont(new java.awt.Font("Calibri", 0, 48)); // NOI18N
        lblB.setForeground(new java.awt.Color(255, 255, 255));
        lblB.setHorizontalAlignment(javax.swing.SwingConstants.RIGHT);

        lblA.setFont(new java.awt.Font("Calibri", 0, 48)); // NOI18N
        lblA.setForeground(new java.awt.Color(255, 255, 255));
        lblA.setHorizontalAlignment(javax.swing.SwingConstants.LEFT);
        lblA.setToolTipText("");
```

```
        jTextArea1.setBackground(new java.awt.Color(0, 0, 0));
        jTextArea1.setColumns(20);
        jTextArea1.setRows(5);
        jTextArea1.setAutoscrolls(false);
        jTextArea1.setMargin(new java.awt.Insets(0, 0, 0, 0));
        jTextArea1.addKeyListener(new java.awt.event.KeyAdapter() {
            public void keyPressed(java.awt.event.KeyEvent evt) {
                jTextArea1KeyPressed(evt);
            }
            public void keyReleased(java.awt.event.KeyEvent evt) {
                jTextArea1KeyReleased(evt);
            }
            public void keyTyped(java.awt.event.KeyEvent evt) {
                jTextArea1KeyTyped(evt);
            }
        });
        jScrollPane1.setViewportView(jTextArea1);

        lblCountdown.setFont(new java.awt.Font("Times New Roman", 0, 36)); // NOI18N
        lblCountdown.setForeground(new java.awt.Color(255, 255, 255));
        lblCountdown.setHorizontalAlignment(javax.swing.SwingConstants.CENTER);

        javax.swing.GroupLayout jPanel1Layout = new javax.swing.GroupLayout(jPanel1);
        jPanel1.setLayout(jPanel1Layout);
        jPanel1Layout.setHorizontalGroup(
            jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
            .addGroup(javax.swing.GroupLayout.Alignment.TRAILING,
jPanel1Layout.createSequentialGroup()
                .addContainerGap(javax.swing.GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE)
                .addComponent(jScrollPane1, javax.swing.GroupLayout.PREFERRED_SIZE, 0,
javax.swing.GroupLayout.PREFERRED_SIZE)
                .addGap(1904, 1904, 1904))
            .addGroup(jPanel1Layout.createSequentialGroup()
                .addGap(25, 25, 25)

.addGroup(jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
                    .addComponent(lblCountdown, javax.swing.GroupLayout.PREFERRED_SIZE, 1131,
javax.swing.GroupLayout.PREFERRED_SIZE)
                    .addGroup(jPanel1Layout.createSequentialGroup()
                        .addComponent(lblA, javax.swing.GroupLayout.PREFERRED_SIZE, 474,
javax.swing.GroupLayout.PREFERRED_SIZE)
                        .addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED)
                        .addComponent(lblB, javax.swing.GroupLayout.PREFERRED_SIZE, 701,
javax.swing.GroupLayout.PREFERRED_SIZE)))
                .addContainerGap(javax.swing.GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE))
        );
        jPanel1Layout.setVerticalGroup(
            jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
            .addGroup(jPanel1Layout.createSequentialGroup()
                .addContainerGap()
                .addComponent(jScrollPane1, javax.swing.GroupLayout.PREFERRED_SIZE, 0,
javax.swing.GroupLayout.PREFERRED_SIZE)
```

```
            .addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED, 318,
Short.MAX_VALUE)

.addGroup(jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
                .addComponent(lblB, javax.swing.GroupLayout.Alignment.TRAILING,
javax.swing.GroupLayout.PREFERRED_SIZE, 77, javax.swing.GroupLayout.PREFERRED_SIZE)
                .addComponent(lblA, javax.swing.GroupLayout.PREFERRED_SIZE, 77,
javax.swing.GroupLayout.PREFERRED_SIZE))
            .addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED)
            .addComponent(lblCountdown, javax.swing.GroupLayout.PREFERRED_SIZE, 77,
javax.swing.GroupLayout.PREFERRED_SIZE)
            .addContainerGap(367, Short.MAX_VALUE))
        );

        getContentPane().add(jPanel1);

        pack();
        setLocationRelativeTo(null);
    }// </editor-fold>

    private void jPanel1KeyPressed(java.awt.event.KeyEvent evt) {
        // TODO add your handling code here:
        // Ueberfluessig, lässt sich aber nicht löschen weil GUI Element im Editor erst weg muss...

    }

    private void jTextArea1KeyTyped(java.awt.event.KeyEvent evt) {
        // Überschüssige Funktion, lässt sich nur im gui editor löschen
    }

    private void jTextArea1KeyReleased(java.awt.event.KeyEvent evt) {

        if(evt.getKeyCode()==KeyEvent.VK_K | evt.getKeyCode()==KeyEvent.VK_J )
        {
            if (KeyPressed == 1)
            {
                //timer damit es nicht sofort der nächsten darstellung kommt
                mTimer2= new Timer(1000, new ActionListener() {
                    @Override
                    public void actionPerformed(ActionEvent e)
                    {
                        mTimer2.stop();
                        lblA.setText("");
                        lblB.setText("");
                        //Pruefen ob Pause eingeschoben wird
                        if (CheckPause() == true)
                            {
                                lblCountdown.setText("Pause, weiter mit F1");
                            }
                            else
                            {
                                Darstellung();
```

```
                }

            }
        });
        //starte den countdown...
        KeyPressed = 2;

        mTimer2.start();
    }
  }
}

private void jTextArea1KeyPressed(java.awt.event.KeyEvent evt) {

  jTextArea1.requestFocus();
  //double time2 =System.nanoTime();
  Date time2 =new Date();
  //System.out.println(time2);
  //System.out.println(evt.getKeyCode());
  //System.out.println(new SimpleDateFormat("yyyy-MM-dd HH:mm:ss.SSS").format(time2));

  if(evt.getKeyCode()== KeyEvent.VK_SPACE)
  {
    if(countdown == false)
    {
      countdown = true;
      //Setup timer
      mTimer= new Timer(1000, new ActionListener() {
        @Override
        public void actionPerformed(ActionEvent e)
        {
          //countdown starts here
          System.out.println("Countdown");
          lblCountdown.setText(String.valueOf(CountdownCounter));
          CountdownCounter --;
          if (CountdownCounter == -1)
          {
            lblCountdown.setText("");
            mTimer.stop();
            Darstellung();
          }
        }
      });
      //Check config ob CTA angezeigt werden soll oder nicht...
      if(mConfig.ClickThroughAgreement == true)
        {
        ClickTroughAgreement mCTA = new ClickTroughAgreement();
        mCTA.setVisible(true);
        }
      //starte den countdown...
      mTimer.start();
    }
```

```
}

//Taste umd die Pause zu beenden
if(evt.getKeyCode()==KeyEvent.VK_F1)
{
   if (CheckPause() == true)
   {

     lblCountdown.setText("");
     mTimer= new Timer(1000, new ActionListener() {
         @Override
         public void actionPerformed(ActionEvent e)
         {
           mTimer.stop();
           Darstellung();
         }
     });
     mTimer.start();
   }
}

if(evt.getKeyCode()==KeyEvent.VK_J)
{
   if (KeyPressed == 0)
   {
      long time = System.nanoTime();
      long reactiontime = (time - StartTime)/1000000;
      Result mResult = new Result();
      System.out.println(reactiontime + ";" + lblB.getText() + ";" + lblA.getText());
      mResult.setReactionTime(reactiontime);
      mResult.setSelection(lblB.getText());
      mResult.setNonSelection(lblA.getText());
      lblB.setForeground(Color.GREEN);
      ResultArray.add(mResult);
      KeyPressed = 1;
   }
}

if(evt.getKeyCode()==KeyEvent.VK_K)
{
   if (KeyPressed == 0)
   {
      long time = System.nanoTime();
      long reactiontime = (time - StartTime)/1000000;
      Result mResult = new Result();
      System.out.println(reactiontime + ";" + lblA.getText() + ";" + lblB.getText());
      mResult.setReactionTime(reactiontime);
      mResult.setSelection(lblA.getText());
      mResult.setNonSelection(lblB.getText());
      lblA.setForeground(Color.GREEN);
      ResultArray.add(mResult);
      KeyPressed = 1;
```

```
      }
   }
}

private void SaveResults()
{
   System.out.println("Saving File...");
   //funktion zum speicher der ergebnisse, wer hätte das gedacht
   try{
      PrintWriter writer = new PrintWriter("result.txt", "ISO-8859-1");
      //Tabellenkopf speichern
      writer.println("Reaktionszeit;Auswahl;Nicht gewählt");
      //Schleife zum speichern der eigentlichen daten
      for(int i = 1;i <= ResultArray.size();i++)
      {
         writer.println(ResultArray.get(i-1).getReactionTime() + ";" +
            ResultArray.get(i-1).getSelection()+ ";"+
            ResultArray.get(i-1).getNonSelection()+ ";");
      }
      writer.close();
   }
   catch (IOException e)
   {
    System.out.println(e);
   }
   try
   {
      PrintWriter writerHäufigkeit = new PrintWriter("resultHaeufigkeit.txt","ISO-8859-1");
          if (BegriffsHäufigkeitArray.size() == 0)
         {
             BegriffHäufigkeit mBegriffHäufigkeit = new BegriffHäufigkeit();
             mBegriffHäufigkeit.Begriff = ResultArray.get(0).getSelection();
             mBegriffHäufigkeit.Häufigkeit = 0;
             BegriffsHäufigkeitArray.add(mBegriffHäufigkeit);

         }

      //Gehe durch alle Ergebnisse durch...
      for(int i = 1;i <= ResultArray.size();i++)
      {
         boolean BegriffAdded = false;
         //.. Und Prüfe ob  bereits ein Eintrag in Häufigkeitsarray vorliegt
         for (int n = 1; n <= BegriffsHäufigkeitArray.size();n++)
         {
            //... wenn ja erhöhe diesen eintrag um eins
            if (ResultArray.get(i-1).getSelection().equals(BegriffsHäufigkeitArray.get(n-1).Begriff))
            {
               BegriffsHäufigkeitArray.get(n-1).Häufigkeit +=1;
               BegriffAdded = true;
            }
         }
```

```
            if (BegriffAdded == false)
            {
            //... wenn nein lege ihn an
            BegriffHäufigkeit mBegriffHäufigkeit = new BegriffHäufigkeit();
            mBegriffHäufigkeit.Begriff = ResultArray.get(i-1).getSelection();
            mBegriffHäufigkeit.Häufigkeit = 1;
            BegriffsHäufigkeitArray.add(mBegriffHäufigkeit);
            }

        }

        for (int i = 1; i <= BegriffsHäufigkeitArray.size();i++)
        {
            writerHäufigkeit.println(BegriffsHäufigkeitArray.get(i-1).Begriff + ";" +
                BegriffsHäufigkeitArray.get(i-1).Häufigkeit);
        }
        writerHäufigkeit.close();
    }
    catch(IOException e)
    {
        System.out.println(e);
    }
    System.out.println("Fertig");
}
private BegriffsPaar getBegriffsPaar()
{
    //gibt ein zufällig ausgewählten begriffspaar aus, und löscht es au der liste
    BegriffsPaar mBegriff;
    if (BegriffsArray.size() >= 1)
    {
        int i = new Random().nextInt(BegriffsArray.size());
        mBegriff = BegriffsArray.get(i);
        BegriffsArray.remove(i);
        return mBegriff;
    }
    return null;
}

public boolean CheckPause()
{
//teste ob hälfte der begriffe ereicht ist, bei hälfte der begriffe -> pause
if (mConfig.Pause == true)
    {
    return BegriffsArray.size() == BegriffsAnzahl/2;
    }
else
    {
    return false;
    }
}
public void Darstellung()
{
```

```
      //bekomme ein begriffspaar
      BegriffsPaar mBegriffsPaar  = this.getBegriffsPaar();
      if (mBegriffsPaar != null)
      {
      //stelle die beiden begriffe auf den labeln da
      lblA.setForeground(Color.WHITE);
      lblB.setForeground(Color.WHITE);
      lblA.setText(mBegriffsPaar.A);
      lblB.setText(mBegriffsPaar.B);
      // erlaubt reaktion über tastatur
      KeyPressed = 0;
      //zeitpunkt der darstellung
      StartTime = System.nanoTime();

      //System.out.println(StartTime);
      }
      else
      {
        //keine begriffe mehr, alles speichern, danke sagen und schluss
          lblCountdown.setText("Vielen Dank für die Teilnahme");
          this.SaveResults();
      }




   }
   private void LoadBegriffe()
   {
     try
     {
     String filePath = new File("").getAbsolutePath() + "\\Begriffe.txt";
     File f = new File(filePath);
     BufferedReader BegriffsReader  = new BufferedReader(new InputStreamReader(new
FileInputStream(f), "ISO-8859-1"));
     System.out.println("Reading: " + filePath + "\\Begriffe.txt" );

      String line = null;

      // if no more lines the readLine() returns null
      while ((line = BegriffsReader.readLine()) != null)
         {
            //Einlesen der Datei, per Zeile. Speichern der mit ";" getrennten Begriffspaare in Array
            try
            {
            String [] BegriffsPaar = line.split(";");
            BegriffsPaar mPaar = new BegriffsPaar();
            mPaar.setBegriff(BegriffsPaar[0],BegriffsPaar[1]);
            BegriffsArray.add(mPaar);
            }
            catch(Exception e)
```

```
            {
                //damit leere zeilen ignoriert werden
            }
          }

       BegriffsAnzahl = BegriffsArray.size();
      }
      catch (IOException e) //Fehlerabfangen des Leseprozesses
      {
        //Schreib den Fehler in die Konsole
        System.out.println(e);
      }
  }

   /**
    * @param args the command line arguments
    */
   public static void main(String args[]) {
      /* Set the Nimbus look and feel */
      //<editor-fold defaultstate="collapsed" desc=" Look and feel setting code (optional) ">
      /* If Nimbus (introduced in Java SE 6) is not available, stay with the default look and feel.
       * For details see http://download.oracle.com/javase/tutorial/uiswing/lookandfeel/plaf.html
       */
      try {
          for (javax.swing.UIManager.LookAndFeelInfo info :
javax.swing.UIManager.getInstalledLookAndFeels()) {
              if ("Nimbus".equals(info.getName())) {
                  javax.swing.UIManager.setLookAndFeel(info.getClassName());
                  break;
              }
          }
      } catch (ClassNotFoundException ex) {

java.util.logging.Logger.getLogger(EntscheidungsrsGui.class.getName()).log(java.util.logging.Level.SE
VERE, null, ex);
      } catch (InstantiationException ex) {

java.util.logging.Logger.getLogger(EntscheidungsrsGui.class.getName()).log(java.util.logging.Level.SE
VERE, null, ex);
      } catch (IllegalAccessException ex) {

java.util.logging.Logger.getLogger(EntscheidungsrsGui.class.getName()).log(java.util.logging.Level.SE
VERE, null, ex);
      } catch (javax.swing.UnsupportedLookAndFeelException ex) {

java.util.logging.Logger.getLogger(EntscheidungsrsGui.class.getName()).log(java.util.logging.Level.SE
VERE, null, ex);
      }
      //</editor-fold>

      /* Create and display the form */
      java.awt.EventQueue.invokeLater(new Runnable() {
```

```
            public void run() {
                new EntscheidungsrsGui().setVisible(true);


            }
        });

    }

    // Variables declaration - do not modify
    private javax.swing.JPanel jPanel1;
    private javax.swing.JScrollPane jScrollPane1;
    private javax.swing.JTextArea jTextArea1;
    private javax.swing.JLabel lblA;
    private javax.swing.JLabel lblB;
    private javax.swing.JLabel lblCountdown;
    // End of variables declaration

}
```

Anhang D. Standardisierte Einführung zum ersten Versuch

TU Berlin | Fakultät V | IPA | FG Mensch-Maschine-Systeme |
Sek. MAR 3-1 | Marchstraße 23 | 10587 Berlin

Fakultät V Fakultät Verkehrs- und Maschinensysteme
Institut für Psychologie und Arbeitswissenschaft

Fachgebiet
Mensch-Maschine-Systeme

M. Sc. Sven Bock

Sekretariat MAR 3-1
Marchstraße 23
10587 Berlin

Telefon +49 (0)30 314-79524
Sven.Bock@mms.tu-berlin.de

Einleitung

Diese Studie beschäftigt sich mit der Entscheidungsfindung von Personen und der Analyse dieser und besteht aus einen Entscheidungsfindungsexperiment sowie einem anschließenden Fragebogen und einem kurzen Interview.

Dabei wird beim Entscheidungsfindungsexperiment jeweils ein Begriffspaar bestehend aus zwei Wörtern dargeboten. Ihre Aufgabe ist es, das für Sie favorisierende Wort auszuwählen, indem Sie den entsprechenden Knopf drücken. Mit dem linken Knopf wählen Sie den linken Begriff und mit dem rechten Knopf wählen Sie den rechten Begriff. Bei der Auswahl des favorisierenden Begriffs ist es von besonderer Relevanz wahrheitsgemäß den entsprechenden Begriff auszuwählen und sich nicht von sozialem Druck oder Moral beeinflussen zu lassen. Darüber hinaus wird von dem Teilnehmer gefordert so schnell wie möglich eine Entscheidung zu treffen. Es werden insgesamt ca. 450 Begriffspaare abgefragt. Ein Beispiel wäre „Rose“ oder „Tulpe“. Während des Experiments wird bei jedem Begriffspaar die Reaktionszeit zwischen dargebotenem Begriff und der Auswahl durch den Tastendruck gemessen. Die Begriffspaare sind dabei in Kategorien wie Musik, Religion, Politik und Weitere eingeordnet. Ziel der Studie ist es zu ermitteln, ob zwischen den Kategorien die Reaktionszeiten signifikante Unterschiede aufweisen.

Von dem Interview wird zwecks Auswertung bzw. spätere Transkription eine Tonaufnahme aufgezeichnet.

Hiermit erkläre ich mich mit den unten angeführten Punkten einverstanden und bestätige die Teilnahme an der Studie im Rahmen des oben beschriebenen Experiments

Berlin,_____ _____
Datum Unterschrift

Anhang E. Teinahmebedingungen zum ersten Versuch

Technische Universität Berlin

Teilnahmebestimmungen für das Entscheidungsexperiment
Teilnahmebestimmungen (TB)

Teilnahmebestimmungen für das Entscheidungsexperiment im Rahmen der Dissertation, welche die Thematik Sicherheit und Privatsphäre im Bereich mobiler Endgeräte behandelt.

1. Vorbemerkungen
1.1
Die nachfolgenden Bestimmungen beziehen sich auf die durch den Teilnehmenden getätigten Angaben und sind für Personen, die sich bei der Teilnahme an diesem Experiment registriert haben, verbindlich. Mit der Teilnahme erklärt der Nutzer, mit diesen Bestimmungen einverstanden zu sein.

1.2
Für die Teilnahme an diesem Experiment ist eine zuvor erlangte Volljährigkeit zwingend von Nöten.

1.3
Eine wiederholte Teilnahme an diesem Experiment ist strikt untersagt und führt bei Nichteinhaltung zum Ausschluss von diesem. Hierbei werden jegliche Daten als nichtig deklariert.

1.4
Im Rahmen der Durchführung des Experiments ist es den Teilnehmenden gestattet, bei jeglichen Unklarheiten den Versuchsleiter um weitere Informationen zu erfragen. Dem Teilnehmenden ist es jederzeit gestattet, das Experiment abzubrechen, was jedoch zur Aufhebung des Anspruchs auf die entsprechende Gegenleistung führt.

2. Teilnahme
2.1
Für die Teilnahme an diesem Experiment ist eine vollständige und wahrheitsgemäße Beantwortung des zuvor ausgehändigten Fragebogens unabdingbar. Kommt der Teilnehmende dieser Verpflichtung nicht nach, hat er sämtliche für ihn hieraus entstehende Nachteile selbst zu tragen.

2.2
Dem Teilnehmenden wird im Rahmen des Experiments eine Teilnehmernummer zugeordnet, welche auf der Reihenfolge der Teilnahme basiert.

2.3
Die abgeforderte Leistung im Rahmen des Experiments erfolgt stets nach bestem Wissen, Gewissen und höchstmöglicher Leistung.

2.4
Durch die Teilnahme am Experiment kommt ein Vertrag zwischen dem Teilnehmenden und dem Versuchsleiter zustande. Die Laufzeit des Vertrages und jeder damit zusammenhängende Erhalt der offerierten Gegenleistungen erfolgt nach dem erfolgreichen Abschluss des Experiments; der Nutzer kann die Teilnahme jederzeit selbständig beenden, verliert jedoch bei Unvollständigkeit des Experiments jeglichen Anspruch auf die eben erwähnte Gegenleistung.

3. Pflichten beider Parteien
3.1
Sowohl Teilnehmer als auch Versuchsleiter verpflichten sich zu einem rechtmäßigen Umgang mit den aus dem Experiment resultierenden Ergebnissen.

> Seite 2/4

3.2
Beide Vertragspartner versichern, im Rahmen des Experiments keine strafrechtlich relevanten Inhalte zu verbreiten sowie gegen sonstige Rechte Dritter (insbesondere gewerbliche Schutzrechte, das Wettbewerbsrecht und das allgemeine Persönlichkeitsrecht) zu verstoßen. Vor allem ist die Verbreitung von jugendgefährdenden, kinderpornografischen, extremistischen und rassistischen Inhalten untersagt.

3.3
Bei der Auswahl der Teilnehmenden am Experiment dürfen keine Benachteiligungen aus Gründen der Rasse oder wegen der ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters (mit Ausnahme von Minderjährigen) oder der sexuellen Identität erfolgen.

3.4
Der Versuchsleiter behält sich das Recht vor, bei jeder Zuwiderhandlung, Störung des Systems, artfremder oder durch diese Bedingungen untersagter Handlungen, den verantwortlichen Teilnehmer unwiderruflich und ohne Rückfrage vom Experiment auszuschließen.

3.5
Bei mutwilliger Zerstörung oder Beschädigung der vorhandenen Gerätschaften im Experimentalraum wird der Versuchsleiter im Rahmen der gesetzlichen Bestimmungen die personenbezogenen Daten an die Strafverfolgungs- und Ordnungsbehörden weitergeben. Der Verursacher wird i. S. d. § 303 StGB (Sachbeschädigung) zur Anzeige gebracht.

3.6
Der Teilnehmer stellt den Versuchsleiter von allen Ansprüchen frei, die wegen einer Verletzung dieser Bestimmungen durch den Vertragspartner gegen den Versuchsleiter erhoben werden.

4. Haftung
Haftungsansprüche gegen den Versuchsleiter, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Bearbeitung der Aufgaben innerhalb des Experiments verursacht wurden sind grundsätzlich ausgeschlossen, sofern seitens des Versuchsleiters kein nachweislich vorsätzliches oder grob fahrlässiges Verschulden vorliegt.

5. Datenschutz
5.1
Der Teilnehmer erklärt sich damit einverstanden, dass sämtliche von ihm in diesem Experiment aufgenommene Daten gemäß dem Bundesdatenschutzgesetz (BDSG) gespeichert und weiterverarbeitet werden, soweit dies für die Durchführung des Vertragsverhältnisses notwendig ist.

5.2
Der Teilnehmende nimmt zur Kenntnis, dass im Rahmen des Experiments gewonnene Informationen für die Versuchsleiter und deren Institution von besonderer Bedeutung sind und deshalb nach den geltenden Bestimmungen geschützt werden. Vor diesem Hintergrund verpflichtet sich der Teilnehmer gegenüber dem Berechtigten, alle Informationen sowie Vorgänge bei der Vorbereitung und Durchführung des Experiments vertraulich zu behandeln und ohne ausdrückliche, schriftliche Erlaubnis, nicht für eigene Zwecke zu gebrauchen, zu verwerten oder an Dritte weiterzugeben.

5.3
Darüber hinaus werden die Daten vertraulich und in Übereinstimmung mit den entsprechenden Nutzern behandelt. Eine über den hier beschriebenen Umfang hinausgehende Erhebung oder Verarbeitung von personenbezogenen Daten der Nutzer kann ohne vorherige Einwilligung seitens der Nutzer erfolgen.

> Seite 3/4

5.4
Das Sammeln von Daten und die Zusammenführung dieser mit anderen Teilnehmern erfolgt mit dem Ziel, eine statistische Auswertung durchzuführen und die daraus zu verwendenden Ergebnisse zu veröffentlichen. Zudem erfolgt eine Weitergabe von Daten an Dritte, in dem Umfang, wie es erforderlich ist (insbesondere Alter, Geschlecht); im Übrigen bestimmt jeder Nutzer mit, in welchem Umfang er seine persönlichen Daten an Dritte weitergibt. Dabei kann die Höhe der Gegenleistung variieren.

5.5
Die Daten werden nur solange aufbewahrt, wie es im Rahmen dieser Vereinbarung und unter Einhaltung des anwendbaren Rechts erforderlich ist.

5.6
Der Teilnehmer ist über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung der erforderlichen personenbezogenen Daten ausführlich unterrichtet worden. Der Teilnehmer stimmt dieser Datenverarbeitung mit der Teilnahme am Experiment ausdrücklich zu.

6. Schlussbestimmungen
6.1
Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland.

6.2
Als Erfüllungsort für alle beiderseitigen, aus dem Vertrag geschuldeten Leistungen, wird Berlin vereinbart.

6.3
Sollte eine oder mehrere Bestimmungen dieser Vereinbarung unwirksam sein oder werden, so wird die Wirksamkeit der Vereinbarung im Übrigen nicht davon berührt.

Anhang F. Liste der Begriffspaare

1. Android;IOS

2. Windows;Linux
3. Windows;MacOS
4. MacOS;Linux

5. Großstadt;Kleinstadt
6. Land;Stadt

7. Geld;Jobzufriedenheit
8. Karriere;Familie
9. Single;Beziehung

10. Umwelt;Luxus

11. Auto;Fahrrad
12. Auto;S-Bahn
13. Auto;U-Bahn
14. Auto;Zug
15. Auto;Flugzeug
16. U-Bahn;S-Bahn

17. Wohnung;Haus
18. Balkon;Terrasse
19. Dusche;Badewanne

20. Berlin;Hamburg
21. Berlin;Köln
22. Berlin;München
23. Hamburg;Köln
24. Hamburg;München
25. Köln;München

26. Berge;Küste
27. Winter;Sommer
28. Frühling;Herbst
29. Herbst;Sommer
30. Herbst;Winter
31. Frühling;Sommer
32. Frühling;Winter

33. Preis;Qualität
34. sparsam;bequem

35. Lidl;Edeka
36. Lidl;Aldi
37. Lidl;Kaufland
38. Kaufland;Aldi
39. Kaufland;Edeka
40. Edeka;Aldi

41. Marke;Noname

42. Pesto;Tomatensoße
43. Kaffee;Tee
44. Pasta;Pizza
45. Rotwein;Weißwein

46. ARD;ZDF
47. Öffentliche-Rechtliche;Private
48. Free-TV;Pay-TV

49. Online-Banking;Bankautomat
50. Stationärer Handel;Amazon
51. Visa;Mastercard
52. Paypal;Bankeinzug

53. DHL;Hermes
54. DHL;UPS
55. Hermes;UPS
56. DHL;FedEx
57. Hermes;FedEx
58. UPS;FeDex

59. Kombi;Limousine
60. Kombi;Coupé
61. Limousine;Coupé
62. Kombi;Cabrio
63. Cabrio;Coupé
64. Cabrio;Limousine

65. Audi;BMW
66. Audi;Ford
67. Audi;Honda
68. Audi;Mercedes-Benz
69. Audi;Opel
70. Audi;Porsche
71. Audi;Skoda
72. Audi;Volkswagen

73. BMW;Ford
74. BMW;Honda
75. BMW;Mercedes-Benz
76. BMW;Opel
77. BMW;Porsche
78. BMW;Skoda
79. BMW;Volkswagen

80. Ford;Honda
81. Ford;Mercedes-Benz
82. Ford;Opel
83. Ford;Porsche
84. Ford;Skoda
85. Ford;Volkswagen

86. Honda;Mercedes-Benz
87. Honda;Opel
88. Honda;Porsche
89. Honda;Skoda
90. Honda;Volkswagen

91. Mercedes-Benz;Opel
92. Mercedes-Benz;Porsche
93. Mercedes-Benz;Skoda
94. Mercedes-Benz;Volkswagen

95. Opel;Porsche
96. Opel;Skoda
97. Opel;Volkswagen

98. Porsche;Skoda
99. Porsche;Volkswagen

100. Skoda;Volkswagen

101. Apfel;Banane
102. Apfel;Birne
103. Apfel;Orange
104. Apfel;Erdbeere
105. Apfel;Ananas

106. Apfel;Himbeere
107. Apfel;Kokusnuss
108. Apfel;Kirschen

109. Banane;Birne
110. Banane;Orange
111. Banane;Erdbeere
112. Banane;Ananas
113. Banane;Himbeere
114. Banane;Kokusnuss
115. Banane;Kirschen

116. Birne;Orange
117. Birne;Erdbeere
118. Birne;Ananas
119. Birne;Himbeere
120. Birne;Kokusnuss
121. Birne;Kirschen

122. Orange;Erdbeere
123. Orange;Ananas
124. Orange;Himbeere
125. Orange;Kokusnuss
126. Orange;Kirschen

127. Erdbeere;Ananas
128. Erdbeere;Himbeere
129. Erdbeere;Kokusnuss
130. Erdbeere;Kirschen

131. Ananas;Himbeere
132. Ananas;Kokusnuss
133. Ananas;Kirschen

134. Himbeere;Kokusnuss
135. Himbeere;Kirschen

136. Kokusnuss;Kirschen

137. Adidas;Nike
138. Adidas;Puma
139. Adidas;Lacoste
140. Adidas;Boss
141. Adidas;Converse
142. Adidas;Levis
143. Adidas;Calvin Klein
144. Adidas;Esprit

145. Nike;Puma
146. Nike;Lacoste
147. Nike;Boss
148. Nike;Converse
149. Nike;Levis
150. Nike;Calvin Klein
151. Nike;Esprit

152. Puma;Lacoste
153. Puma;Boss
154. Puma;Converse
155. Puma;Levis
156. Puma;Calvin Klein
157. Puma;Esprit

158. Lacoste;Boss
159. Lacoste;Converse
160. Lacoste;Levis
161. Lacoste;Calvin Klein
162. Lacoste;Esprit

163. Boss;Converse
164. Boss;Levis
165. Boss;Calvin Klein
166. Boss;Esprit

167. Converse;Levis
168. Converse;Calvin Klein
169. Converse;Esprit

170. Levis;Calvin Klein
171. Levis;Esprit

172. Calvin Klein;Esprit

173. Belgien;Deutschland
174. Belgien;Frankreich
175. Belgien;Niederlande
176. Belgien;Österreich
177. Belgien;Schweiz
178. Belgien;Schweden
179. Belgien;Dänemark
180. Belgien;Norwegen
181. Belgien;Großbritannien

182. Deutschland;Frankreich
183. Deutschland;Niederlande
184. Deutschland;Österreich
185. Deutschland;Schweiz
186. Deutschland;Schweden
187. Deutschland;Dänemark
188. Deutschland;Norwegen
189. Deutschland;Großbritannien

190. Frankreich;Niederlande
191. Frankreich;Österreich
192. Frankreich;Schweiz
193. Frankreich;Schweden
194. Frankreich;Dänemark
195. Frankreich;Norwegen
196. Frankreich;Großbritannien

197. Niederlande;Österreich
198. Niederlande;Schweiz
199. Niederlande;Schweden
200. Niederlande;Dänemark
201. Niederlande;Norwegen
202. Niederlande;Großbritannien

203. Österreich;Schweiz
204. Österreich;Schweden
205. Österreich;Dänemark
206. Österreich;Norwegen
207. Österreich;Großbritannien

208. Schweiz;Schweden
209. Schweiz;Dänemark
210. Schweiz;Norwegen
211. Schweiz;Großbritannien

212. Schweden;Dänemark
213. Schweden;Norwegen
214. Schweden;Großbritannien

215. Dänemark;Norwegen
216. Dänemark;Großbritannien

217. Norwegen;Großbritannien

218. Europa;Asien
219. Europa;Nordamerika
220. Europa;Südamerika
221. Europa;Afrika
222. Europa;Ozeanien

223. Asien;Nordamerika
224. Asien;Südamerika
225. Asien;Afrika
226. Asien;Ozeanien

227. Nordamerika;Südamerika
228. Nordamerika;Afrika
229. Nordamerika;Ozeanien

230. Südamerika;Afrika
231. Südamerika;Ozeanien

232. Afrika;Ozeanien

233. Atheismus;Judentum
234. Atheismus;Islam
235. Atheismus;Buddhismus
236. Atheismus;Hinduismus
237. Atheismus;Katholizismus
238. Atheismus;Protestantismus

239. Judentum;Islam
240. Judentum;Buddhismus
241. Judentum;Hinduismus
242. Judentum;Katholizismus
243. Judentum;Protestantismus

244. Islam;Buddhismus
245. Islam;Hinduismus
246. Islam;Katholizismus
247. Islam;Protestantismus

248. Buddhismus;Hinduismus
249. Buddhismus;Katholizismus
250. Buddhismus;Protestantismus

251. Hinduismus;Katholizismus
252. Hinduismus;Protestantismus

253. Katholizismus;Protestantismus

254. CDU;SPD
255. CDU;Grüne
256. CDU;CSU
257. CDU;Linke
258. CDU;AFD
259. CDU;NPD
260. CDU;Piraten Partei
261. CDU;FDP

262. SPD;Grüne
263. SPD;CSU
264. SPD;Linke
265. SPD;AFD
266. SPD;NPD
267. SPD;Piraten Partei
268. SPD;FDP

269. Grüne;CSU
270. Grüne;Linke
271. Grüne;AFD
272. Grüne;NPD
273. Grüne;Piraten Partei
274. Grüne;FDP

275. CSU;Linke
276. CSU;AFD
277. CSU;NPD
278. CSU;Piraten Partei
279. CSU;FDP

280. Linke;AFD
281. Linke;NPD
282. Linke;Piraten Partei
283. Linke;FDP

284. AFD;NPD
285. AFD;Piraten Partei
286. AFD;FDP

287. NPD;Piraten Partei
288. NPD;FDP

289. Piraten Partei;FDP

290. ARD;ZDF
291. ARD;RBB
292. ARD;Phoenix
293. ARD;ProSieben
294. ARD;Sat. 1
295. ARD;RTL
296. ARD;RTL 2
297. ARD;Arte

298. ZDF;RBB
299. ZDF;Phoenix
300. ZDF;ProSieben
301. ZDF;Sat. 1
302. ZDF;RTL
303. ZDF;RTL 2
304. ZDF;Arte

305. RBB;Phoenix
306. RBB;ProSieben
307. RBB;Sat. 1
308. RBB;RTL
309. RBB;RTL 2
310. RBB;Arte

311. Phoenix;Sat. 1
312. Phoenix;RTL
313. Phoenix;RTL 2
314. Phoenix;Arte

315. ProSieben;Sat. 1
316. ProSieben;RTL
317. ProSieben;RTL 2
318. ProSieben;Arte

319. Sat. 1;RTL
320. Sat. 1;RTL 2
321. Sat. 1;Arte

322. RTL;RTL 2

323. RTL;Arte

324. RTL 2;Arte

325. Entspannen;Sport
326. Entspannen;Schlafen
327. Entspannen;Arbeiten
328. Entspannen;Feiern
329. Entspannen;Spazieren gehen
330. Entspannen;Freunde treffen
331. Entspannen;Kino
332. Entspannen;Theater
333. Entspannen;Konzert
334. Entspannen;Festival

335. Sport;Schlafen
336. Sport;Arbeiten
337. Sport;Feiern
338. Sport;Spazieren gehen
339. Sport;Freunde treffen
340. Sport;Kino
341. Sport;Theater
342. Sport;Konzert
343. Sport;Festival

344. Schlafen;Arbeiten
345. Schlafen;Feiern
346. Schlafen;Spazieren gehen
347. Schlafen;Freunde treffen
348. Schlafen;Kino
349. Schlafen;Theater
350. Schlafen;Konzert
351. Schlafen;Festival

352. Arbeiten;Feiern
353. Arbeiten;Spazieren gehen
354. Arbeiten;Freunde treffen
355. Arbeiten;Kino
356. Arbeiten;Theater
357. Arbeiten;Konzert
358. Arbeiten;Festival

359. Feiern;Spazieren gehen
360. Feiern;Freunde treffen
361. Feiern;Kino
362. Feiern;Theater
363. Feiern;Konzert
364. Feiern;Festival

365. Spazieren gehen;Freunde treffen
366. Spazieren gehen;Kino
367. Spazieren gehen;Theater
368. Spazieren gehen;Konzert
369. Spazieren gehen;Festival

370. Freunde treffen;Kino
371. Freunde treffen;Theater
372. Freunde treffen;Konzert
373. Freunde treffen;Festival

374. Kino;Theater
375. Kino;Konzert
376. Kino;Festival

377. Theater;Konzert
378. Theater;Festival

379. Konzert;Festival

380. Rock;Techno
381. Rock;Pop
382. Rock;Indie
383. Rock;Metal
384. Rock;Jazz
385. Rock;Klassik
386. Rock;Hip Hop
387. Rock;Reggae
388. Rock;Punk

389. Techno;Pop
390. Techno;Indie
391. Techno;Metal
392. Techno;Jazz
393. Techno;Klassik
394. Techno;Hip Hop
395. Techno;Reggae
396. Techno;Punk

397. Pop;Indie
398. Pop;Metal
399. Pop;Jazz
400. Pop;Klassik
401. Pop;Hip Hop
402. Pop;Reggae
403. Pop;Punk

404. Indie;Metal
405. Indie;Jazz
406. Indie;Klassik
407. Indie;Hip Hop
408. Indie;Reggae
409. Indie;Punk

410. Metal;Jazz
411. Metal;Klassik
412. Metal;Hip Hop
413. Metal;Reggae
414. Metal;Punk

415. Jazz;Klassik
416. Jazz;Hip Hop
417. Jazz;Reggae
418. Jazz;Punk

419. Klassik;Hip Hop
420. Klassik;Reggae
421. Klassik;Punk

422. Hip Hop;Reggae
423. Hip Hop;Punk

424. Reggae;Punk

Anhang G. Dokument zur Weitergabe der Daten

TU Berlin | Fakultät V | IPA | FG Mensch-Maschine-Systeme |
Sek. MAR 3-1 | Marchstraße 23 | 10587 Berlin

Fakultät V Fakultät Verkehrs- und Maschinensysteme
Institut für Psychologie und Arbeitswissenschaft

Fachgebiet
Mensch-Maschine-Systeme

M. Sc. Sven Bock

Sekretariat MAR 3-1
Marchstraße 23
10587 Berlin

Telefon +49 (0)30 314-79524
Sven.Bock@mms.tu-berlin.de

Liebe Versuchsteilnehmer,

die in diesem psychologischen Experiment gewonnenen Resultate dienen der Analyse der Entscheidungsfindung. Aufgrund der Tatsache, dass viele Institutionen und Unternehmen sich mit diesem Thema beschäftigen, welches eine immer größere Rolle spielt, hätten auch diese ein Interesse an der Nutzung Ihrer Daten. Sie können natürlich selber entscheiden, ob und wem Sie Einsicht in Ihre Daten gewähren wollen und werden dafür natürlich entsprechend kompensiert. Die Daten werden ausschließlich anonym übermittelt und die meisten Universitäten sind Partneruniversitäten der Technischen Universität Berlin oder andere Berliner Universitäten. Der Rückseite können Sie entnehmen, welche Institutionen und Unternehmen Teil der jeweiligen Verbunde sind. Sollten sie sich für keinen Verbund entscheiden werden die Daten ausschließlich für mein Promotionsvorhaben verwendet.

Meine Daten sollen nicht an Dritte weitergegeben werden. 2 €	◯
Verbund 1: Universitäten in Berlin 3 €	◯
Verbund 2: Universitäten und Marktforschungsunternehmen mit Sitz in Berlin 5 €	◯
Verbund 3: nationale Universitäten 6 €	◯
Verbund 4: Nationale Universitäten und Marktforschungsunternehmen 8 €	◯
Verbund 5: Internationale Universitäten 9 €	◯
Verbund 6: Internationale Universitäten und Marktforschungsunternehmen 10 €	◯

Verbund 1: Universitäten in Berlin ○ Technische Universität Berlin ○ Humboldt Universität Berlin ○ Freie Universität Berlin ○ Beuth-Hochschule
Verbund 2: Universitäten und Marktforschungsunternehmen mit Sitz in Berlin ○ Verbund 1 ○ Fraunhofer ○ BrainEffect: ○ Green City Solution ○ Ecoligo
Verbund 3: nationale Universitäten ○ Verbund 1 ○ RWTH Aachen ○ Universität zu Köln ○ Julius-Maximilians-Universität Würzburg ○ Philipps Universität Marburg
Verbund 4: Nationale Universitäten und Marktforschungsunternehmen ○ Verbund 2 & 3 ○ Spiegel Institut ○ MindTake Research GmbH ○ AMR Advanced Market Research GmbH ○ GIM Gesellschaft für Innovative Marktfoschung
Verbund 5: Internationale Universitäten ○ Verbund 3 ○ Universität Wien ○ Universidad de Santiago de Compostela ○ University of Calgary ○ University of Southern California (USC)
Verbund 6: Internationale Universitäten und Marktforschungsunternehmen ○ Verbund 4 & 5 ○ Nielsen Media Research ○ YouGov ○ Quantifica ○ Research International

Anhang H. Interviewfragen

1. Waren Sie während des Versuchs durch etwas verunsichert? Wenn ja, was?
2. Ist Ihnen etwas merkwürdig vorgekommen?
3. Haben Sie sich die Teilnahmevereinbarung durchgelesen?
4. Ist Ihnen beim Durchlesen der AGBs etwas aufgefallen?
5. Haben Sie beim Unterzeichnen der Einverständniserklärung gezögert?
6. Hatten Sie während des Experiments ein Gefühl von Unwohlsein beim Preisgeben persönlicher Präferenzen?

Anhang I. Aufklärung

TU Berlin | Fakultät V | IPA | FG Mensch-Maschine-Systeme |
Sek. MAR 3-1 | Marchstraße 23 | 10587 Berlin

Fakultät V Fakultät Verkehrs- und Maschinensysteme
Institut für Psychologie und Arbeitswissenschaft

Fachgebiet
Mensch-Maschine-Systeme

M. Sc. Sven Bock

Sekretariat MAR 3-1
Marchstraße 23
10587 Berlin

Telefon +49 (0)30 314-79524
Sven.Bock@mms.tu-berlin.de

Aufklärung über die Zielsetzung des Experimentes

Teilnehmercode: _____

Sehr geehrte Damen und Herren,

in den soeben durchgeführten Versuch wurden weder persönlichkeitsmerkmale noch die getroffenen Entscheidungen gespeichert, auch werden keine Daten an dritte Weitergegeben. Das eigentliche Ziel war es den Umgang mit persönlichen Daten ihrerseits näher zu betrachten. Im Fokus lag hierbei der Umgang mit den Teilnahmebestimmungen und der Weitergabe von Daten, hierbei wurde gemessen wieviel Zeit sie für die Teilnahmebestimmungen aufgewandt haben, ob sie bereit waren ihre Daten gegen einen monetären Wert an Dritte weiterzugeben und ob sie bei dem Einverständnis beider Dokumente Unsicherheiten gezeigt haben. Die Täuschung erfolgte aus dem Grund, dass bei direkten Befragungen zum Thema Datenschutz, diesen regelmäßig ein hoher Stellenwert zugeschrieben wird, das tatsächliche Verhalten aber häufig davon abweicht.

Ich wurde darüber in Kenntnis gesetzt, dass die während der Studie gesammelten Audio- und Sensordaten sowie die Angaben der Fragebögen, werden zur Auswertung herangezogen. Die Tonaufnahmen werden nach erfolgter Transkription des Interviews gelöscht. Die generierten, anonymisierten Daten werden für die Erstellung von wissenschaftlichen Forschungsarbeiten benutzt. Diese Arbeiten werden veröffentlicht. Aus rechtlichen Gründen werden die Daten bis zu zehn Jahren aufbewahrt. Bei Bedarf hat der Teilnehmer die Möglichkeit eine Anfrage auf die Löschung seiner Daten zu stellen, welcher umgehend nachgegangen wird.

Sollten sie Einwände gegen die erläuterte Verwendung ihrer Daten haben, so werden diese umgehend gelöscht.

Unabhängig hiervon und von ihrer Auswahl bei der Weitergabe ihrer Daten erhalten sie eine Gegenleistung von 10 Euro oder 1 Versuchspersonenstunde.

Hiermit bestätige dich die Aufklärung über das Experiment erhalten zu haben und willige der Verwendung der Daten zu:

Berlin, _____ _____
Datum Unterschrift Versuchsteilnehmer

Anhang J. Tabellen zum ersten Versuch

Tabelle 2 *Mann-Whitney-U-Test gemessene Lesedauer und Präsentationsform*

Ränge				
	Präsentationsform	H	Mittlerer Rang	Summe der Ränge
Gemessene Lesedauer	Papier	26	27,73	721,00
	CTA	25	24,20	605,00
	Gesamtsumme	51		

Teststatistiken[a]	
	Gemessene Lesedauer
Mann-Whitney-U-Test	280,000
Wilcoxon-W	605,000
Z	-,850
Asymp. Sig. (2-seitig)	,395

a. Gruppierungsvariable: Präsentationsform

Tabelle 3 *T-Test der gemessenen Lesedauer und Präsentationsform*

		Test bei unabhängigen Stichproben								
		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Gemessene Lesedauer	Varianzgleichheit angenommen	,075	,786	,427	49	,671	6,32577	14,82270	-23,46157	36,11311
	Varianzgleichheit nicht angenommen			,427	48,978	,671	6,32577	14,81708	-23,45059	36,10213

Tabelle 4 *Mann-Whitney-U-Test gemessene Lesedauer und Geschlecht*

Ränge

	Geschlecht	H	Mittlerer Rang	Summe der Ränge
Gemessene Lesedauer	Männlich	20	21,85	437,00
	Weiblich	31	28,68	889,00
	Gesamtsumme	51		

Teststatistiken[a]

	Gemessene Lesedauer
Mann-Whitney-U-Test	227,000
Wilcoxon-W	437,000
z	-1,606
Asymp. Sig. (2-seitig)	,108

a. Gruppierungsvariable: Geschlecht

Tabelle 5 *T-Test gemessene Lesedauer und Geschlecht*

		Test bei unabhängigen Stichproben								
		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Gemessene Lesedauer	Varianzgleichheit angenommen	3,202	,080	-1,664	49	,102	-24,61885	14,79293	-54,34636	5,10865
	Varianzgleichheit nicht angenommen			-1,734	45,884	,090	-24,61885	14,19527	-53,19439	3,95668

Tabelle 6 *Mann-Whitney-U-Test der Gruppe, die soziale Medien häufig nutzt, und der Lesedauer*

Ränge

	Gruppe, die Social Media Applikationen am häufigsten nutzt	H	Mittlerer Rang	Summe der Ränge
Gemessene Lesedauer	Nein	46	26,17	1204,00
	Ja	5	24,40	122,00
	Gesamtsumme	51		

Teststatistiken[a]

	MES_Lesedauer
Mann-Whitney-U-Test	107,000
Wilcoxon-W	122,000
z	-,254
Asymp. Sig. (2-seitig)	,799
Exakte Sig. [2*(1-seitige Sig.)]	,818[b]

a. Gruppierungsvariable: Dazu gehören Facebook & Instagram

b. Nicht für Bindungen korrigiert.

Tabelle 7 *Mann-Whitney-U-Test der Gruppe, die Messenger-Applikationen häufig nutzt, und Lesedauer*

Ränge

	Gruppe, die Messenger-Applikationen am häufigsten nutzt	H	Mittlerer Rang	Summe der Ränge
Gemessene Lesedauer	Nein	31	25,39	787,00
	Ja	20	26,95	539,00
	Gesamtsumme	51		

Teststatistiken[a]

	MES_Lesedauer
Mann-Whitney-U-Test	291,000
Wilcoxon-W	787,000
z	-,368
Asymp. Sig. (2-seitig)	,713

a. Gruppierungsvariable: Dazu gehören WhatsApp, Facebook Messenger, Threema, Telegram, Signal, Wire, Viber

Tabelle 8 *Korrelationen zwischen Alter und Lesedauer*

Korrelationen				
			Gemessene Lesedauer	Alter
Spearman-Rho	Gemessene Lesedauer	Korrelationskoeffizient	1,000	-,201
		Sig. (2-seitig)	.	,156
		N	51	51

Tabelle 9 *Korrelationen zwischen gewählter Vergütung und gemessener Lesedauer*

Korrelationen				
			Gemessene Lesedauer	Gewählte Vergütung
Spearman-Rho	Gemessene Lesedauer	Korrelationskoeffizient	1,000	,200
		Sig. (2-seitig)	.	,159
		N	51	51

Tabelle 10 *Korrelation zwischen gemessener Lesedauer und Häufigkeit des Lesens der AGB vor der Installation einer Software*

Korrelationen				
			Gemessene Lesedauer	Häufigkeit des Lesens
Spearman-Rho	Gemessene Lesedauer	Korrelationskoeffizient	1,000	-,084
		Sig. (2-seitig)	.	,556
		N	51	51

Tabelle 11 *Korrelationen zwischen den Begründungen für das Unterlassen des Lesens der AGBs und der gemessenen Lesedauer*

Korrelationen

		Lesedauer	Vertrauen	Keine Motivation	Zustimmung in jedem Fall erforderlich	Zu Komplizierte Sprache	Zu lang	Text immer gleich
Lesedauer	Pearson-Korrelation	1	,275	,173	-,052	TB	,156	-,061
	Sig. (2-seitig)		,051	,225	,719	,017	,273	,671
	N	51	51	51	51	51	51	51

*. Korrelation ist bei Niveau 0,05 signifikant (zweiseitig)

Tabelle 12 *Korrelationen zwischen den Begründungen für das Lesen der AGBs und der gemessenen Lesedauer*

Korrelationen

		Lesedauer	Kontrolle	Kosten	Datenschutz	Bei Misstrauen	Gewissen beruhigen
Lesedauer	Pearson-Korrelation	1	-,250	,211	-,209	-,239	.[a]
	Sig. (2-seitig)		,077	,138	,140	,092	,000
	N	51	51	51	51	51	51

a. Kann nicht berechnet werden, da mindestens eine der Variablen konstant ist

Tabelle 13 *Wilcoxon-Test für gemessene Lesedauer der Teilnahmevereinbarungen, die im Fragebogen angegebene Lesedauer und die im Interview geschätzte Lesedauer*

Ränge				
		H	Mittlerer Rang	Summe der Ränge
Geschätzte Lesedauer Interview – Gemessene Lesedauer	Negative Ränge	6[a1]	5,50	33,00
	Positive Ränge	40[b1]	26,20	1048,00
	Bindungen	0[c1]		
	Gesamtsumme	46		
Gemessene Lesedauer - Angegebene Lesedauer Fragebogen	Negative Ränge	5[d]	13,40	67,00
	Positive Ränge	39[e]	23,67	923,00
	Bindungen	0[f]		
	Gesamtsumme	44		
Geschätzte Lesedauer Interview - Angegebene Lesedauer Fragebogen	Negative Ränge	11[a]	12,73	140,00
	Positive Ränge	20[b]	17,80	356,00
	Bindungen	9[c]		
	Gesamtsumme	40		

a1. Geschätzte Lesedauer Interview < Gemessene Lesedauer; a2. Gemessene Lesedauer < Angegebene Lesedauer Fragebogen; a. Geschätzte Lesedauer Interview < Angegebene Lesedauer Fragebogen

b1. Geschätzte Lesedauer Interview > Gemessene Lesedauer; b2. Gemessene Lesedauer > Angegebene Lesedauer Fragebogen; b3. Geschätzte Lesedauer Interview > Angegebene Lesedauer Fragebogen

c1. Geschätzte Lesedauer Interview = Gemessene Lesedauer; c2. Gemessene Lesedauer = Angegebene Lesedauer Fragebogen; c3. Geschätzte Lesedauer Interview = Angegebene Lesedauer Fragebogen

Teststatistiken[a]			
	Geschätzte Lesedauer Interview – Gemessene Lesedauer	Gemessene Lesedauer - Angegebene Lesedauer Fragebogen	Geschätzte Lesedauer Interview - Angegebene Lesedauer Fragebogen
z	-5,545[b]	-4,995[c]	-2,119[c]
Asymp. Sig. (2-seitig)	,000	,000	,034

a. Wilcoxon-Test

b. Basierend auf negativen Rängen.

c. Basierend auf positiven Rängen.

Tabelle 14 *Korrelationen Alter und Nutzung von verschiedenen Applikationen*

Korrelationen		
	Applikation, die am meisten genutzt wird	Alter
Sonstige Aggregiert	Pearson-Korrelation	.[a]
	Sig. (2-seitig)	.
	N	13
Nachrichten Aggregiert	Pearson-Korrelation	.[a]
	Sig. (2-seitig)	.
	N	5
Wetter Aggregiert	Pearson-Korrelation	.[a]
	Sig. (2-seitig)	.
	N	4
Email Apps Aggregiert	Pearson-Korrelation	.[a]
	Sig. (2-seitig)	.
	N	5
Browser Aggregiert	Pearson-Korrelation	.[a]
	Sig. (2-seitig)	.
	N	6
Kartendienste Aggregiert	Pearson-Korrelation	,018
	Sig. (2-seitig)	,861
	N	97
Messenger Aggregiert	Pearson-Korrelation	-,229*
	Sig. (2-seitig)	,024
	N	97
SocialMedia Aggregiert	Pearson-Korrelation	-,172
	Sig. (2-seitig)	,092
	N	97
Keine	Pearson-Korrelation	.[a]
	Sig. (2-seitig)	.
	N	7

[a].Kann nicht berechnet werden, da mindestens eine der Variablen konstant ist

Tabelle 15 *T-Test Alter und Zeitpunkt der Unterschrift*

		Test bei unabhängigen Stichproben								
		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Alter	Varianzgleichheit angenommen	1,129	,299	-,228	24	,822	-1,013	4,440	-10,176	8,151
	Varianzgleichheit nicht angenommen			-,245	23,273	,808	-1,013	4,127	-9,545	7,520

Tabelle 16 *Korrelationen zwischen Geschlecht und Zeitpunkt der Unterschrift*

Korrelationen			
		Geschlecht	Unterschrift nach Lesen
Geschlecht	Pearson-Korrelation	1	,098
	Sig. (2-seitig)		,635
	N	97	26
Unterschrift nach Lesen	Pearson-Korrelation	,098	1
	Sig. (2-seitig)	,635	
	N	26	26

Tabelle 17 *Mann-Whitney-U-Test Zeitpunkt der Unterschrift und Lesedauer*

Ränge				
	MES_Unterschrift_Vorm_Lesen	H	Mittlerer Rang	Summe der Ränge
Gemessene Lesedauer	VorUnterschriftGelesen	10	16,85	168,50
	NachUnterschriftGelesen	16	11,41	182,50
	Gesamtsumme	26		

Teststatistiken[a]	
	MES_Lesedauer
Mann-Whitney-U-Test	46,500
Wilcoxon-W	182,500
z	-1,766
Asymp. Sig. (2-seitig)	,077
Exakte Sig. [2*(1-seitige Sig.)]	,077[b]

a. Gruppierungsvariable: MES_Unterschrift_Vorm_Lesen

b. Nicht für Bindungen korrigiert.

Tabelle 18 *Mann-Whitney-U-Test Vergütung in Euro und Geschlecht*

Ränge

	Geschlecht	H	Mittlerer Rang	Summe der Ränge
Gewählte Vergütung	Männlich	20	27,05	541,00
	Weiblich	31	25,32	785,00
	Gesamtsumme	51		

Teststatistiken[a]

	Gewählte Vergütung
Mann-Whitney-U-Test	289,000
Wilcoxon-W	785,000
z	-,678
Asymp. Sig. (2-seitig)	,498

a. Gruppierungsvariable: Geschlecht

Tabelle 19 *Korrelationen zwischen Vergütung in Euro und Alter*

Korrelationen				
			Alter	Gewählte Vergütung
Spearman-Rho	Alter:	Korrelationskoeffizient	1,000	-,112
		Sig. (2-seitig)	.	,434
		N	51	51
	Gewählte Vergütung	Korrelationskoeffizient	-,112	1,000
		Sig. (2-seitig)	,434	.
		N	51	51

Tabelle 20 *Mann-Whitney-U-Test Vergütung und Präsentationsform*

Ränge				
	Präsentationsform	H	Mittlerer Rang	Summe der Ränge
Gewählte Vergütung	Papier	26	27,48	714,50
	CTA	25	24,46	611,50
	Gesamtsumme	51		

Teststatistiken[a]	
	Gewählte Vergütung
Mann-Whitney-U-Test	286,500
Wilcoxon-W	611,500
z	-1,214
Asymp. Sig. (2-seitig)	,225

a. Gruppierungsvariable: MES_CTA

Tabelle 21 *Mann-Whitney-U-Test Vergütung in Euro und Zeitpunkt der Unterschrift*

Ränge

	Unterschrift nach Lesen	H	Mittlerer Rang	Summe der Ränge
Gewählte Vergütung	Vor der Unterschrift gelesen	10	13,15	131,50
	Nach der Unterschrift gelesen	16	13,72	219,50
	Gesamtsumme	26		

Teststatistiken[a]

	Gewählte Vergütung
Mann-Whitney-U-Test	76,500
Wilcoxon-W	131,500
z	-,399
Asymp. Sig. (2-seitig)	,690
Exakte Sig. [2*(1-seitige Sig.)]	,856[b]

a. Gruppierungsvariable: Unterschrift nach Lesen

b. Nicht für Bindungen korrigiert.

Tabelle 22 *Mann-Whitney-U-Test für Vergütung in Euro und Nutzung verschiedener Applikationsgruppen*

Ränge

Messenger		H	Mittlerer Rang	Summe der Ränge
Vergütung	Nein	31	24,53	760,50
	Ja	20	28,28	565,50
	Gesamtsumme	51		

Social Media		H	Mittlerer Rang	Summe der Ränge
Vergütung	Nein	46	26,76	1231,00
	Ja	5	19,00	95,00
	Gesamtsumme	51		

Teststatistiken[a]

Gruppierungsvariable	Vergütung	
	Messenger	Social Media
Mann-Whitney-U-Test	264,5	80
Wilcoxon-W	760,5	95
z	-1,469	-1,856
Asymp. Sig. (2-seitig)	0,142	0,064
Exakte Sig. [2*(1-seitige Sig.)]		,284[b]

a. Gruppierungsvariable: Vergütung
b. Nicht für Bindungen korrigiert.

Tabelle 23 *Korrelationen Vergütung und Begründung für Häufigkeiten des Lesens der AGBs*

Korrelationen

		Gewählte Vergütung	Nicht gelesen: Vertrauen	Nicht gelesen: Keine Motivation	Nicht gelesen: Muss Zugestimmt Werden	Nicht gelesen: Zu Komplizierte Sprache	Nicht gelesen: Zu Lang	Nicht gelesen: Text Immer Gleich	Gelesen: Kontrolle	Gelesen: Kosten	Gelesen: Datenschutz	Gelesen: Bei Misstrauen	Gelesen: Gewissen Beruhigen
Gewählte Vergütung	Pearson-Korrelation	1	,037	,069	,053	,089	-,018	,079	-,293*	,096	,013	,077	.b
	Sig. (2-seitig)		,795	,632	,710	,534	,902	,581	,037	,501	,930	,592	,000
	N	51	51	51	51	51	51	51	51	51	51	51	51

*. Korrelation ist bei Niveau 0,05 signifikant (zweiseitig).

b. Kann nicht berechnet werden, da mindestens eine der Variablen konstant ist.

Tabelle 24 *Mann-Whitney-U-Tests von verschiedenen Applikationsgruppen und der gemessenen Vergütung in Euro*

Ränge

Social Media am wenigsten vertraut		H	Mittlerer Rang	Summe der Ränge
Gewählte Vergütung	Nein	37	25,34	937,50
	Ja	14	27,75	388,50
	Gesamtsumme	51		

Messenger am wenigsten vertraut		H	Mittlerer Rang	Summe der Ränge
Gewählte Vergütung	Nein	43	25,92	1114,50
	Ja	8	26,44	211,50
	Gesamtsumme	51		

Messenger am häufigsten genutzt		H	Mittlerer Rang	Summe der Ränge
Gewählte Vergütung	Nein	31	24,53	760,50
	Ja	20	28,28	565,50
	Gesamtsumme	51		

Teststatistiken[a]

	Vergütung		
Gruppierungsvariable	Messenger am wenigsten vertraut	Social Media am wenigsten vertraut	Messenger am häufigsten genutzt
Mann-Whitney-U-Test	168,500	234,500	264,500
Wilcoxon-W	1114,500	937,500	760,500
z	-,152	-,866	-1,469
Asymp. Sig. (2-seitig)	,879	,387	,142
Exakte Sig. [2*(1-seitige Sig.)]	,929[b]		

a. Gruppierungsvariable

b. Nicht für Bindungen korrigiert.

Tabelle 25 *Korrelationen zwischen Geschlecht und den Begründungen warum AGBs nicht gelesen wurden*

Korrelationen

		Geschlecht	Vertrauen	Keine Motivation	Zustimmung in jedem Fall erforderlich	Zu Komplizierte Sprache	Zu Lang	Text Immer Gleich
Geschlecht	Phi	1	-,076	,070	-,162	-,072	-,002	,065
	Cramer-V		,076	,070	,062	,072	,002	,065
	Sig. (2-seitig)		,451	,489	,110	,478	,987	,524
	N	97	97	97	97	97	97	97

Tabelle 26 *Korrelationen zwischen Geschlecht und den Begründungen warum AGBs gelesen wurden*

Korrelationen

		Geschlecht	Kontrolle	Kosten	Datenschutz	Bei Misstrauen	Gewissen Beruhigen
Geschlecht	Phi	1	-,001	,149	,047	,014	-,014
	Cramer-V		,001	,149	,047	,014	,014
	Sig. (2-seitig)		,995	,143	,641	,890	,894
	N	97	97	97	97	97	97

Tabelle 27 *Korrelationen des Geschlechtes mit den verschiedenen Kategorien der Applikationen*

Korrelationen									
		Sonstige Aggregiert	Nachrichten Aggregiert	Wetter Aggregiert	Email Apps Aggregiert	Browser Aggregiert	Messenger Aggregiert	Social Media Aggregiert	Kartendienste Aggregiert
Geschlecht	Phi	.[a]	.[a]	.[a]	.[a]	.[a]	,021	,037	,085
	Cramer V						,021	,037	,085
	Sig. (2-seitig)	.	.	.	.	.	,839	,719	,404
	N	13	5	4	5	6	97	97	97

[a]. Kann nicht berechnet werden, da mindestens eine der Variablen konstant ist

Tabelle 28 *Mann-Whitney-U-Tests Vergleich zwischen dem Stellenwert des Datenschutzes und der Anzahl an angegebenen Konsequenzen*

Ränge

	Stellenwert des Datenschutzes[a] (< 6 = 1; ≥ 6 = 0)	H	Mittlerer Rang	Summe der Ränge
Anzahl der Konsequenzen	,00	15	51,47	772,00
	1,00	82	48,55	3981,00
	Gesamtsumme	97		

Teststatistiken[a]

	Anzahl der Konsequenzen
Mann-Whitney-U-Test	578,000
Wilcoxon-W	3981,000
z	-,393
Asymp. Sig. (2-seitig)	,695

a. Gruppierungsvariable: FRA_KategorisierungStellenwert_unter6_0_ueber6_1

Tabelle 29 *Mann-Whitney-U-Tests Vergleich zwischen dem Stellenwert des Datenschutzes und dem Geschlecht*

Ränge

	Geschlecht	H	Mittlerer Rang	Summe der Ränge
Welchen Stellenwert nimmt für Sie der Schutz persönlicher Daten ein?	Männlich	44	48,16	2119,00
	Weiblich	53	49,70	2634,00
	Gesamtsumme	97		

Teststatistiken[a]

	Welchen Stellenwert nimmt für Sie der Schutz persönlicher Daten ein?
Mann-Whitney-U-Test	1129,000
Wilcoxon-W	2119,000
z	-,272
Asymp. Sig. (2-seitig)	,786

a. Gruppierungsvariable: Geschlecht

Tabelle 30 *Korrelationen zwischen finanziellem Aufwand für neue Applikationen und finanziellem Aufwand für Schutz der Privatsphäre*

Korrelationen

			Ausgaben für Applikationen in Euro pro Monat	Finanzieller Aufwand in Euro pro Monat zum Schutz der Daten
Spearman-Rho	Ausgaben für Applikationen in Euro pro Monat	Korrelationskoeffizient	1,000	,369**
		Sig. (2-seitig)	.	,008
		N	51	51
	Finanzieller Aufwand in Euro pro Monat zum Schutz der Daten	Korrelationskoeffizient	,369**	1,000
		Sig. (2-seitig)	,008	.
		N	51	51

**. Korrelation ist bei Niveau 0,01 signifikant (zweiseitig).

Anhang K. Variablen zum ersten Versuch

1. FragebogenOderExperiment
2. Teilnahmecode
3. MES_Lesedauer
4. MES_Unterschrift_Nach_Lesen
5. MES_VergütungInEuro
6. MES_CTA
7. FRA_AntwortID
8. FRA_Geschlecht
9. FRA_Alter
10. FRA_Alter_Gruppiert
11. FRA_DatumGestartet
12. FRA_UhrzeitGestartet
13. FRA_DatumAbgeschickt
14. FRA_UhrzeitAbgeschickt
15. FRA_Lesedauer
16. FRA_LetzteSeite
17. FRA_StartSprache
18. FRA_WelcheBetriebssystemenutzenSieauflhrenmobilenEndgeräten
19. FRA_WelcheBetriebssystemenutzenSieauflhrenmobilenEndgeräten_A
20. FRA_WelcheBetriebssystemenutzenSieauflhrenmobilenEndgeräten_B
21. FRA_WelcheBetriebssystemenutzenSieauflhrenmobilenEndgeräten_C
22. FRA_WelcheAppnutzenSieammeisten
23. FRA_WelcheAppNutzenSieAmMeistenSonstigeAggregiert
24. FRA_WelcheAppNutzenSieAmMeistenNachrichtenAggregiert
25. FRA_WelcheAppNutzenSieAmMeistenWetterAggregiert
26. FRA_WelcheAppNutzenSieAmMeistenSpiegelOnline
27. FRA_WelcheAppNutzenSieAmMeistenSitUps
28. FRA_WelcheAppNutzenSieAmMeistenPodcast
29. FRA_WelcheAppNutzenSieAmMeistenKeine
30. FRA_WelcheAppNutzenSieAmMeistenEbay
31. FRA_WelcheAppNutzenSieAmMeistenEmailAppsAggregiert
32. FRA_WelcheAppNutzenSieAmMeistenSpotify
33. FRA_WelcheAppNutzenSieAmMeistenBanking
34. FRA_WelcheAppNutzenSieAmMeistenEvernote
35. FRA_WelcheAppNutzenSieAmMeistenBrowserAggregiert
36. FRA_WelcheAppNutzenSIeAmMeistenKontakte
37. FRA_WelcheAppNutzenSieAmMeistenWarroom2
38. FRA_WelcheAppNutzenSieAmMeisten9GAG
39. FRA_WelcheAppNutzenSieAmMeistenKicker
40. FRA_WelcheAppNutzenSieAmMeistenKalender
41. FRA_WelcheAppNutzenSieAmMeistenTaschenrechner
42. FRA_WelcheAppNutzenSieAmMeistenThreema
43. FRA_WelcheAppNutzenSieAmMeistenWire
44. FRA_WelcheAppNutzenSieAmMeistenViber
45. FRA_WelcheAppNutzenSieAmMeistenSignal
46. FRA_WelcheAppNutzenSieAmMeistenTelegram
47. FRA_WelcheAppNutzenSieAmMeistenWhatsApp
48. FRA_WelcheAppNutzenSieAmMeistenGoogleMaps
49. FRA_WelcheAppNutzenSieAmMeisenÖPNVAPPS
50. FRA_WelcheAppNutzenSieAmMeistenAggregiertMessenger
51. FRA_WelcheAppNutzenSieAmMeistenInstagram
52. FRA_WelcheAppNutzenSieAmMeistenYoutube
53. FRA_WelcheAppNutzenSieAmMeistenFacebook
54. FRA_WelcheAppNutzenSieAmMeistenLiveJOurnal
55. FRA_WelcheAppNutzenSieAmMeistenSocialMedia
56. FRA_WelcheAppNutzenSieAmMeistenAggregiertSocialMedia
57. FRA_WelcheAppNutzenSieAmMeistenAggregiertKartendienste
58. FRA_NennenSiediejenigedervonIhnengenutztenAppsderSieamwe
59. FRA_AmWenigstenVertrauteAppsWhatsApp
60. FRA_AmWenigstenVertrauteAppsMessengerSonstige
61. FRA_AmWenigstenVertrauteAppsMessengerAggregiert
62. FRA_AmWenigstenVertrauteAppsFacebook
63. FRA_AmWengistenVertrauteAppsSocialMediaSonstige
64. FRA_AmWenigstenVertrauteAppsSocialMediaAggregiert
65. FRA_AmWenigstenVertrauteAppsKartenSonstige
66. FRA_AmWenigstenVertrauteAppsSonstige
67. FRA_AmWenigstenVertrauenAppsKeiner
68. FRA_WieoftinstallierenSieneueSoftwareauflhrenmobilenEndger
69. FRA_WieoftlesenSiesichvordemInstalliereneinerSoftwarediea
70. FRA_BegründenSieweshalbSieINSERTANS641666X913X12395dieAGBs
71. FRA_BegründungAGBLesenWieOft_Nein_Vertrauen
72. FRA_BegründungAGBLesenWieOft_Nein_KeineMotivation
73. FRA_BegründungAGBLesenWIeOft_Nein_MussEhZugestimmtWerden
74. FRA_BegründungAGBLesenWieOft_Nein_ZuKomplizierteSprache
75. FRA_BegründungAGBLesenWieOft_Nein_ZuLang
76. FRA_BegründungAGBLesenWieOft_Nein_TextImmerGleich
77. FRA_BegründungAGBLesenWieOft_Ja_Kontrolle
78. FRA_BegründungAGBLesenWieOft_Ja_Kosten

79. FRA_BegründungAGBLesenWieOft_Ja_Datenschutz
80. FRA_BegründungAGBLesenWieOft_Ja_BeiMisstrauen
81. FRA_BegründungAGBLesenWieOft_Ja_GewissenBeruhigen
82. FRA_VersetzenSiesichindieSituationinderSiezuletzteineAppl
83. FRA_VersetzenSiesichindieSituationinderSiezuletzteineAppl_A
84. FRA_VersetzenSiesichindieSituationinderSiezuletzteineAppl_B
85. FRA_VersetzenSiesichindieSituationinderSiezuletzteineAppl_C
86. FRA_VersetzenSiesichindieSituationinderSiezuletzteineAppl_D
87. FRA_VersetzenSiesichindieSituationinderSiezuletzteineAppl_E
88. FRA_VersetzenSiesichindieSituationinderSiezuletzteineAppl_F
89. FRA_VersetzenSiesichindieSituationinderSiezuletzteineAppl_G
90. FRA_VersetzenSiesichindieSituationinderSiezuletzteineAppl_H
91. FRA_DauerAGBBetrachten
92. FRA_DauerAGBBetrachtenKleinerAls1000
93. FRA_LesenSiediedengesamtenTextodernurbestimmteAbschnittedu
94. FRA_BittebegründenSieweshalbSiedieAGBsINSERTANS641666X913X
95. FRA_LeseverhaltenRelevanz
96. FRA_LeseverhaltenUnübersichtlich
97. FRA_LeseverhaltenSicherheit
98. FRA_LeseverhaltenÜberfliegen
99. FRA_LeseverhaltenDatenschutz
100. FRA_LeseverhaltenKosten
101. FRA_LeseverhaltenStandard
102. FRA_LeseverhaltenZuLang
103. FRA_EinigeApplikationenundPlattformenzeigeneinekurzeZusammenf
104. FRA_EinigeApplikationenundPlattformenzeigeneinekurzeZusammenf_A
105. FRA_EinigeApplikationenundPlattformenzeigeneinekurzeZusammenf_B
106. FRA_WelcheKonsequenzenkönntedieWeitergabeIhrerDatenfürSie
107. FRA_KonsequenzenDatenweitergabe_VerlustVonPrivatsphäre
108. FRA_KonsequenzenDatenweitergabe_VerkaufUndProfiling
109. FRA_KonsequenzenDatenweitergabe_Unbekannt_falsch_Verstanden
110. FRA_KonsequenzenDatenweitergabe_Spam
111. FRA_KonsequenzenDatenweitergabe_PersonalisierteWerbung
112. FRA_KonsequenzenDatenweitergabe_Hacks
113. FRA_KonsequenzenDatenweitergabe_Misstrauen_Deinstallation
114. FRA_KonsequenzenDatenweitergabe_Kosten
115. FRA_HabenSieaufgrundderAGBsschoneinmaldasInstalliernvonSo
116. FRA_NennenSiebittedensinngemäßdenInhaltderAGBderfürSie
117. FRA_ApplikationNichtInstalliert
118. FRA_ApplikationNichtInstalliert_Datenweitergabe
119. FRA_ApplikationNichtInstalliet_Kosten
120. FRA_ApplikationNichtInstalliert_GrundUnbekannt
121. FRA_ApplikationNichtInstalliert_ZuVieleOderFalscheRechteAngefor
122. FRA_ApplikationNichtInstalliert_AbgabeVonRechtenAnInhalten
123. FRA_HabenSieBedenkenandemSpeichernundderWeitergabevonIhren
124. FRA_HabenSieBedenkenandemSpeichernundderWeitergabevonIhren_A
125. FRA_HabenSieBedenkenandemSpeichernundderWeitergabevonIhren_B
126. FRA_WelcheArtvonDatenmeinenSiewerdenweitergegeben
127. FRA_WelcheArtvonDatenWerdenWeitergeben_KeineAhnung
128. FRA_WelcheArtvonDatenWerdenWeitergeben_Nutzungsverrhalten
129. FRA_WelcheArtvonDatenWerdenWeitergeben_Alle
130. FRA_WelcheArtVonDatenWerdenWeitergeben_EigenenKontaktDaten
131. FRA_WelcheArtVonDatenWerdenWeitergeben_Kontakte
132. FRA_WelcheArtvonDatenWerdenWeitergeben_Kommunikationsinhalte
133. FRA_WelcheArtVonDatenWerdenWeitergeben_Positionsdaten
134. FRA_WelcheArtVonDatenWerdenWeitergeben_Bilder
135. FRA_WelcheArtVonDatenWerdenWeitergeben_Demographische
136. FRA_WelcheArtVonDatenWerdenWeitergeben_Konsumverhalten
137. FRA_WelcheArtVonDatenWerdenWeitergeben_Kontodaten
138. FRA_WelcheArtVonDatenWerdenWeitergeben_PersönlicheVorlieben
139. FRA_SchätzenSiewasfüreinenmonetärenWertIhrepersönlichen
140. FRA_SchätzenSiewasfüreinenmonetärenWertIhrepersönlichen_A
141. FRA_SchätzenSiewasfüreinenmonetärenWertIhrepersönlichen_B
142. FRA_SchätzenSiewasfüreinenmonetärenWertIhrepersönlichen_C

143. FRA_SchätzenSiewasfüreinen monetärenWertIhrepersönlichen_D
144. FRA_SchätzenSiewasfüreinen monetärenWertIhrepersönlichen_E
145. FRA_SchätzenSiewasfüreinen monetärenWertIhrepersönlichen_F
146. FRA_KategorisierungStellenwert_unter6_0_ueber6_1
147. FRA_WelchenStellenwertnimmtfürSiederSchutzpersDaten10Hoch
148. FRA_WievielgebenSiedurchschnittlichimMonatfürApplikationen
149. FRA_WelchenfinanziellenAufwandwürdenSieimMonatbetreibenumI
150. FRA_Gesamtzeit
151. FRA_GruppenzeitDemographie
152. FRA_FragenzeitA
153. FRA_FragenzeitB
154. FRA_FragenzeitC
155. FRA_FragenzeitD
156. FRA_FragenzeitE
157. FRA_FragenzeitF
158. FRA_FragenzeitG
159. FRA_FragenzeitG2
160. FRA_FragenzeitH
161. FRA_FragenzeitI
162. FRA_FragenzeitJ
163. FRA_FragenzeitJ2
164. FRA_FragenzeitJ3
165. FRA_FragenzeitK
166. FRA_FragenzeitL
167. FRA_FragenzeitM
168. FRA_FragenzeitN
169. FRA_FragenzeitO
170. FRA_FragenzeitP
171. FRA_FragenzeitQ
172. FRA_FragenzeitR
173. FRA_FragenzeitS
174. INT_Verunsichert
175. INT_V_durch_Experiment
176. INT_V_durch_AGB
177. INT_Merkwürdig
178. INT_M_durch_AGBs
179. INT_M_durchExperiment
180. INT_Teilnahembedingungen_gelesen
181. INT_Lesedauer
182. INT_WarumNichtGelesen_ImmerGleich
183. INT_Besonderheiten
184. INT_ZuLangZumGanzLesen
185. INT_Auffälligkeiten
186. INT_A_DetaillierterAlsSonst
187. INT_A_Datenweitergabe
188. INT_A_ABG_Unwichtig
189. INT_A_BesondereStelle
190. INT_Gezögert
191. INT_Unwohlsein
192. INT_UWS_durchPreisgebenPersönlicherDaten
193. INT_UWS_durchMangelnder Alternativen
194. INT_keinUWS_daAnonym
195. INT_keinUWS_keineSensiblen Daten
196. INT_keinUWS_daDatenSchon BeiAnderenSachenPreisgegebenWerden

Anhang L. Daten der Personas

	Handy 1	Handy 2	Handy 3	Handy 4	Handy 5
Email	tubdroid01@gmail.com	tubdroid02@gmail.com	tubdroid@03gmail.com	tubdroid04@gmail.com	tubdroid05@gmail.com
Telefon	15227870273	01522 7870274			
Name	Ernst Müller	Elise Becker	Jens Jordan	Martha Schmidt	Detlef Niemweg
Geburtsdatum	01.04.1993	01.01.1991	01.02.1988	01.03.1992	01.05.1990
Gewicht	80 kg	60 kg	90 kg	55 kg	75 kg
Größe	180 cm	170 cm	190 cm	165 cm	175 cm

Anhang M. Liste der Antworten zu der Frage der am meisten genutzten Applikationen

Whatsapp	WhatsApp	WhatsApp
whatsapp	What's App	whatsapp
BVG	WhatsApp	Kalender, social media, Taschenrechner, maps, banking
whatsapp	Whatsapp	
WHATSAPP	WhatsApp	
keine	firefox	
Whatsapp	Öffi	WhatsApp
Telegram	Verbindungen	Whats App
keine	gmx	Whatsapp
whatsapp, instagram, livejournal, wetter,viber	E-Mail App	Instagram, 9 gag
	keine	WhatsApp
WhatsApp	chrome	Telegram
facebook	whatsapp	Evernote
whattsapp	inbox	Warroom 2
Whatsapp	sit ups	What's app
WhatsApp	Wetter	whatsapp
Podcast Addict	gmx	Signal (Open Whisper Systems)
Spiegel Online	facebook (computer)	
WhatsApp, 9gag	Chrome	whatsapp
Spotify	Wetter	WhatsApp
WhatsApp	Whatsapp	WhatsApp
Whatsapp	Ebay Kleinanzeigen	Telegram
Facebook	keine	whatsapp
Kontakte	whatsapp	Whats App
whatsapp	t-online	WhatsApp
Browser	whats app	WhatsApp
WhatsApp spotify	Spiegel	threema, firefox, wetterapp, wire,
mensseger	spiegel online	
whatsapp	Youtube	
Facebook		

Instagram Whatsapp WhatsApp google maps	kein Smartphone Chrome WhatsApp keine keine Angaben whatsapp Youtube	Whatsapp whatsapp Telegram Whatsapp Kicker Magazin WhatsApp WhatsApp

Anhang N. Liste zur Frage der am wenigsten vertrauten Applikationen

Facebook whatsapp facebook BVG TWITTER keine antwort Viber Tinmd keine whatsapp, instagra facebook keine google maps Gmail GoogleMaps keine WhatsApp Facebook, WhatsApp Whats App Facebook Facebook Facebook keine whatsapp WhatsApp Facebook whatsapp GoogleMaps WhatsApp facebook messenger Facebook facebook Facebook Runtastic	Facebook Snapchat WhatsApp whatsapp Facebook Messenger deutschlandkarte Browser nutze keine Apps instagramm keine Online Banking banking apps gOOGLE amazon keine Chrome facebook Whatsapp Facebook facebook google play whats app facebook facebook Facebook word, firefox Schallmessung Online Banking App entfällt nutze keine Apps whatsapp Snapchat	keine Apps install onlinebanking app Social Media Facebook Whats App Whatsapp WhatsApp Payback What's App Facebook Facebook What's app whatsapp BVG Fahrinfo facebook Playapps WhatsApp CamScanner google Whats App Facebook Facebook threema Instagram Facebook Facebook Facebook I never Party Facebook Facebook

Anhang O. Abbildungen der Skalen zum Vortest

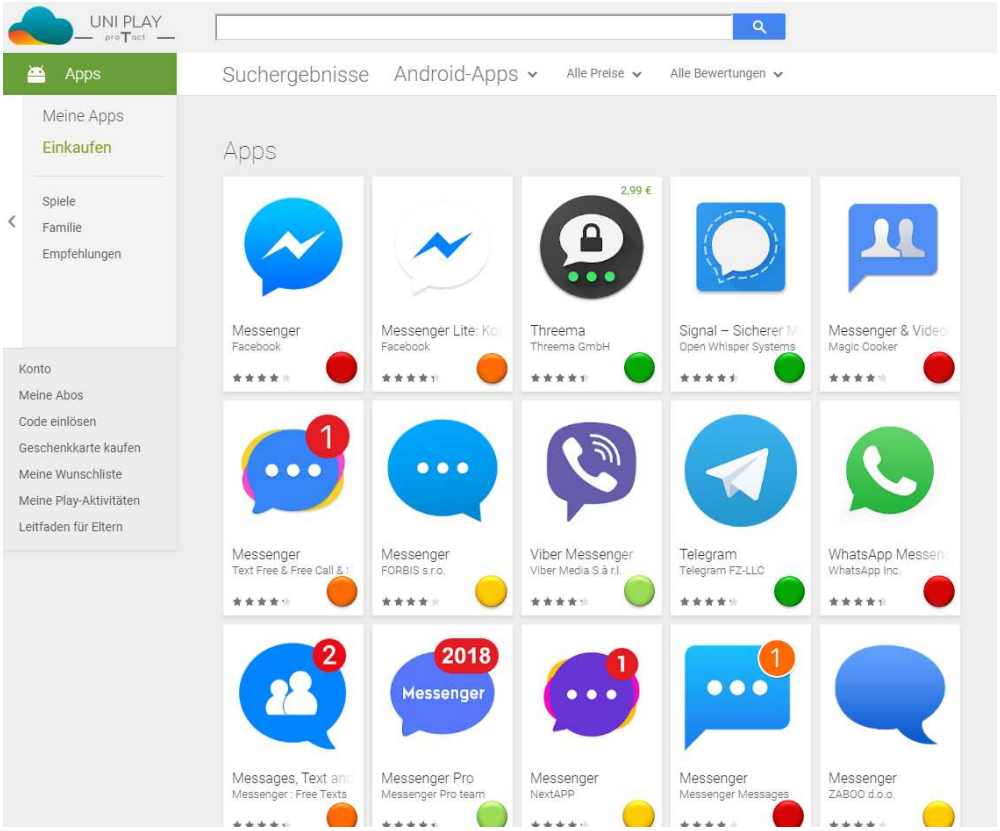


Abbildung 28. Bubble-Scale.

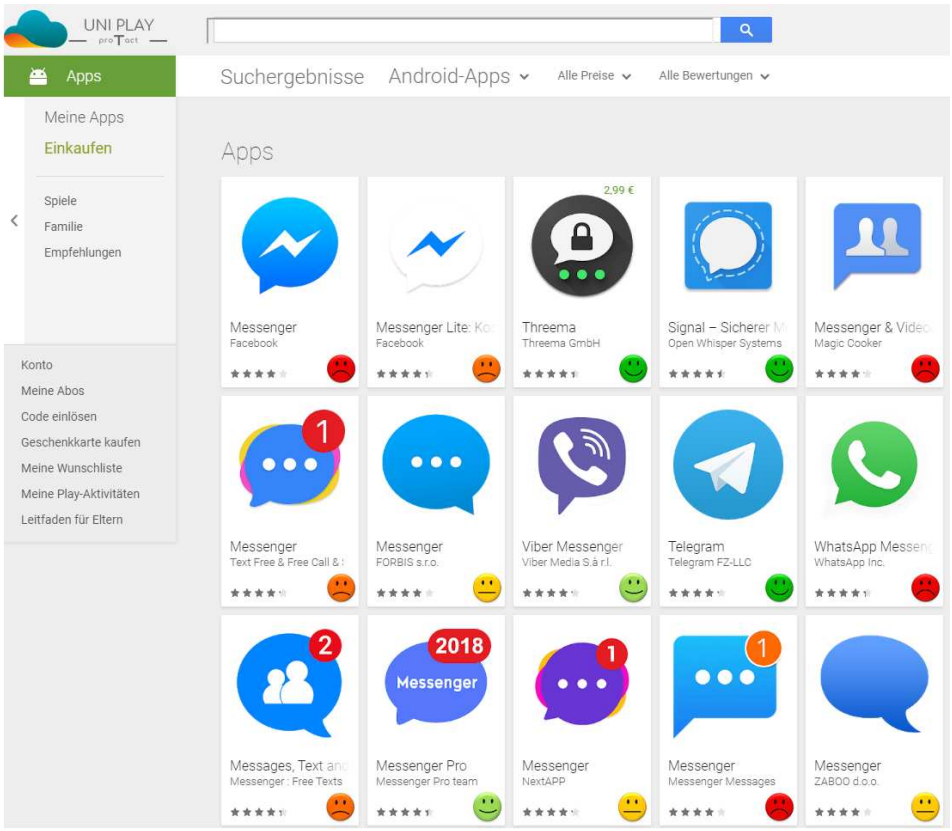


Abbildung 29. Smiley-Scale.

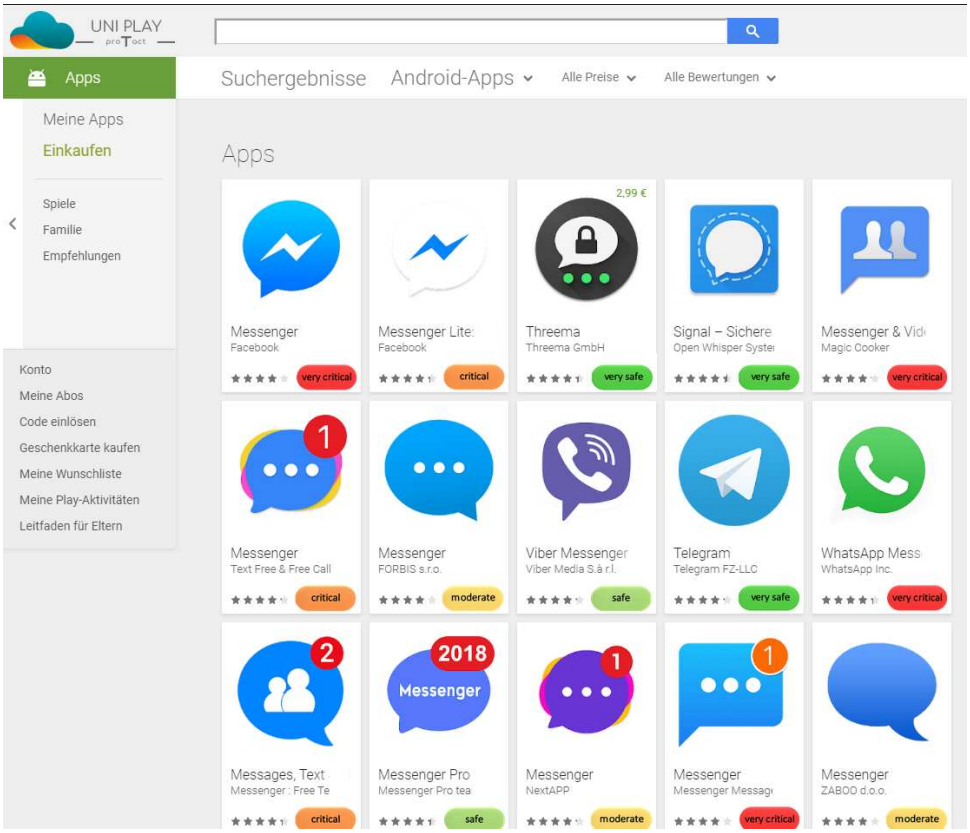


Abbildung 30. Label-Scale.

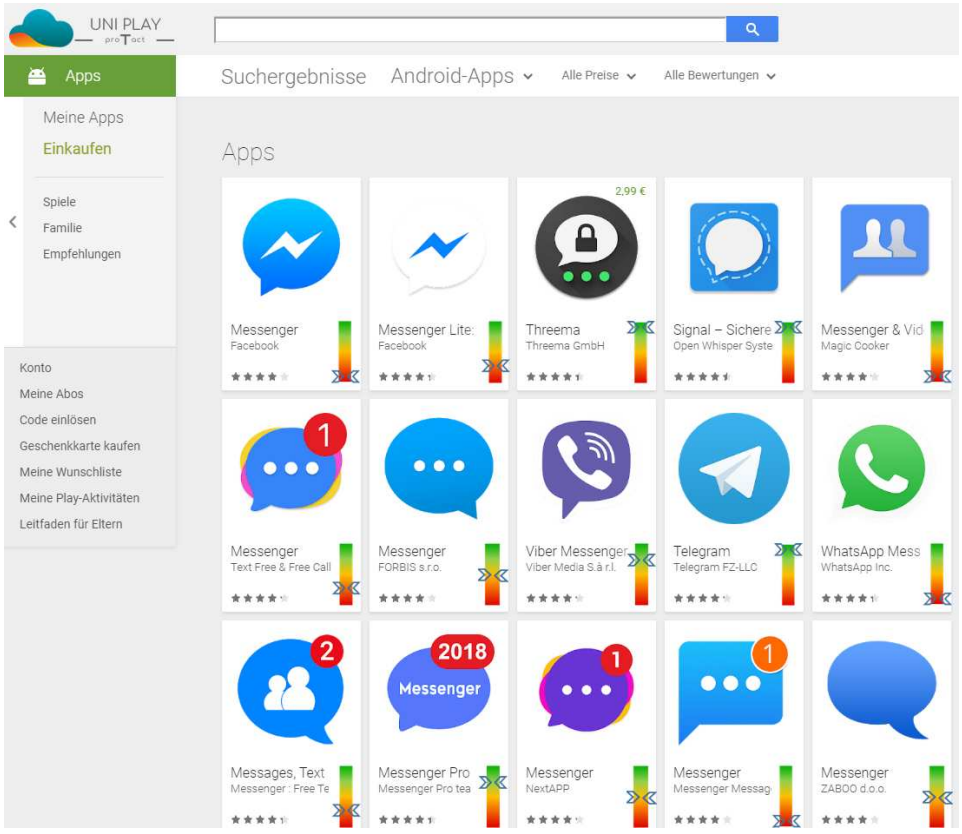


Abbildung 31. Arrow-Bar-Scale.

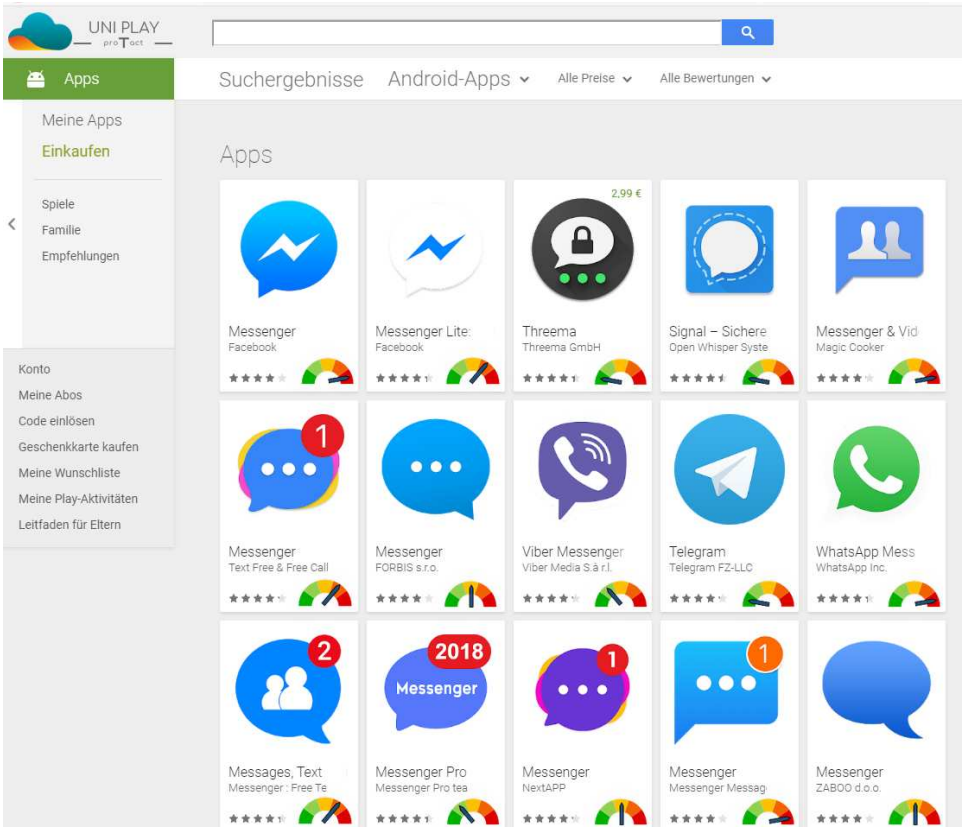


Abbildung 32. Arrow-Speedometer-Scale.

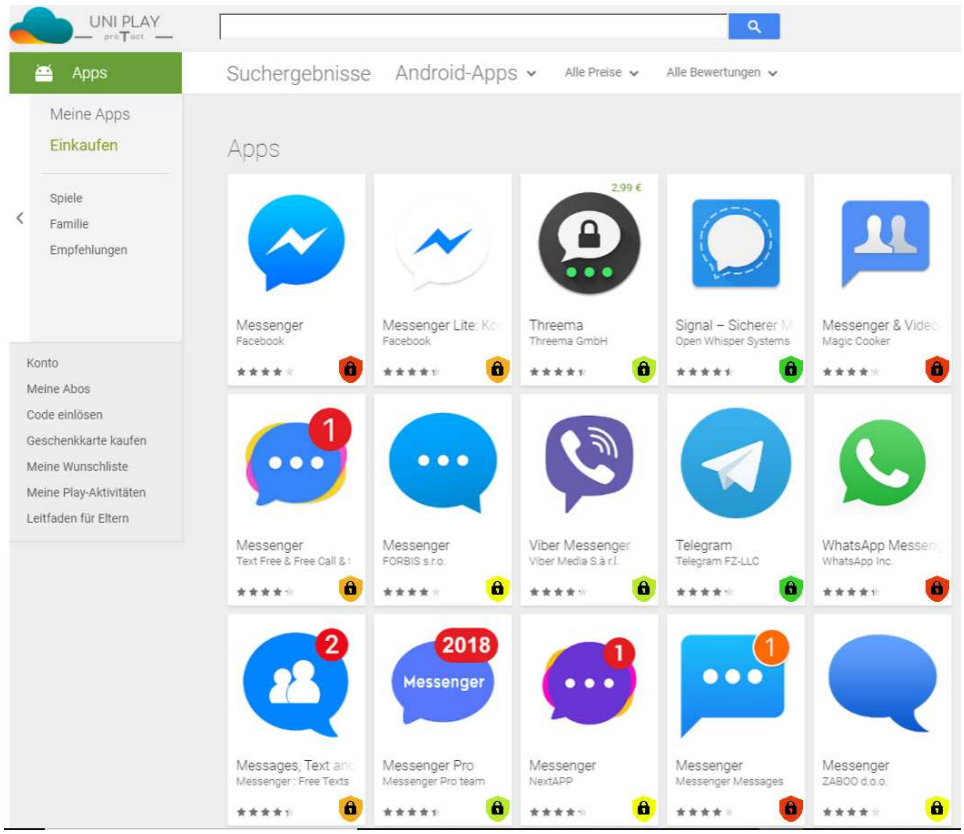


Abbildung 33. Lock Scale.

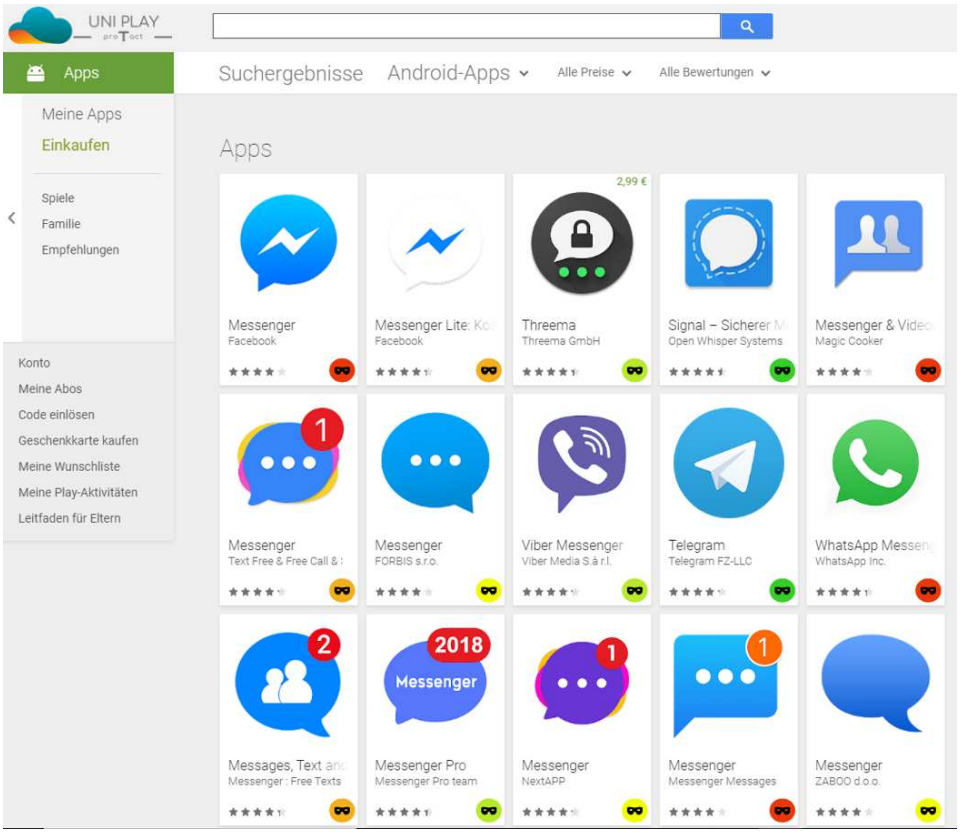


Abbildung 34. Mask Scale.

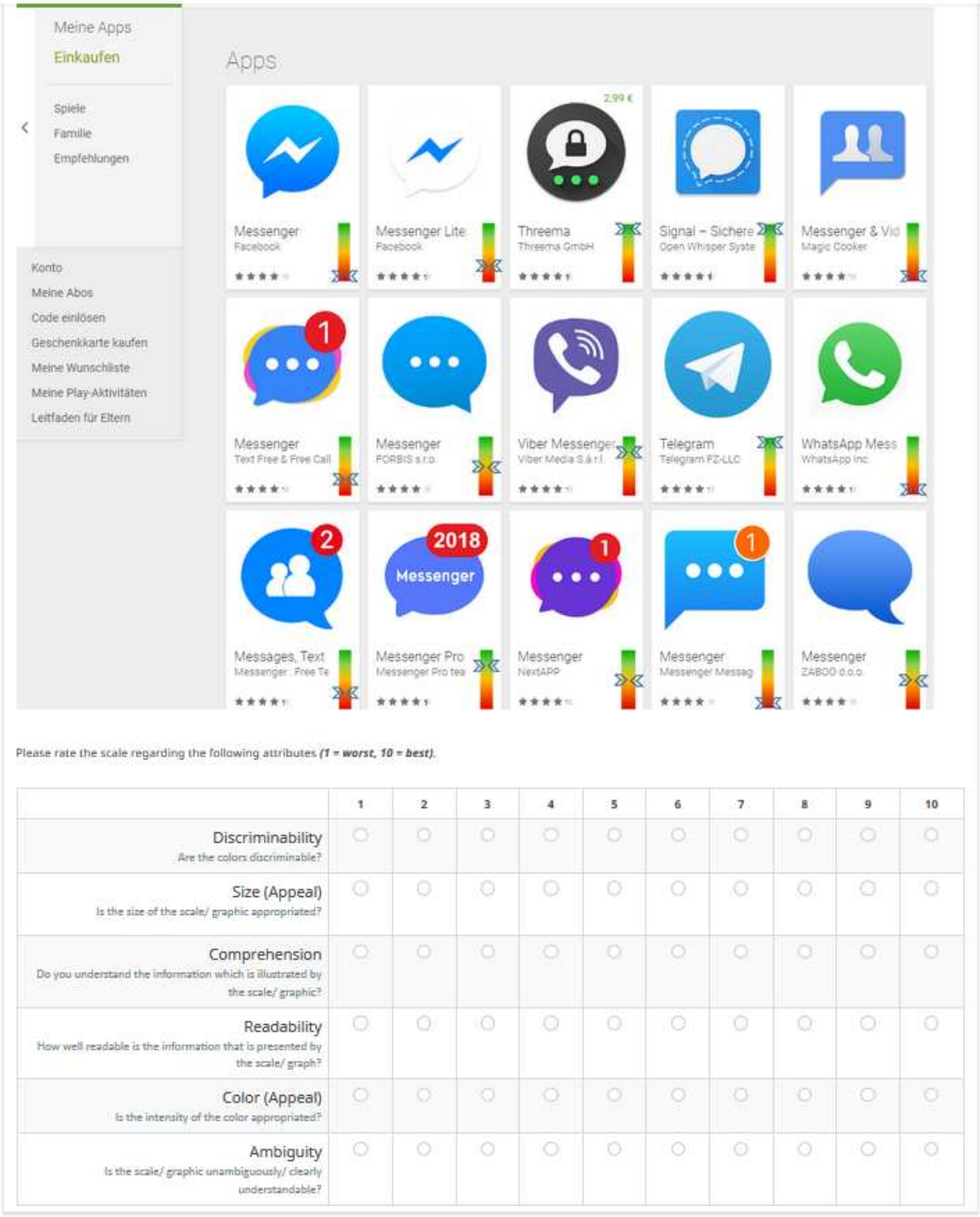


Abbildung 35. Beispielhafte Darstellung des Online-Fragebogens.

Section A: Demographic Information

A1. Please indicate your gender.

- ☐ Female
- ☐ Male

A2. Please indicate your age.

☐☐☐☐☐☐☐☐☐☐

A3. Approximately, how many hours per day do you spend using mobile devices?

- ☐ Less than half an hour
- ☐ more than half an hour but less than an hour
- ☐ more than an hour but less than two hours
- ☐ more than two hours but less than four hour
- ☐ more than four hours

A4. Do you care about the protection of your personal data stored on your mobile device?

1 2 3 4 5 6 7 8 9 10

1= I do not care | 10 = I care a lot

☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

A5. Which action did you take to protect your personal data?

- ☐ I did not take any action.
- ☐ I installed an application to protect my data.
- ☐ I am trying to disclose as little of my data as possible.
- ☐ I always read the terms and conditions before installing an application.
- ☐ Other

Other

Anhang Q. Beschreibung der Datenschutzskala mit Diagrammen zu Abfrage der Rechte und Risiko zur Freigabe persönlicher Informationen

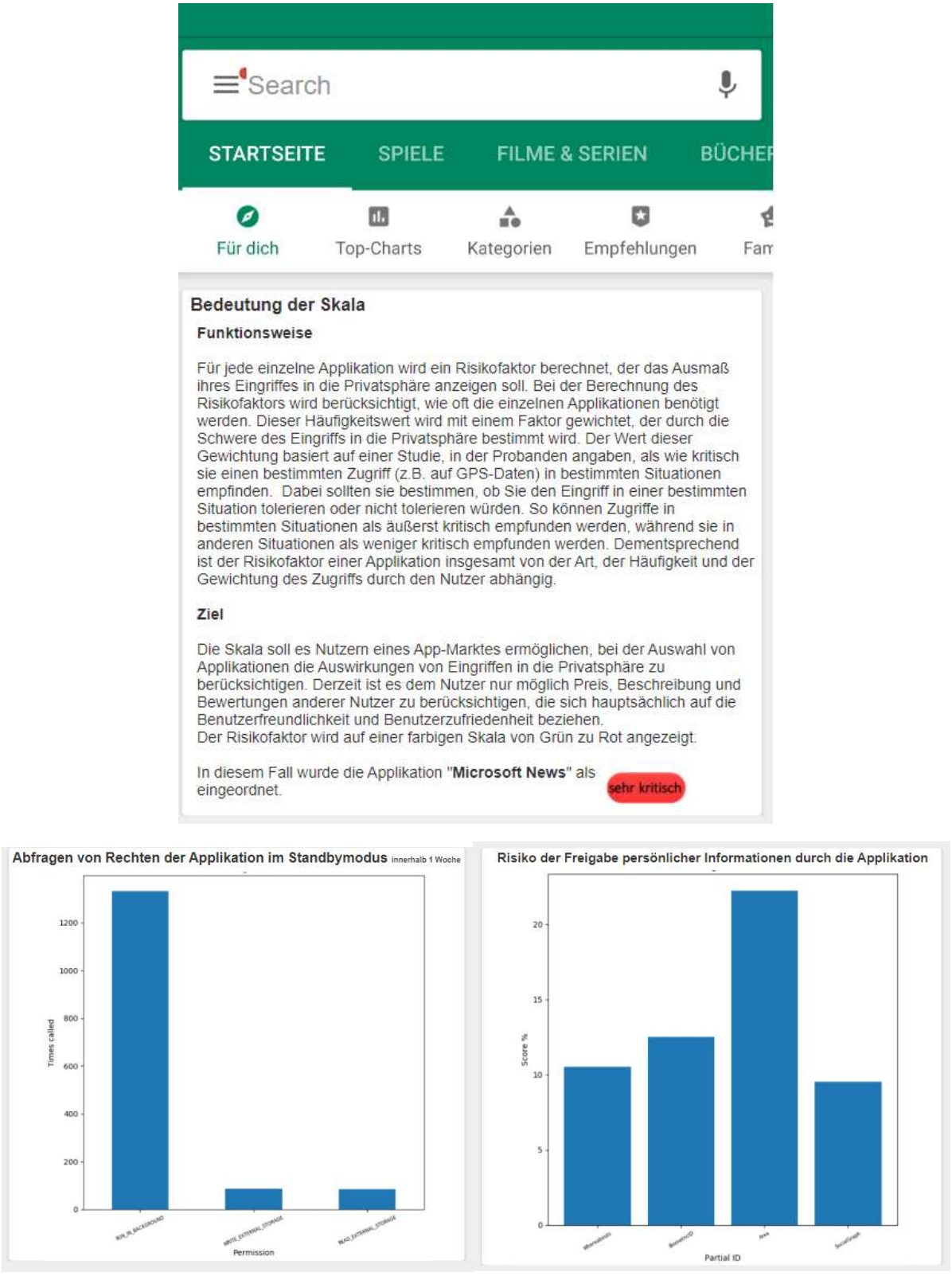


Abbildung 36. Beschreibung der Datenschutzskala mit Diagramm zur Abfrage der Rechte und Freigabe persönlicher Daten.

Anhang R. Einverständniserklärung zur zweiten Studie

TU Berlin | Fakultät V | IPA | FG Mensch-Maschine-Systeme |
Sek. MAR 3-1 | Marchstraße 23 | 10587 Berlin

Fakultät V Fakultät Verkehrs- und Maschinensysteme
Institut für Psychologie und Arbeitswissenschaft

Fachgebiet
Mensch-Maschine-Systeme

M. Sc. Sven Bock

Sekretariat MAR 3-1
Marchstraße 23
10587 Berlin

Telefon +49 (0)30 314-79523
Sven.Bock@mms.tu-berlin.de

Einverständniserklärung zur Studie
„Benutzerfreundlichkeit eines App-Marktes in bestimmten Situationen"

In dieser Studie soll die Benutzerfreundlichkeit und der Umgang eines App-Marktes genauer untersucht werden. Dafür werden Sie zunächst gebeten einen Fragebogen auszufüllen, in dem Sie angeben, ob bestimmte Applikationen auf Ihren mobilen Endgeräten installiert sind. Anschließend findet ein Versuch an einem stationären Computer statt. Hierbei sind umfangreichere Möglichkeiten gegeben, um das Verhalten zu beobachten und zu analysieren. So wird es möglich sein, das Blickverhalten mittels eines Eye-Trackers zu verfolgen. Stellen Sie sich bitte dennoch vor, Sie würden ein mobiles Endgerät (Smartphone) benutzen, welches Sie sowohl für private als auch geschäftliche Zwecke verwenden würden. Darüber hinaus werden Ihnen acht verschiedene Szenarien vorgelegt, in welche Sie sich hineinversetzen sollen, um die Ihnen gestellte Aufgabe adäquat zu lösen. Anschließend folgt ein Interview, welches einige Fragen zu Ihrem im Versuch gezeigten Verhalten umfasst. Abschließend werden Sie gebeten einen Fragebogen zum Experiment auszufüllen.
Die Studie wird ca. 60 Minuten dauern und mit zehn Euro oder einer Versuchspersonenstunde vergütet.

Mir wurde der Zweck der Studie erläutert. Ich wurde darüber informiert, dass ich die Studie jederzeit ohne Angabe von Gründen abbrechen kann und mir dadurch keine Nachteile entstehen. Des Weiteren wurde ich darüber in Kenntnis gesetzt, dass die während der Studie gesammelten Video-, Audio- und Sensordaten zur Auswertung der Studie herangezogen werden. Diese werden aus rechtlichen Gründen bis zu zehn Jahre aufbewahrt. Die Tonaufnahmen werden nach erfolgter Transkription des Interviews gelöscht. Sämtliche Daten werden für die wissenschaftliche Nutzung gesammelt und hierbei vertraulich und anonym behandelt. Die anonymisierten Ergebnisse werden nach der Auswertung im Rahmen der Doktorarbeit veröffentlicht. Personenbezogenen Daten, wie z.B. diese Einverständniserklärung, werden streng vertraulich behandelt und getrennt voneinander aufbewahrt. Ich bin damit einverstanden, dass die erhobenen Daten in anonymisierter Form gespeichert und zu wissenschaftlichen Zwecken ausgewertet werden. Ich weiß, dass ich bei Bedarf die Möglichkeit habe, innerhalb von zwei Wochen eine Anfrage auf die Löschung der Versuchsdaten zu stellen, welcher umgehend nachgegangen wird. Hierfür ist die Mitteilung des persönlichen Teilnahmecodes erforderlich. Anschließend wird die Zuordnungsliste zwischen persönlichem Code und fortlaufender VP-Nummer gelöscht, sodass eine Löschung der Versuchsdaten nicht mehr gewährleistet ist.
Ich bin über Wesen, Bedeutung und Tragweite der geplanten Eye-Tracking-Erhebung hinreichend aufgeklärt worden. Ich habe die Fragen zur Überprüfung von Voraussetzungen wahrheitsgemäß beantwortet. Ich bin darauf aufmerksam gemacht worden, dass bei Erhebung dieser Daten keine medizinische Diagnostik durchgeführt wird.

Meine Teilnahme an der Studie erfolgt freiwillig. Ich hatte die Möglichkeit Rückfragen zu stellen und sie wurden zu meiner Zufriedenheit beantwortet. Ich habe die Teilnehmerinformationen vollständig gelesen und verstanden. Mit dem Unterschreiben der Einverständniserklärung erkläre ich mich mit diesen einverstanden.

Berlin, _____ _____ _____
Datum Unterschrift Name in Druckschrift

Anhang S. Anleitung zur Generierung des persönlichen Codes

TU Berlin | Fakultät V | IPA | FG Mensch-Maschine-Systeme |
Sek. MAR 3-1 | Marchstraße 23 | 10587 Berlin

Erklärung zur Erstellung des persönlichen Personencodes

Technische Universität Berlin

Fakultät V Fakultät Verkehrs- und Maschinensysteme
Institut für Psychologie und Arbeitswissenschaft

Fachgebiet
Mensch-Maschine-Systeme

M. Sc. Sven Bock

Sekretariat MAR 3-1
Marchstraße 23
10587 Berlin

Telefon +49 (0)30 314-79523
Sven.Bock@mms.tu-berlin.de

Bitte erstellen Sie mithilfe dieser Anleitung Ihren persönlichen Personencode. Ihre Daten werden nicht unter Ihrem Namen gespeichert sondern unter einer laufenden Nummer. Diese laufende Nummer wird dem Personencode zugeordnet. Dieser Code ist individuell, er ermöglicht jedoch keine Rückschlüsse auf Ihre Person. Dadurch soll die Anonymisierung gewährleistet werden. Der Code kann jedoch von Ihnen selbst jederzeit rekonstruiert werden. Dies ist erforderlich für den Fall, dass Sie Ihr Einverständnis innerhalb der Frist von vierzehn Tagen widerrufen möchten. Nach dieser Frist wird die Zuordnung ihrer Personennummer zu Ihrem Code gelöscht. Eine Zuordnung ist dann nicht mehr möglich.

Dies sind die Bestandteile Ihres Personencodes:

1. Erster Buchstabe des Vornamens Ihrer Mutter.
2. Erster Buchstabe des Vornamens Ihres Vaters.
3. Erster Buchstabe Ihres eigenen Geburtsortes.
4. Letzte Ziffer Ihres eigenen Geburts*jahres*.
5. Letzte Ziffer Ihres eigenen Geburts*tages*.

Beispiel:

Name der Mutter:	**H**elga	**H**
Name des Vaters:	**W**olfgang	**W**
Geburtsort:	**H**ildesheim	**H**
Geburtsjahr:	19**4**7	**7**
Geburtstag:	**1**2. Juni	**2**

Personencode: **HWH72**

Anhang T. Einverständniserklärung für Video- und Tonaufnahme

TU Berlin | Fakultät V | IPA | FG Mensch-Maschine-Systeme |
Sek. MAR 3-1 | Marchstraße 23 | 10587 Berlin

Einwilligungserklärung für Bild- und Tonaufnahmen
Im Rahmen der Studie „Benutzerfreundlichkeit eines App-Marktes in bestimmten Situationen"

Technische Universität Berlin

Fakultät V Fakultät Verkehrs- und Maschinensysteme
Institut für Psychologie und Arbeitswissenschaft

Fachgebiet Mensch-Maschine-Systeme

M. Sc. Sven Bock

Sekretariat MAR 3-1
Marchstraße 23
10587 Berlin

Telefon +49 (0)30 314-79523
Sven.Bock@mms.tu-berlin.de

Ich wurde schriftlich vom Versuchsleiter darüber informiert, dass im Rahmen der Studie Video- und Tonaufnahmen gemacht werden.

Die Aufnahmen dienen dazu, dass an den Tag gelegte Verhalten später besser reflektieren zu können.

Auf den von mir gemachten Video- und Tonaufnahmen bin ich potentiell erkennbar.

Die Video- und Tonaufnahmen können nur unter sehr großem Aufwand vollständig anonymisiert werden. Diese Anonymisierung kann im Rahmen dieser Studie nicht gewährleistet werden. Daher besteht die sehr geringe Wahrscheinlichkeit, dass eine an der Datenauswertung beteiligte Person mich in den von mir gemachten Aufnahmen erkennt. Aus diesem Grund unterliegen alle an der Auswertung beteiligten Personen einer absoluten Schweigepflicht und dürfen unter keinen Umständen vertrauliche Informationen an Dritte weitergeben.

Die Aufzeichnung und Auswertung der Video- und Tonaufnahmen erfolgt unter Verwendung eines persönlichen Codewortes, das ich selbst erstellt habe und das nur ich selbst kenne, d. h. unter Verwendung eines Pseudonyms und ohne Angabe meines Namens. Es existiert eine Kodierliste auf Papier, die mein Pseudonym mit einer Nummer verbindet.

Da ich in den von mir gemachten Aufnahmen potentiell erkannt werden kann, habe ich das Recht diese Aufnahmen jederzeit Löschen zu lassen, ohne dass mir daraus Nachteile entstehen. Dazu wende ich mich innerhalb der nächsten vierzehn Tage an die oben angegebenen Kontaktdaten der Ansprechperson und gebe mein persönliches Codewort an, die Kodierliste wird bis zur Löschung der Aufnahmen aufbewahrt.

Die Video- und Tonaufnahmen werden in einem verschlossenen Schrank aufbewahrt und nach der Auswertung der Daten nach spätestens 10 Jahren gelöscht.

Die Einverständniserklärung für die Video- und Tonaufnahme ist freiwillig. Ich kann diese Erklärung im Zeitraum von vierzehn Tagen widerrufen. Im Falle einer Ablehnung oder eines Rücktritts entstehen für mich keinerlei Kosten oder anderweitige Nachteile; eine Teilnahme an der Studie ist dann allerdings nicht möglich.

Ich hatte genügend Zeit für eine Entscheidung und erkläre mich hiermit bereit, dass eine Video- und Tonaufnahme von mir gemacht wird. Außerdem hatte ich die Möglichkeit, Rückfragen zu stellen, und sie wurden zu meiner Zufriedenheit beantwortet. Eine Ausfertigung dieser Einwilligungserklärung habe ich erhalten.

Ort, Datum und Unterschrift **Teilnehmer/in**	Name (Teilnehmer/in) in Druckschrift
_____	_____
Ort, Datum und Unterschrift **Versuchsleitung**	Name (Versuchsleitung) in Druckschrift
_____	_____

Bei Fragen oder anderen Anliegen kann ich mich an die oben genannten Kontaktdaten wenden.

Teil A: Bitte geben Sie Ihre fortlaufende Versuchspersonennummer an

A1. Bitte geben Sie Ihre Versuchspersonennummer an .

Teil B: Bereits auf dem eigenen mobilen Endgerät (Smartphone) installierte Applikation.

B1.

	installiert und bereits verwendet	installiert und noch nicht verwendet	bereits verwendet, derzeit jedoch nicht installiert	nicht installiert und noch nicht verwendet
BiP Messenger	☐	☐	☐	☐
WhatsApp	☐	☐	☐	☐
Threema	☐	☐	☐	☐
Signal	☐	☐	☐	☐
Facebook Messenger	☐	☐	☐	☐
Wire	☐	☐	☐	☐
Kik	☐	☐	☐	☐
Messenger (Forbis)	☐	☐	☐	☐
Telegram	☐	☐	☐	☐
Hangouts	☐	☐	☐	☐
Line	☐	☐	☐	☐
Skype	☐	☐	☐	☐
Google Duo	☐	☐	☐	☐
TrueConf	☐	☐	☐	☐
JusTalk	☐	☐	☐	☐
Glide	☐	☐	☐	☐
Zoom	☐	☐	☐	☐
Video Call	☐	☐	☐	☐
Imo	☐	☐	☐	☐
Tango	☐	☐	☐	☐

	installiert und bereits verwendet	installiert und noch nicht verwendet	bereits verwendet, derzeit jedoch nicht installiert	nicht installiert und noch nicht verwendet
Viber	☐	☐	☐	☐
Accu-Weather	☐	☐	☐	☐
Yr	☐	☐	☐	☐
Wetter-Online	☐	☐	☐	☐
Bayer Agrar Wetter	☐	☐	☐	☐
Weather Live (Innovative Team)	☐	☐	☐	☐
Yahoo Wetter	☐	☐	☐	☐
Morecast (UBIMET)	☐	☐	☐	☐
wetter.com	☐	☐	☐	☐
Windy	☐	☐	☐	☐
Weather-zone	☐	☐	☐	☐
Microsoft Outlook	☐	☐	☐	☐
K-9 Mail	☐	☐	☐	☐
myMail	☐	☐	☐	☐
Nine	☐	☐	☐	☐
Blue Mail	☐	☐	☐	☐
MailDroid	☐	☐	☐	☐
E-Mail für Outlook und andere	☐	☐	☐	☐
Open Mail	☐	☐	☐	☐
Play Musik	☐	☐	☐	☐
FreeMusic Player	☐	☐	☐	☐
Song Flip- Free Music Streaming & Player	☐	☐	☐	☐
Deezer	☐	☐	☐	☐
SoundCloud	☐	☐	☐	☐

	installiert und bereits verwendet	installiert und noch nicht verwendet	bereits verwendet, derzeit jedoch nicht installiert	nicht installiert und noch nicht verwendet
Spotify	☐	☐	☐	☐
Freie Musik MH Musik	☐	☐	☐	☐
Gratis Musik/ Free Music	☐	☐	☐	☐
Audiomack Musik und Mixtapes	☐	☐	☐	☐
Musikspieler	☐	☐	☐	☐
Schrittzähler- Gratis Pedometer & Kalorienzähler	☐	☐	☐	☐
Pacer Health Schrittzähler & Abnehmtrainer	☐	☐	☐	☐
Google Fit	☐	☐	☐	☐
Endomondo	☐	☐	☐	☐
Fitbit	☐	☐	☐	☐
Wandern Schrittzähler Diät	☐	☐	☐	☐
Strava Training	☐	☐	☐	☐
Laufen zur Gewichtsabnahme	☐	☐	☐	☐
Sportractive workout	☐	☐	☐	☐
Sudoku 2 (Magma Mobile)	☐	☐	☐	☐
Sudoku classic (Quarzo Apps)	☐	☐	☐	☐
Sudoku (Volcano Entertainment)	☐	☐	☐	☐
Sudoku (Card Games)	☐	☐	☐	☐
Sudoku Free (Titan IncGeduldsspiele)	☐	☐	☐	☐
Sudoku Free (Jigsaw Puzzle Free)	☐	☐	☐	☐
Sudoku (Timeglass Works)	☐	☐	☐	☐
Material Sudoku (OkayCode)	☐	☐	☐	☐
Sudoku Master (Dat Viet Entertainment)	☐	☐	☐	☐
Sudoku kostenlos deutsch (Marco Meyer)	☐	☐	☐	☐

	installiert und bereits verwendet	installiert und noch nicht verwendet	bereits verwendet, derzeit jedoch nicht installiert	nicht installiert und noch nicht verwendet
FlipBoard	☐	☐	☐	☐
bbc News	☐	☐	☐	☐
CNN Breaking News	☐	☐	☐	☐
News Suite	☐	☐	☐	☐
SQUID	☐	☐	☐	☐
Euronews	☐	☐	☐	☐
RT News	☐	☐	☐	☐
Die Zeit	☐	☐	☐	☐
Google news	☐	☐	☐	☐
Microsoft News	☐	☐	☐	☐

Teil C: Erläuterung der Auswahl zu den jeweiligen Aufgaben

C1. Messenger

	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
Es ist mir leicht gefallen, die richtige Applikation für die Aufgabe auszuwählen.	☐	☐	☐	☐	☐	☐	☐
Ich halte die ausgewählte Applikation für vertrauenswürdig im Hinblick auf den Schutz meiner Daten.	☐	☐	☐	☐	☐	☐	☐

C2. Videokonferenz

	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
Es ist mir leicht gefallen, die richtige Applikation für die Aufgabe auszuwählen.	☐	☐	☐	☐	☐	☐	☐
Ich halte die ausgewählte Applikation für vertrauenswürdig im Hinblick auf den Schutz meiner Daten.	☐	☐	☐	☐	☐	☐	☐

C3. Wetter

	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
Es ist mir leicht gefallen, die richtige Applikation für die Aufgabe auszuwählen.	☐	☐	☐	☐	☐	☐	☐
Ich halte die ausgewählte Applikation für vertrauenswürdig im Hinblick auf den Schutz meiner Daten.	☐	☐	☐	☐	☐	☐	☐

C4. E-Mail

	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
Es ist mir leicht gefallen, die richtige Applikation für die Aufgabe auszuwählen.	☐	☐	☐	☐	☐	☐	☐
Ich halte die ausgewählte Applikation für vertrauenswürdig im Hinblick auf den Schutz meiner Daten.	☐	☐	☐	☐	☐	☐	☐

C5. Musik

	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
Es ist mir leicht gefallen, die richtige Applikation für die Aufgabe auszuwählen.	☐	☐	☐	☐	☐	☐	☐
Ich halte die ausgewählte Applikation für vertrauenswürdig im Hinblick auf den Schutz meiner Daten.	☐	☐	☐	☐	☐	☐	☐

C6. Fitness

	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
Es ist mir leicht gefallen, die richtige Applikation für die Aufgabe auszuwählen.	☐	☐	☐	☐	☐	☐	☐
Ich halte die ausgewählte Applikation für vertrauenswürdig im Hinblick auf den Schutz meiner Daten.	☐	☐	☐	☐	☐	☐	☐

C7. Spiele

	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
Es ist mir leicht gefallen, die richtige Applikation für die Aufgabe auszuwählen.	☐	☐	☐	☐	☐	☐	☐
Ich halte die ausgewählte Applikation für vertrauenswürdig im Hinblick auf den Schutz meiner Daten.	☐	☐	☐	☐	☐	☐	☐

C8. Nachrichten/Neuigkeiten

	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
Es ist mir leicht gefallen, die richtige Applikation für die Aufgabe auszuwählen.	☐	☐	☐	☐	☐	☐	☐
Ich halte die ausgewählte Applikation für vertrauenswürdig im Hinblick auf den Schutz meiner Daten.	☐	☐	☐	☐	☐	☐	☐

Teil D: Bewertung der Privatsphäreskala

D1. Bitte bewerten Sie folgende Aussagen bezüglich der Privatsphäreskala.

	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
Die Privatsphäreskala ist vertrauenswürdig.	☐	☐	☐	☐	☐	☐	☐

	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
Die Benutzerfreundlichkeit der Privatsphäreskala ist gut.	☐	☐	☐	☐	☐	☐	☐
Die Privatsphäreskala ist leicht zu verstehen.	☐	☐	☐	☐	☐	☐	☐
Die Privatsphäreskala ist intuitiv.	☐	☐	☐	☐	☐	☐	☐
Die Privatsphäreskala ist gültig.	☐	☐	☐	☐	☐	☐	☐
Die Privatsphäreskala ist zuverlässig.	☐	☐	☐	☐	☐	☐	☐
Die Privatsphäreskala hatte Auswirkungen auf meine Wahl.	☐	☐	☐	☐	☐	☐	☐
Die Privatsphäreskala ist verwirrend.	☐	☐	☐	☐	☐	☐	☐
Die von der Privatsphäreskala bereitgestellten Informationen sind für die Benutzenden nicht ausreichend.	☐	☐	☐	☐	☐	☐	☐
Die Privatsphäreskala erhöht das Gefühl des Schutzes der Privatsphäre.	☐	☐	☐	☐	☐	☐	☐
Ich hätte gerne eine Privatsphäreskala in meinem eigenen App-Markt.	☐	☐	☐	☐	☐	☐	☐
Die Privatsphäreskala ist unnötig komplex.	☐	☐	☐	☐	☐	☐	☐
Wenn es möglich wäre, die Privatsphäreskala zu aktivieren und deaktivieren würde ich die Privatsphäreskala aktivieren.	☐	☐	☐	☐	☐	☐	☐
Die Privatsphäreskala erhöht die Vertrauenswürdigkeit der Applikation.	☐	☐	☐	☐	☐	☐	☐

D2. Haben Sie Verbesserungsvorschläge bezüglich der Privatsphäreskala?

Teil E: MUIPC - Fragen über den Datenschutz

E1. Bitte kreuzen Sie an, ob die folgenden Aussagen auf Sie zutreffen.

	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
Ich glaube, dass der Standort meines mobilen Gerätes zumindest zeitweise überwacht wird.	☐	☐	☐	☐	☐	☐	☐
Ich mache mir Sorgen, dass Applikationen zu viele Informationen über mich sammeln.	☐	☐	☐	☐	☐	☐	☐

	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
Ich mache mir Sorgen, dass Applikationen meine Aktivitäten auf meinem mobilen Gerät überwachen.	☐	☐	☐	☐	☐	☐	☐
Ich habe das Gefühl, dass andere durch meine Verwendung von Applikationen mehr über mich wissen, als mir angenehm ist.	☐	☐	☐	☐	☐	☐	☐
Ich glaube, dass aufgrund meiner Verwendung von Applikationen, Informationen über mich, die ich für privat halte, jetzt besser für andere verfügbar sind, als ich es möchte.	☐	☐	☐	☐	☐	☐	☐
Ich habe das Gefühl, dass aufgrund meiner Verwendung von Applikationen, Informationen über mich verfügbar sind, die, wenn sie genutzt werden, in meine Privatsphäre eindringen.	☐	☐	☐	☐	☐	☐	☐
Ich mache mir Sorgen, dass Applikationen meine persönlichen Daten für andere Zwecke verwenden dürfen ohne mich zu benachrichtigen oder meine Berechtigung einzuholen.	☐	☐	☐	☐	☐	☐	☐
Wenn ich persönliche Informationen zur Verwendung von Applikationen herausgebe, habe ich Bedenken, dass die Applikationen meine Informationen für andere Zwecke benutzen.	☐	☐	☐	☐	☐	☐	☐
Ich mache mir Sorgen, dass Applikationen meine persönlichen Daten mit anderen Instanzen teilen können ohne meine Berechtigung einzuholen.	☐	☐	☐	☐	☐	☐	☐
Ich werde wahrscheinlich meine persönlichen Informationen offenlegen, um Applikationen in den nächsten 12 Monaten nutzen zu können.	☐	☐	☐	☐	☐	☐	☐

E2. Wie oft haben Sie persönlich Vorfälle innerhalb der letzten 2 Jahre erlebt, bei denen Ihre persönlichen Daten von Unternehmen oder E-Commerce-Webseiten ohne Ihre Genehmigung verwendet wurden?

kein mal ☐

1 - 2 mal ☐

3 - 4 mal ☐

mehr als 5 mal ☐

E3. Wie oft haben Sie in den letzten zwei Jahren über die Verwendung und den potenziellen Missbrauch des Sammelns von Informationen gehört oder gelesen?

kein mal ☐

1 - 2 mal ☐

3 - 4 mal ☐

mehr als 5 mal ☐

E4. Wie oft waren Sie in den letzten zwei Jahren persönlich Opfer dessen, was Sie als unangemessenen Eingriff in ihre Privatsphäre empfanden?

kein mal ☐

1 - 2 mal ☐

3 - 4 mal ☐

mehr als 5 mal ☐

Teil F: Demographische Daten

Bitte beantworten Sie die folgenden Fragen zu Ihrer Person.

F1. Bitte geben Sie Ihr Geschlecht an.

weiblich ☐

männlich ☐

F2. Bitte geben Sie Ihr Alter in Jahren an.

☐☐☐☐☐☐☐☐☐☐

F3. Bitte geben Sie Ihren höchsten Bildungsabschluss an.

kein Abschluss ☐

Hauptschule / mittlere Reife ☐

Abitur / Allgemeine Hochschulreife ☐

Berufsausbildung ☐

Akademischer Abschluss ☐

Sonstiges ☐

Sonstiges

F4. Technikaffinität

	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
Ich habe eine hohe Affinität zur Technik.	☐	☐	☐	☐	☐	☐	☐

F5. Bitte schätzen Sie, wie viele Stunden am Tag Sie sich mit Ihrem Smartphone oder Tablet beschäftigen.

- ☐ weniger als eine halbe Stunde
- ☐ mehr als eine halbe Stunde, aber weniger als eine Stunde
- ☐ mehr als eine Stunde, aber weniger als zwei Stunden
- ☐ mehr als zwei Stunden, aber weniger als vier Stunden
- ☐ mehr als vier Stunden

F6. Mir ist der Schutz meiner Privatsphäre wichtig.

trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
☐	☐	☐	☐	☐	☐	☐

F7. Sind Sie aktiv tätig, um Ihre Daten zu schützen?

- ☐ Nein.
- ☐ Ja.
- ☐ Ich habe eine Applikation installiert, um meine Daten zu schützen.
- ☐ Ich versuche so wenig wie möglich von meinen Daten preiszugeben.
- ☐ Ich lese die AGBs bevor ich eine Applikation installiere.
- ☐ Sonstiges

Sonstiges

F8. Bite geben Sie an welche Relevanz die folgende Punkte bei der Auswahl einer Applikation für sie haben.

	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	☐	☐	☐	☐	☐	☐	☐
Ich halte die Sterne für sehr relevant.	☐	☐	☐	☐	☐	☐	☐
Ich halte die Anzahl der Aufrufe für sehr relevant.	☐	☐	☐	☐	☐	☐	☐
Ich halte die Anzahl der Downloads für sehr relevant.	☐	☐	☐	☐	☐	☐	☐
Ich halte die Privatsphäreskala für sehr relevant.	☐	☐	☐	☐	☐	☐	☐

Anhang V. Szenarien

8 Szenarien:

1. **Messenger**

„Stell dir vor du möchtest dich mit einer Freundin zum Abendessen verabreden. Schreibe ihr eine Kurznachricht." *„Hallo, ich möchte dich heute Abend zum Essen einladen."*

2. **Video Konferenzen**

„Stell dir vor du bist auf einer Reise und möchtest mit einer Freundin sprechen. Starte eine Video-Konferenz mit Ihr."

3. **Wetter**

„Stell dir vor, du packst deinen Koffer für eine Reise und möchtest die Wettervorhersage anschauen, um die richtigen Sachen einzupacken."

4. **E-Mail**

„Stell dir vor, du möchtest eine Freundin zu einem Konzert einladen. Schreibe ihr eine E-Mail."
„Hallo, ich möchte dich heute zu einem Konzert einladen."

5. **Musik**

„Stell dir vor, du möchtest ein Lied der aktuellen Charts mit deinem Smartphone hören."

6. **Fitness**

„Stell dir vor, du möchtest deine körperlichen Aktivitäten nachvollziehen. Richte dafür eine Fitness-Applikation ein. (Die eingegebenen Daten können fiktiv, sollen jedoch nicht unrealistisch sein.)"

7. **Spiele**

„Stell dir vor, dir ist langweilig und du hast einen langen Flug unmittelbar vor dir. Zur Unterhaltung möchtest du dir das Spiel Sudoku herunterladen, welches du auf deinem Smartphone spielen kannst"

8. **Nachrichten / Neuigkeiten**

„Stell dir vor, du möchtest wissen, welche aktuellen Neuigkeiten es gibt. Öffne eine Nachrichten-Applikation."

Anhang W. Aufklärung über den Zweck der zweiten Studie

Version Gruppe A:

„Vielen Dank, dass Sie die Aufgaben bearbeitet haben. Ich möchte Sie nun darüber in Kenntnis setzen, dass Sie Proband/Probandin der Interventions-Stichprobe waren, die eine Privatsphäreskala im App-Markt präsentiert bekommen hat. Darüber hinaus haben Sie eine detaillierte Beschreibung über die eben genannte Skala erhalten. Ziel der Studie ist die Untersuchung der zugrundeliegenden Prozesse bei der Auswahl von Applikationen und ob diese Prozesse durch die Illustrierung weiterer Informationen die Nutzer dahingehend sensibilisieren, um ihnen eine möglichst adäquate Entscheidung zu ermöglichen, welche den Schutz der Privatsphäre miteinbezieht. Die Ausführungen der eigentlichen Aufgaben, wie sie in den Szenarien beschrieben waren, werden in der Auswertung nicht weiter berücksichtigt."

Version Gruppe B:

„Vielen Dank, dass Sie die Aufgaben bearbeitet haben. Ich möchte Sie nun darüber in Kenntnis setzen, dass Sie Proband/Probandin der Interventions-Stichprobe waren, die eine Privatsphäreskala im App-Markt präsentiert bekommen hat. Ziel der Studie ist die Untersuchung der zugrundeliegenden Prozesse bei der Auswahl von Applikationen und ob diese Prozesse durch die Illustrierung weiterer Informationen die Nutzer dahingehend sensibilisieren, um ihnen eine möglichst adäquate Entscheidung zu ermöglichen, welche den Schutz der Privatsphäre miteinbezieht. Die Ausführungen der eigentlichen Aufgaben, wie sie in den Szenarien beschrieben waren, werden in der Auswertung nicht weiter berücksichtigt."

Version Gruppe C:

„Vielen Dank, dass Sie die Aufgaben bearbeitet haben. Ich möchte Sie nun darüber in Kenntnis setzen, dass Sie Proband/Probandin der Kontroll-Stichprobe waren. Ziel der Studie ist die Untersuchung der zugrundeliegenden Prozesse bei der Auswahl von Applikationen und ob diese Prozesse durch die Illustrierung weiterer Informationen die Nutzer dahingehend sensibilisieren, um ihnen eine möglichst adäquate Entscheidung zu ermöglichen, welche den Schutz der Privatsphäre miteinbezieht. Die Ausführungen der eigentlichen Aufgaben, wie sie in den Szenarien beschrieben waren, werden in der Auswertung nicht weiter berücksichtigt."

Anhang X. Bildschirmabzug der A-Ware Applikation

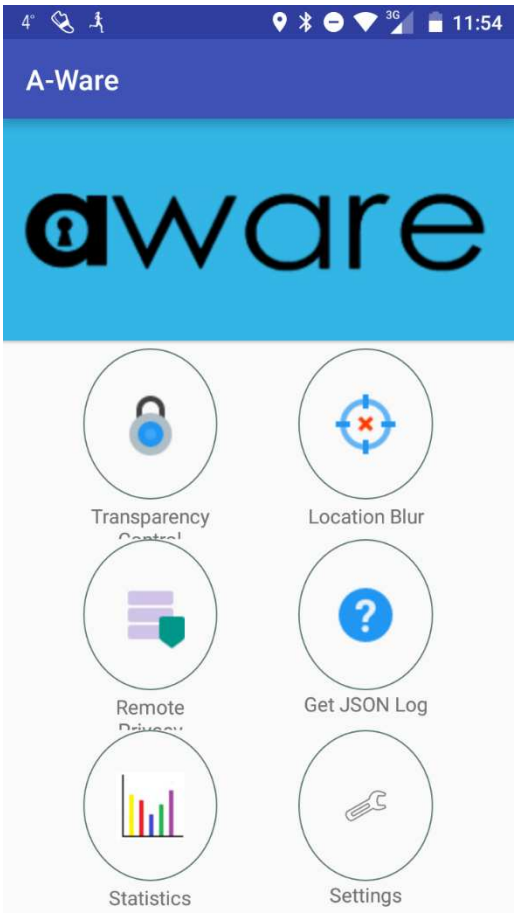


Abbildung 37. Bildschirmabzug der A-Ware Applikation.

Anhang Y. Tabellen zum zweiten Versuch

Tabelle 31 *Auflistung der Applikationen zur Messung der Aggressivität nach Kategorien*

Messenger	**Videokonferenz**	**Wetter**	**E-Mail**	**Musik**	**Fitness**	**Spiele**	**Nachrichten**
WhatsApp*	Skype*	Accu-Weather*	Microsoft Outlook	Play Musik*	Schrittzähler-Gratis Pedometer & Kalorienzähler *	Sudoku(Magma Mobile)*	FlipBoard*
Google Allo*	Google Duo*	Yr*	K-9 Mail	FreeMusic Player*	Pacer Health Schrittzähler & Abnehm-trainer	Sudoku classic (Quarzo Apps) *	bbc News*
Signal*	TrueConf	Wetter-Online*	AndroPots	Song Flip-Free MUsic Streaming & Player*	Google Fit	Sudoku (Volcano Entertainment)*	CNN Braking News*
Facebook Messenger*	JusTalk*	Bayer Agrar Wetter*	myMail	Deezer*	Endomondo	Sudoku(Card Games)*	News Suite*
Wire	Glide*	Weather Live (Innovative Team)*	Nine	**SoundCloud***	Fitbit	Sudoku Free (Titan IncGeduldsspiele)*	SQUID*
Kik	Zoom	Yahoo Wetter *	Blue Mail	**Spotify***	ASUS ZenFit	Sudoku Free (Jigsaw Puzzle Free)*	Euronews*
WeChat*	Video Call*	Morecast (UBIMET)*	MailDroid*	Freie Musik MH Musik*	Wandern Schrittzähler Diät	Sudoku (Timeglass Works)*	RT News*
Telegram*	Imo*	wetter.com*	ProtonMail*	Gratis Musik/ Free Musik (Notenschlüssel Bild)*	Strava Training	Material Sudoku (OkayCode)*	Die Zeit*
Hangouts	Tango*	Windy*	Go Mail	Audiomack Musik und Mixtapes*	Laufen zur Gewichts-abnahme	Sudoku Master (Dat Viet Entertainment)*	Google news*
Line*	Viber*	Weather-zone*	Open Mail*	Free Music Plus*	Sportractive workout	Sudoku kostenlos deutsch (Marco Meyer)*	Microsoft News*

*keine Angabe von persönlichen Daten möglich

Tabelle 32 *Friedman-Test der Bewertung der fünf Skalen*

Ränge	
	Mittlerer Rang
Bubble Scale	2,65
Arrow-Scale-Bar	2,38
Arrow-Scale-Meter	3,38
Label-Meter	3,51
Smiley-Meter	3,09

Teststatistiken	
H	168
Chi-Quadrat	80,465
df	4
Asymp. Sig.	,000

Tabelle 33 *Friedman-Test der Bewertung der sieben Skalen*

Ränge	
	Mittlerer Rang
Bubble Scale	3,96
Arrow-Scale-Bar	3,64
Arrow-Scale-Meter	4,20
Label-Meter	4,66
Smiley-Meter	4,53
Lock-Scale	3,74
Mask-Scale	3,27

Teststatistiken	
H	132
Chi-Quadrat	54,346
df	6
Asymp. Sig.	,000

Tabelle 34 *Häufigkeiten der Auswahl nach Dartstellungsposition in der Benutzeroberfläche*

Häufigkeiten									
Rang	Szenarien								
	Messenger	Videokonferenz	Wetter	E-mail	Musik	Fitness	Spiele	Nachrichten	Gesamt
1	5	59	1	40	61	32	21	6	225,00
2	0	1	2	4	0	2	1	8	18,00
3	11	2	18	9	1	6	2	6	55,00
4	2	14	21	3	0	4	3	0	47,00
5	2	1	22	0	1	7	38	51	122,00
6	3	0	16	1	18	2	6	0	46,00
7	0	0	0	18	1	1	1	1	22,00
8	52	0	0	0	0	25	0	6	83,00
9	7	0	2	4	0	2	1	4	20,00
10	0	0	0	3	0		9	0	12,00
11	3		0						3,00

Tabelle 35 *Demographische Daten Alter und Geschlecht*

Demographische Daten															
	Gruppe A			Gruppe B			Gruppe C			Gruppe D			Gesamt		
Alter	M	SD	NV	M	SD	NV	M	SD	NV	M	SD	NV	M	SD	NV
	29,95	9,06	0,009	35,53	13,99	0,002	31,82	11,31	0	31,58	10,98	0,032	32,15	11,37	0
	Männlich	Weiblich		Männlich	Weiblich		Männlich	Weiblich	k.A.	Männlich	Weiblich		Männlich	Weiblich	k.A.
Geschlecht	11	10		7	12		14	8	1	11	8		43	38	1

Tabelle 36 *Demographische Daten Bildung*

Bildung				
	Mittlere Reife	Abitur	Berufsausbildung	Akademische Abschluss
Gesamt	6	28	7	41

Tabelle 37 *Tägliche Handynutzung in Stunden*

Tägliche Handynutzung					
	<30 Min	30 Min - 1 Std	< 1 Std, aber > 2 Std	2- 4 Std	> 5 Std
Häufigkeit	1	6	25	37	13

Tabelle 38 *Technikaffinität*

Technikaffinität						
	trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft zu	trifft völlig zu
Häufigkeit	1	2	34	11	24	10

Tabelle 39 *Häufigkeiten der Auswahl zu allgemeinen Fragen bezüglich der Privatsphäre*

Allgemeine Fragen zur Privatsphäre			
Aussage	Auswahl	Häufigkeit	Prozent
Mir ist der Schutz meiner Privatsphäre wichtig.	trifft nicht zu	1	1,2
	trifft eher nicht zu	32	39,5
	weder noch	3	3,7
	trifft zu	23	28,4
	trifft völlig zu	22	27,2
	Gesamtsumme	81	100,0
Sind Sie aktiv tätig, um Ihre Daten zu schützen? [Nein.]	Ja	25	30,9
	Nein	56	69,1
	Gesamtsumme	81	100,0
Sind Sie aktiv tätig, um Ihre Daten zu schützen? [Ja.]	Ja	23	28,4
	Nein	58	71,6
	Gesamtsumme	81	100,0
Sind Sie aktiv tätig, um Ihre Daten zu schützen? [Ich habe eine Applikation installiert, um meine Daten zu schützen.]	Ja	8	9,9
	Nein	73	90,1
	Gesamtsumme	81	100,0
Sind Sie aktiv tätig, um Ihre Daten zu schützen? [Ich versuche so wenig wie möglich von meinen Daten preiszugeben.]	Ja	49	60,5
	Nein	32	39,5
	Gesamtsumme	81	100,0
Sind Sie aktiv tätig, um Ihre Daten zu schützen? [Ich lese die AGBs bevor ich eine Applikation installiere.]	Ja	17	21,0
	Nein	64	79,0
	Gesamtsumme	81	100,0
Sind Sie aktiv tätig, um Ihre Daten zu schützen? [Sonstiges]	No	75	92,6
	Ich habe oft das Gefühl, aus Nachlässigkeit mehr preiszugeben als ich sollte.	1	1,2
	Ich lese Reviews zum Datenschutz von Apps von fachkundigen Leuten	1	1,2
	Ich nutze ausschließlich Applegeräte.	1	1,2
	ich versuche nach Kosten/Nutzenprinzip mit meinen Daten zu verfahren	1	1,2
	Überprüfung der geforderten Zugriffberechtigung vor Installation	1	1,2
	Warte derzeit auf meine Google-freie Android-Version	1	1,2
	Gesamtsumme	81	100,0

Tabelle 40 *Demographische Daten Alter und Geschlecht für das Eye-Tracking-Video*

Demographische Daten																
	Gruppe A			Gruppe B			Gruppe C			Gruppe D			Gesamt			
Alter	M	SD	NV	M	SD	NV	M	SD	NV	M	SD	NV	M	SD	NV	
	27,78	4,532	0,2	35,25	13,051	0,006	30	10,488	0	29,56	6,723	0,047	30,5	9,403	0,047	
	Männlich	Weiblich		Männlich	Weiblich		Männlich	Weiblich	k.A.	Männlich	Weiblich		Männlich	Weiblich	k.A.	
Geschlecht	8	10		5	11		12	7	1	10	8		35	36	1	

Tabelle 41 *Entscheidungszeiten in Sekunden der jeweiligen Szenarien*

Entscheidungszeiten getrennt nach Szenarien			
	N	M	SD
Messenger	73	13,4275	18,04085
Videokonferenz	73	11,6969	28,15733
Wetter	73	17,0091	18,11631
E-Mail	73	28,2409	47,19668
Musik	73	11,2506	26,81233
Fitness	73	25,5285	41,22083
Spiele	73	19,7123	31,60119
Nachrichten	73	17,4526	20,36640

Tabelle 42 *Friedman-Test der Entscheidungszeiten zwischen den Szenarien*

Ränge								
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mittel Rang	4,21	2,99	5,00	5,64	2,86	5,90	4,71	4,69

Teststatistiken[a]	
H	73
Chi-Quadrat	105,790
Df	7
Asymp. Sig.	,000

a. Friedman-Test

Tabelle 43 *Wilcoxon-Test für den Vergleich der Entscheidungszeiten zwischen den Szenarien*

Ränge

		H	Mittlerer Rang	Summe der Ränge	Anmerkungen
Videokonferenz – Messenger	Negative Ränge	52[a]	38,02	1977,00	a. Videokonferenz< Messenger
	Positive Ränge	21[b]	34,48	724,00	b. Videokonferenz> Messenger
	Bindungen	0[c]			c. Videokonferenz= Messenger
	Gesamtsumme	73			
Wetter - Messenger	Negative Ränge	27[d]	34,91	942,50	d. Wetter < Messenger
	Positive Ränge	46[e]	38,23	1758,50	e. Wetter > Messenger
	Bindungen	0[f]			f. Wetter = Messenger
	Gesamtsumme	73			
E-Mail - Messenger	Negative Ränge	25[g]	27,62	690,50	g. E-Mail < Messenger
	Positive Ränge	48[h]	41,89	2010,50	h. E-Mail > Messenger
	Bindungen	0[i]			i. E-Mail = Messenger
	Gesamtsumme	73			
Musik - Messenger	Negative Ränge	49[j]	39,44	1932,50	j. Musik< Messenger
	Positive Ränge	24[k]	32,02	768,50	k. Musik> Messenger
	Bindungen	0[l]			l. Musik= Messenger
	Gesamtsumme	73			
Fitness - Messenger	Negative Ränge	22[m]	32,98	725,50	m. Fitness< Messenger
	Positive Ränge	51[n]	38,74	1975,50	n. Fitness> Messenger
	Bindungen	0[o]			o. Fitness= Messenger
	Gesamtsumme	73			
Spiele - Messenger	Negative Ränge	31[p]	32,74	1015,00	p. Spiele< Messenger
	Positive Ränge	42[q]	40,14	1686,00	q. Spiele> Messenger
	Bindungen	0[r]			r. Spiele= Messenger
	Gesamtsumme	73			
Nachrichten - Messenger	Negative Ränge	28[s]	33,43	936,00	s. Nachrichten< Messenger
	Positive Ränge	44[t]	38,45	1692,00	t. Nachrichten> Messenger
	Bindungen	1[u]			u. Nachrichten= Messenger
	Gesamtsumme	73			

Fortsetzung Tabelle 43

		H	Mittlerer Rang	Summe der Ränge	Anmerkungen
Fitness - Wetter	Negative Ränge	27[at]	34,33	927,00	at. Fitness< Wetter
	Positive Ränge	46[au]	38,57	1774,00	au. Fitness> Wetter
	Bindungen	0[av]			av. Fitness= Wetter
	Gesamtsumme	73			
Spiele - Wetter	Negative Ränge	40[aw]	31,38	1255,00	aw. Spiele< Wetter
	Positive Ränge	33[ax]	43,82	1446,00	ax. Spiele> Wetter
	Bindungen	0[ay]			ay. Spiele= Wetter
	Gesamtsumme	73			
Nachricht - Wetter	Negative Ränge	42[az]	33,27	1397,50	az. Nachrichten< Wetter
	Positive Ränge	31[ba]	42,05	1303,50	ba. Nachrichten> Wetter
	Bindungen	0[bb]			bb. Nachrichten= Wetter
	Gesamtsumme	73			
Musik – E-Mail	Negative Ränge	58[bc]	38,54	2235,50	bc. Musik < E-Mail
	Positive Ränge	14[bd]	28,04	392,50	bd. Musik > E-Mail
	Bindungen	1[be]			be. Musik = E-Mail
	Gesamtsumme	73			
Fitness – E-Mail	Negative Ränge	35[bf]	39,39	1378,50	bf. Fitness< E-Mail
	Positive Ränge	37[bg]	33,77	1249,50	bg. Fitness> E-Mail
	Bindungen	1[bh]			bh. Fitness= E-Mail
	Gesamtsumme	73			
Spiele – E-Mail	Negative Ränge	45[bi]	41,39	1862,50	bi. Spiele < E-Mail
	Positive Ränge	28[bj]	29,95	838,50	bj. Spiele > E-Mail
	Bindungen	0[bk]			bk. Spiele = E-Mail
	Gesamtsumme	73			
Nachrichten – E-Mail	Negative Ränge	47[bl]	39,29	1846,50	bl. Nachrichten < E-Mail
	Positive Ränge	26[bm]	32,87	854,50	bm. Nachrichten > E-Mail
	Bindungen	0[bn]			bn. Nachrichten = E-Mail
	Gesamtsumme	73			
Fitness – Musik	Negative Ränge	12[bo]	22,79	273,50	bo. Fitness< Musik
	Positive Ränge	61[bp]	39,80	2427,50	bp. Fitness> Musik
	Bindungen	0[bq]			bq. Fitness= Musik
	Gesamtsumme	73			

Fortsetzung Tabelle 43

		H	Mittlerer Rang	Summe der Ränge	Anmerkungen
Spiele – Musik	Negative Ränge	18[br]	31,39	565,00	br. Spiele < Musik
	Positive Ränge	55[bs]	38,84	2136,00	bs. Spiele > Musik
	Bindungen	0[bt]			bt. Spiele = Musik
	Gesamtsumme	73			
Nachrichten – Musik	Negative Ränge	15[bu]	31,70	475,50	bu. Nachrichten < Musik
	Positive Ränge	56[bv]	37,15	2080,50	bv. Nachrichten > Musik
	Bindungen	2[bw]			bw. Nachrichten = Musik
	Gesamtsumme	73			
Spiele -Fitness	Negative Ränge	51[bx]	37,86	1931,00	bx. Spiele < Fitness
	Positive Ränge	22[by]	35,00	770,00	by. Spiele > Fitness
	Bindungen	0[bz]			bz. Spiele = Fitness
	Gesamtsumme	73			
Nachrichten – Fitness	Negative Ränge	50[ca]	37,04	1852,00	ca. Nachrichten < Fitness
	Positive Ränge	22[cb]	35,27	776,00	cb. Nachrichten > Fitness
	Bindungen	1[cc]			cc. Nachrichten = Fitness
	Gesamtsumme	73			
Nachrichten – Spiele	Negative Ränge	37[cd]	36,20	1339,50	cd. Nachrichten < Spiele
	Positive Ränge	35[ce]	36,81	1288,50	ce. Nachrichten > Spiele
	Bindungen	1[cf]			cf. Nachrichten = Spiele
	Gesamtsumme	73			

Tabelle 44 *Entscheidungszeiten getrennt nach Szenarien und Gruppen*

Entscheidungszeiten getrennt nach Szenarien																			
Szenario	Gruppe A				Gruppe B				Gruppe C				Gruppe D				Gesamt			
	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV
Messenger	18	18,63	24,30	0	16	16,86	25,22	0	20	11,64	10,44	0,003	18	7,50	4,67	0,052	72	13,51	18,15	0
Videokonferenz	18	10,18	12,19	0,001	16	8,00	7,54	0,063	20	10,65	15,44	0	18	5,57	6,60	0,001	72	8,67	11,23	0
Wetter	18	14,55	12,72	0,001	16	20,71	23,79	0	20	19,09	21,34	0,003	18	11,80	9,19	0,009	72	16,49	17,69	0
E-Mail	18	24,31	32,81	0	16	16,97	15,49	0,002	20	27,08	37,28	0	18	28,51	46,75	0	72	24,50	34,96	0
Musik	18	8,99	15,39	0	16	6,89	6,21	0,117	20	19,48	46,16	0	18	4,76	3,42	0,003	72	10,38	25,93	0
Fitness	18	24,34	29,43	0	16	12,88	10,00	0,2	20	25,23	35,28	0	18	23,53	23,35	0,003	72	21,84	26,75	0
Spiele	18	28,75	53,12	0	16	12,64	7,65	0,2	20	14,33	17,25	0,002	18	17,32	15,72	0,013	72	18,31	29,44	0
Nachrichten	18	14,88	16,71	0,001	16	13,09	13,39	0,032	20	15,48	13,64	0,12	18	24,18	31,05	0	72	16,97	20,09	0
Gesamt		**18,08**	**24,58**			**13,50**	**13,66**			**17,87**	**24,61**			**15,40**	**17,59**			**16,33**	**23,03**	

Anmerkung. Entscheidungszeiten mit absteigender Länge verglichen unter den Gruppen farblich in folgender Reihenfolge markiert: rot, orange, gelb, grün. Vorhandene Normalverteilungen bei p > 0,05 wurden rosa markiert.

Tabelle 45 *Kruskal-Wallis-Test Vergleich der Entscheidungszeiten in Sekunden zwischen den Gruppen*

Ränge

	Gruppe	H	Mittlerer Rang
Entscheidungszeiten in Sekunden	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	37,17
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	36,88
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	37,00
	D: Keine Datenschutzskala	18	34,94
	Gesamtsumme	72	

Teststatistiken[a,b]

	EV_Alle_zeitAnteilEntscheidunginS
Chi-Quadrat	,134
df	3
Asymp. Sig.	,987

a. Kruskal-Wallis-Test

b. Gruppierungsvariable: Gruppe

Tabelle 46 *Mann-Whitney-U-Test Vergleich der Entscheidungszeiten zwischen den Gruppen*

Ränge				
	Gruppe	H	Mittlerer Rang	Summe der Ränge
Entscheidungszeiten Gesamt	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,22	310,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	17,81	285,00
	Gesamtsumme	34		
	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	19,94	359,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,10	382,00
	Gesamtsumme	38		
	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	19,00	342,00
	D: Keine Datenschutzskala	18	18,00	324,00
	Gesamtsumme	36		
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	18,06	289,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	18,85	377,00
	Gesamtsumme	36		
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	18,00	288,00
	D: Keine Datenschutzskala	18	17,06	307,00
	Gesamtsumme	34		
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,05	401,00
	D: Keine Datenschutzskala	18	18,89	340,00
	Gesamtsumme	38		

Fortsetzung Tabelle 46

Teststatistiken[a]

	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)	Exakte Sig. [2*(1-seitige Sig.)]
Gruppe A – Gruppe B	139,000	310,000	-,173	,863	,878[b]
Gruppe A – Gruppe C	172,000	382,000	-,234	,815	,828[b]
Gruppe A – Gruppe D	153,000	324,000	-,285	,776	,791[b]
Gruppe B – Gruppe C	153,000	289,000	-,223	,824	,838[b]
Gruppe B – Gruppe D	136,000	307,000	-,276	,783	,798[b]
Gruppe C – Gruppe D	169,000	340,000	-,322	,748	,762[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 47 *Mann-Whitney-U-Test Vergleich der Entscheidungszeiten zwischen den Gruppen A und B*

Ränge

Entscheidungszeiten	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,97	341,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	15,84	253,50
	Gesamtsumme	34		
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,47	332,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	16,41	262,50
	Gesamtsumme	34		
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,06	307,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	18,00	288,00
	Gesamtsumme	34		
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,78	338,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	16,06	257,00
	Gesamtsumme	34		

Fortsetzung Tabelle 47

Entscheidungszeiten	Gruppe	H	Mittlerer Rang	Summe der Ränge
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,28	311,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	17,75	284,00
	Gesamtsumme	34		
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	19,28	347,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	15,50	248,00
	Gesamtsumme	34		
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,78	338,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	16,06	257,00
	Gesamtsumme	34		
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,22	328,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf			

Teststatistiken[a]

	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	117,500	126,500	136,000	121,000	140,000	112,000	121,000	131,000
Wilcoxon-W	253,500	262,500	307,000	257,000	311,000	248,000	257,000	267,000
z	-,915	-,604	-,276	-,794	-,138	-1,104	-,794	-,449
Asymp. Sig. (2-seitig)	,360	,546	,782	,427	,890	,270	,427	,654
Exakte Sig. [2*(1-seitige Sig.)]	,365[b]	,551[b]	,798[b]	,443[b]	,905[b]	,281[b]	,443[b]	,670[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 48 *Mann-Whitney-U-Test Vergleich der Entscheidungszeiten zwischen den Gruppen A und C*

Ränge				
Entscheidungszeiten	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	22,28	401,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	17,00	340,00
	Gesamtsumme	38		
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	19,83	357,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,20	384,00
	Gesamtsumme	38		
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	20,33	366,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	18,75	375,00
	Gesamtsumme	38		
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,83	339,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,10	402,00
	Gesamtsumme	38		
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,22	310,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	21,55	431,00
	Gesamtsumme	38		
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,17	327,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,70	414,00
	Gesamtsumme	38		
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	22,44	404,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	16,85	337,00
	Gesamtsumme	38		
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	19,08	343,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,88	397,50
	Gesamtsumme	38		

Fortsetzung Tabelle 48

Teststatistiken[a]

Entscheidungszeiten	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	130,000	174,000	165,000	168,000	139,000	156,000	127,000	172,500
Wilcoxon-W	340,000	384,000	375,000	339,000	310,000	327,000	337,000	343,500
U	-1,462	-,175	-,439	-,351	-1,199	-,702	-1,550	-,219
Asymp. Sig. (2-seitig)	,144	,861	,661	,726	,231	,483	,121	,826
Exakte Sig. [2*(1-seitige Sig.)]	,149[b]	,874[b]	,675[b]	,740[b]	,239[b]	,496[b]	,126[b]	,828[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 49 *Mann-Whitney-U-Test Vergleich der Entscheidungszeiten zwischen den Gruppen A und D*

Ränge

Entscheidungszeiten	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	23,11	416,00
	D: Keine Datenschutzskala	18	13,89	250,00
	Gesamtsumme	36		
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	21,81	392,50
	D: Keine Datenschutzskala	18	15,19	273,50
	Gesamtsumme	36		
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	20,47	368,50
	D: Keine Datenschutzskala	18	16,53	297,50
	Gesamtsumme	36		
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	19,19	345,50
	D: Keine Datenschutzskala	18	17,81	320,50
	Gesamtsumme	36		

Fortsetzung Tabelle 49

Entscheidungszeiten	Gruppe	H	Mittlerer Rang	Summe der Ränge
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als			
	Einführung	18	19,39	349,00
	D: Keine Datenschutzskala	18	17,61	317,00
	Gesamtsumme	36		
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als			
	Einführung	18	18,11	326,00
	D: Keine Datenschutzskala	18	18,89	340,00
	Gesamtsumme	36		
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als			
	Einführung	18	19,44	350,00
	D: Keine Datenschutzskala	18	17,56	316,00
	Gesamtsumme	36		
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als			
	Einführung	18	17,17	309,00
	D: Keine Datenschutzskala	18	19,83	357,00
	Gesamtsumme	36		

Teststatistiken[a]

Entscheidungszeiten	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	79,000	102,500	126,500	149,500	146,000	155,000	145,000	138,000
Wilcoxon-W	250,000	273,500	297,500	320,500	317,000	326,000	316,000	309,000
z	-2,626	-1,883	-1,123	-,396	-,506	-,221	-,538	-,759
Asymp. Sig. (2-seitig)	,009	,060	,261	,692	,613	,825	,591	,448
Exakte Sig. [2*(1-seitige Sig.)]	,008[b]	,059[b]	,265[b]	,696[b]	,628[b]	,839[b]	,606[b]	,462[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 50 *Mann-Whitney-U-Test Vergleich der Entscheidungszeiten zwischen den Gruppen B und C*

Ränge

Entscheidungszeiten	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	18,94	303,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	18,15	363,00
	Gesamtsumme	36		
Videokonferenz	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	17,97	287,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	18,93	378,50
	Gesamtsumme	36		
Wetter	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	19,47	311,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	17,73	354,50
	Gesamtsumme	36		
E-Mail	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	16,50	264,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,10	402,00
	Gesamtsumme	36		
Musik	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	16,19	259,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,35	407,00
	Gesamtsumme	36		
Fitness	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	14,50	232,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	21,70	434,00
	Gesamtsumme	36		
Spiele	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	20,25	324,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	17,10	342,00
	Gesamtsumme	36		
Nachrichten	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	17,25	276,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,50	390,00
	Gesamtsumme	36		

Fortsetzung Tabelle 50

Teststatistiken[a]

Entscheidungszeiten	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	153,000	151,500	144,500	128,000	123,000	96,000	132,000	140,000
Wilcoxon-W	363,000	287,500	354,500	264,000	259,000	232,000	342,000	276,000
z	-,223	-,271	-,493	-1,019	-1,178	-2,037	-,891	-,637
Asymp. Sig. (2-seitig)	,824	,787	,622	,308	,239	,042	,373	,524
Exakte Sig. [2*(1-seitige Sig.)]	,838[b]	,789[b]	,626[b]	,320[b]	,249[b]	,042[b]	,386[b]	,539[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 51 *Mann-Whitney-U-Test Vergleich der Entscheidungszeiten zwischen den Gruppen B und D*

Ränge

Entscheidungszeiten	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	20,06	321,00
	D: Keine Datenschutzskala	18	15,22	274,00
	Gesamtsumme	34		
Videokonferenz	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	19,53	312,50
	D: Keine Datenschutzskala	18	15,69	282,50
	Gesamtsumme	34		
Wetter	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	19,47	311,50
	D: Keine Datenschutzskala	18	15,75	283,50
	Gesamtsumme	34		
E-Mail	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	17,44	279,00
	D: Keine Datenschutzskala	18	17,56	316,00
	Gesamtsumme	34		

Fortsetzung Tabelle 51

Entscheidungszeiten	Gruppe	H	Mittlerer Rang	Summe der Ränge
Musik	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	18,69	299,00
	D: Keine Datenschutzskala	18	16,44	296,00
	Gesamtsumme	34		
Fitness	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	15,22	243,50
	D: Keine Datenschutzskala	18	19,53	351,50
	Gesamtsumme	34		
Spiele	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	16,78	268,50
	D: Keine Datenschutzskala	18	18,14	326,50
	Gesamtsumme	34		
Nachrichten	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	15,50	248,00
	D: Keine Datenschutzskala	18	19,28	347,00
	Gesamtsumme	34		

Teststatistiken[a]

Entscheidungszeiten	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	103,000	111,500	112,500	143,000	125,000	107,500	132,500	112,000
Wilcoxon-W	274,000	282,500	283,500	279,000	296,000	243,500	268,500	248,000
z	-1,415	-1,122	-1,087	-,035	-,656	-1,259	-,397	-1,104
Asymp. Sig. (2-seitig)	,157	,262	,277	,972	,512	,208	,692	,270
Exakte Sig. [2*(1-seitige Sig.)]	,164[b]	,266[b]	,281[b]	,986[b]	,528[b]	,211[b]	,695[b]	,281[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 52 *Mann-Whitney-U-Test Vergleich der Entscheidungszeiten zwischen den Gruppen C und D*

Ränge				
Entscheidungszeiten	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	21,55	431,00
	D: Keine Datenschutzskala	18	17,22	310,00
	Gesamtsumme	38		
Videokonferenz	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	22,88	457,50
	D: Keine Datenschutzskala	18	15,75	283,50
	Gesamtsumme	38		
Wetter	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,45	409,00
	D: Keine Datenschutzskala	18	18,44	332,00
	Gesamtsumme	38		
E-Mail	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,70	414,00
	D: Keine Datenschutzskala	18	18,17	327,00
	Gesamtsumme	38		
Musik	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	22,98	459,50
	D: Keine Datenschutzskala	18	15,64	281,50
	Gesamtsumme	38		
Fitness	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,40	408,00
	D: Keine Datenschutzskala	18	18,50	333,00
	Gesamtsumme	38		
Spiele	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	17,50	350,00
	D: Keine Datenschutzskala	18	21,72	391,00
	Gesamtsumme	38		
Nachrichten	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	18,50	370,00
	D: Keine Datenschutzskala	18	20,61	371,00
	Gesamtsumme	38		

Fortsetzung Tabelle 52

Teststatistiken[a]								
Entscheidungszeiten	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	139,000	112,500	161,000	156,000	110,500	162,000	140,000	160,000
Wilcoxon-W	310,000	283,500	332,000	327,000	281,500	333,000	350,000	370,000
z	-1,199	-1,974	-,555	-,702	-2,032	-,526	-1,169	-,585
Asymp. Sig. (2-seitig)	,231	,048	,579	,483	,042	,599	,242	,559
Exakte Sig. [2*(1-seitige Sig.)]	,239[b]	,048[b]	,593[b]	,496[b]	,041[b]	,613[b]	,251[b]	,573[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 53 *Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen*

Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen							
App	1&2	2 & 3	3 & 4	4 & 5	5 & 6	6 & 7	7 & 8
M	3,14	-0,34	-1,58	-1,78	-5,31	8,36	3,81
SD	23,34	18,25	17,50	27,71	22,99	41,52	31,20
NV (p)	,000	,000	,000	,000	,000	,000	,000

Anmerkung. Differenzen der Entscheidungszeiten nach Größe farblich in folgender Reihenfolge markiert: dunkelgrün (höchste Zeiteinsparung in Sekunden), hellgrün, gelb hellorange, dunkelorange, rosa, rot (größte Differenz im Vergleich zum vorherigen Szenario).

Tabelle 54 *Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen nach Gruppen*

Entscheidungszeiten der chronologisch-sortierten Applikationen nach Gruppen

	Gruppe A			Gruppe B			Gruppe C			Gruppe D		
App	M	SD	NV	M	SD	NV	M	SD	NV	M	SD	NV
1 & 2	1,86	11,58	,200	17,21	26,46	,000	5,10	12,06	,048	-10,27	31,28	,000
2 & 3	-3,80	8,15	,780	0,97	8,03	,200	-3,38	17,14	,001	5,36	29,66	,000
3 & 4	-4,65	14,47	,200	-6,27	15,32	,006	-0,53	21,02	,018	4,49	17,23	,030
4 & 5	-0,55	21,92	,006	5,91	16,20	,130	-3,69	39,09	,000	-7,71	26,23	,007
5 & 6	-1,11	16,27	,001	-5,27	12,33	,004	-6,04	10,44	,200	-8,74	40,67	,005
6 & 7	-0,89	10,94	,000	5,14	10,94	,017	7,37	14,47	,027	21,56	48,05	,001
7 & 8	11,06	51,23	,000	-0,74	8,06	,167	5,78	33,08	,000	-1,57	7,08	,200

Anmerkung. Entscheidungszeiten der chronologisch sortierten Applikationen verglichen unter den Gruppen farblich in aufsteigender Reihenfolge markiert: rot, orange, gelb, grün. Vorhandene Normalverteilungen bei $p > 0{,}05$ wurden rosa markiert.

Tabelle 55 *Kruskal-Wallis-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppen*

Ränge

	Gruppe	H	Mittlerer Rang
App 1 & 2	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	35,22
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	46,88
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	38,38
	D: Keine Datenschutzskala	18	26,47
	Gesamtsumme	72	
App 2 & 3	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	33,03
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	42,09
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	36,73
	D: Keine Datenschutzskala	18	34,75
	Gesamtsumme	72	

Fortsetzung Tabelle 55

	Gruppe	H	Mittlerer Rang
App 3 & 4	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	32,19
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	33,06
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	36,13
	D: Keine Datenschutzskala	18	44,28
	Gesamtsumme	72	
App 4 & 5	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	39,06
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	39,31
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	35,55
	D: Keine Datenschutzskala	18	32,50
	Gesamtsumme	72	
App 5 & 6	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	36,97
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	36,69
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	32,73
	D: Keine Datenschutzskala	18	40,06
	Gesamtsumme	72	
App 6 & 7	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	34,28
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	30,84
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	40,63
	D: Keine Datenschutzskala	18	39,17
	Gesamtsumme	72	
App 7 & 8	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	38,69
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	35,97
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	37,03
	D: Keine Datenschutzskala	18	34,19
	Gesamtsumme	72	

Fortsetzung Tabelle 55

Teststatistiken[a,b]							
	App 1 & 2	App 2 & 3	App 3 & 4	App 4 & 5	App 5 & 6	App 6 & 7	App 7 & 8
Chi-Quadrat	8,292	1,767	3,686	1,256	1,181	2,441	,439
df	3	3	3	3	3	3	3
Asymp. Sig.	,040	,622	,297	,740	,758	,486	,932

a. Kruskal-Wallis-Test

b. Gruppierungsvariable: Gruppe

Tabelle 56 *Mann-Whitney-U-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppe A und B*

Ränge				
	Gruppe	H	Mittlerer Rang	Summe der Ränge
App 1 & 2	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	14,78	266,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	20,56	329,00
	Gesamtsumme	34		
App 2 & 3	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	15,22	274,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	20,06	321,00
	Gesamtsumme	34		
App 3 & 4	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,06	307,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	18,00	288,00
	Gesamtsumme	34		
App 4 & 5	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,22	310,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	17,81	285,00
	Gesamtsumme	34		

Fortsetzung Tabelle 56

	Gruppe	H	Mittlerer Rang	Summe der Ränge
App 5 & 6	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,28	311,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	17,75	284,00
	Gesamtsumme	34		
App 6 & 7	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,50	333,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	16,38	262,00
	Gesamtsumme	34		
App 7 & 8	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,03	324,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	16,91	270,50
	Gesamtsumme	34		

Teststatistiken[a]

	App 1 & 2	App 2 & 3	App 3 & 4	App 4 & 5	App 5 & 6	App 6 & 7	App 7 & 8
Mann-Whitney-U-Test	95,000	103,000	136,000	139,000	140,000	126,000	134,500
Wilcoxon-W	266,000	274,000	307,000	310,000	311,000	262,000	270,500
z	-1,691	-1,415	-,276	-,173	-,138	-,621	-,328
Asymp. Sig. (2-seitig)	,091	,157	,783	,863	,890	,535	,743
Exakte Sig. [2*(1-seitige Sig.)]	,095[b]	,164[b]	,798[b]	,878[b]	,905[b]	,551[b]	,746[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 57 *Mann-Whitney-U-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppe A und C*

Ränge				
	Gruppe	H	Mittlerer Rang	Summe der Ränge
App 1 & 2	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,61	335,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,30	406,00
	Gesamtsumme	38		
App 2 & 3	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,42	331,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,48	409,50
	Gesamtsumme	38		
App 3 & 4	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,19	327,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,68	413,50
	Gesamtsumme	38		
App 4 & 5	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	20,78	374,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	18,35	367,00
	Gesamtsumme	38		
App 5 & 6	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	20,92	376,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	18,23	364,50
	Gesamtsumme	38		
App 6 & 7	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,56	316,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	21,25	425,00
	Gesamtsumme	38		
App 7 & 8	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	20,11	362,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	18,95	379,00
	Gesamtsumme	38		

Fortsetzung Tabelle 57

Teststatistiken[a]

	App 1 & 2	App 2 & 3	App 3 & 4	App 4 & 5	App 5 & 6	App 6 & 7	App 7 & 8
Mann-Whitney-U-Test	164,000	160,500	156,500	157,000	154,500	145,000	169,000
Wilcoxon-W	335,000	331,500	327,500	367,000	364,500	316,000	379,000
z	-,468	-,570	-,687	-,672	-,746	-1,023	-,322
Asymp. Sig. (2-seitig)	,640	,569	,492	,501	,456	,306	,748
Exakte Sig. [2*(1-seitige Sig.)]	,654[b]	,573[b]	,496[b]	,515[b]	,460[b]	,317[b]	,762[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 58 *Mann-Whitney-U-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppe A und D*

Ränge

	Gruppe	H	Mittlerer Rang	Summe der Ränge
App 1 & 2	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	20,83	375,00
	D: Keine Datenschutzskala	18	16,17	291,00
	Gesamtsumme	36		
App 2 & 3	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,39	331,00
	D: Keine Datenschutzskala	18	18,61	335,00
	Gesamtsumme	36		
App 3 & 4	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	15,94	287,00
	D: Keine Datenschutzskala	18	21,06	379,00
	Gesamtsumme	36		
App 4 & 5	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	20,06	361,00
	D: Keine Datenschutzskala	18	16,94	305,00
	Gesamtsumme	36		
App 5 & 6	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,78	320,00
	D: Keine Datenschutzskala	18	19,22	346,00
	Gesamtsumme	36		

Fortsetzung Tabelle 58

	Gruppe	H	Mittlerer Rang	Summe der Ränge
App 6 & 7	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,22	310,00
	D: Keine Datenschutzskala	18	19,78	356,00
	Gesamtsumme	36		
App 7 & 8	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	19,56	352,00
	D: Keine Datenschutzskala	18	17,44	314,00
	Gesamtsumme	36		

Teststatistiken[a]

	App 1 & 2	App 2 & 3	App 3 & 4	App 4 & 5	App 5 & 6	App 6 & 7	App 7 & 8
Mann-Whitney-U-Test	120,000	160,000	116,000	134,000	149,000	139,000	143,000
Wilcoxon-W	291,000	331,000	287,000	305,000	320,000	310,000	314,000
z	-1,329	-,063	-1,455	-,886	-,411	-,728	-,601
Asymp. Sig. (2-seitig)	,184	,950	,146	,376	,681	,467	,548
Exakte Sig. [2*(1-seitige Sig.)]	,192[b]	,963[b]	,152[b]	,389[b]	,696[b]	,481[b]	,563[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 59 *Mann-Whitney-U-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppe B und C*

Ränge				
	Gruppe	H	Mittlerer Rang	Summe der Ränge
App 1 & 2	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	21,25	340,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	16,30	326,00
	Gesamtsumme	36		
App 2 & 3	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	19,72	315,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	17,53	350,50
	Gesamtsumme	36		
App 3 & 4	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	17,81	285,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,05	381,00
	Gesamtsumme	36		
App 4 & 5	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	19,44	311,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	17,75	355,00
	Gesamtsumme	36		
App 5 & 6	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	19,56	313,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	17,65	353,00
	Gesamtsumme	36		
App 6 & 7	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	15,41	246,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,98	419,50
	Gesamtsumme	36		
App 7 & 8	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	18,19	291,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	18,75	375,00
	Gesamtsumme	36		

Fortsetzung Tabelle 59

Teststatistiken[a]

	App 1 & 2	App 2 & 3	App 3 & 4	App 4 & 5	App 5 & 6	App 6 & 7	App 7 & 8
Mann-Whitney-U-Test	116,000	140,500	149,000	145,000	143,000	110,500	155,000
Wilcoxon-W	326,000	350,500	285,000	355,000	353,000	246,500	291,000
z	-1,401	-,621	-,350	-,478	-,541	-1,576	-,159
Asymp. Sig. (2-seitig)	,161	,535	,726	,633	,588	,115	,874
Exakte Sig. [2*(1-seitige Sig.)]	,168[b]	,539[b]	,741[b]	,648[b]	,604[b]	,116[b]	,888[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 60 *Mann-Whitney-U-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppe B und D*

Ränge

	Gruppe	H	Mittlerer Rang	Summe der Ränge
App 1 & 2	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	22,06	353,00
	D: Keine Datenschutzskala	18	13,44	242,00
	Gesamtsumme	34		
App 2 & 3	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	19,31	309,00
	D: Keine Datenschutzskala	18	15,89	286,00
	Gesamtsumme	34		
App 3 & 4	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	14,25	228,00
	D: Keine Datenschutzskala	18	20,39	367,00
	Gesamtsumme	34		
App 4 & 5	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	19,06	305,00
	D: Keine Datenschutzskala	18	16,11	290,00
	Gesamtsumme	34		
App 5 & 6	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	16,38	262,00
	D: Keine Datenschutzskala	18	18,50	333,00
	Gesamtsumme	34		
App 6 & 7	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	16,06	257,00
	D: Keine Datenschutzskala	18	18,78	338,00
	Gesamtsumme	34		
App 7 & 8	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	17,88	286,00
	D: Keine Datenschutzskala	18	17,17	309,00
	Gesamtsumme	34		

Fortsetzung Tabelle 60

Teststatistiken[a]							
	App 1 & 2	App 2 & 3	App 3 & 4	App 4 & 5	App 5 & 6	App 6 & 7	App 7 & 8
Mann-Whitney-U-Test	71,000	115,000	92,000	119,000	126,000	121,000	138,000
Wilcoxon-W	242,000	286,000	228,000	290,000	262,000	257,000	309,000
z	-2,519	-1,001	-1,794	-,863	-,621	-,794	-,207
Asymp. Sig. (2-seitig)	,012	,317	,073	,388	,535	,427	,836
Exakte Sig. [2*(1-seitige Sig.)]	,011[b]	,330[b]	,075[b]	,403[b]	,551[b]	,443[b]	,851[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 61 *Mann-Whitney-U-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppe C und D*

Ränge				
	Gruppe	H	Mittlerer Rang	Summe der Ränge
App 1 & 2	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	22,78	455,50
	D: Keine Datenschutzskala	18	15,86	285,50
	Gesamtsumme	38		
App 2 & 3	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,73	394,50
	D: Keine Datenschutzskala	18	19,25	346,50
	Gesamtsumme	38		
App 3 & 4	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	17,40	348,00
	D: Keine Datenschutzskala	18	21,83	393,00
	Gesamtsumme	38		
App 4 & 5	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,45	409,00
	D: Keine Datenschutzskala	18	18,44	332,00
	Gesamtsumme	38		
App 5 & 6	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	17,85	357,00
	D: Keine Datenschutzskala	18	21,33	384,00
	Gesamtsumme	38		

Fortsetzung Tabelle 61

	Gruppe	H	Mittlerer Rang	Summe der Ränge
App 6 & 7	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,40	388,00
	D: Keine Datenschutzskala	18	19,61	353,00
	Gesamtsumme	38		
App 7 & 8	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,33	406,50
	D: Keine Datenschutzskala	18	18,58	334,50
	Gesamtsumme	38		

Teststatistiken[a]

	App 1 & 2	App 2 & 3	App 3 & 4	App 4 & 5	App 5 & 6	App 6 & 7	App 7 & 8
Mann-Whitney-U-Test	114,500	175,500	138,000	161,000	147,000	178,000	163,500
Wilcoxon-W	285,500	346,500	348,000	332,000	357,000	388,000	334,500
z	-1,915	-,132	-1,228	-,555	-,965	-,058	-,482
Asymp. Sig. (2-seitig)	,055	,895	,219	,579	,335	,953	,630
Exakte Sig. [2*(1-seitige Sig.)]	,055[b]	,897[b]	,228[b]	,593[b]	,346[b]	,965[b]	,633[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 62 *T-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppen A und B*

		Test bei unabhängigen Stichproben								
		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	95 % Konfidenzintervall der Differenz	
									Unterer	Oberer
App 1 & 2	Varianzgleichheit angenommen	7,220	,011	-2,236	32	,032	-15,35475	6,86853	-29,34547	-1,36402
	Varianzgleichheit nicht angenommen			-2,145	20,033	,044	-15,35475	7,15760	-30,28368	-,42581
App 2 & 3	Varianzgleichheit angenommen	,109	,743	-1,717	32	,096	-4,77720	2,78178	-10,44350	,88910
	Varianzgleichheit nicht angenommen			-1,719	31,636	,095	-4,77720	2,77938	-10,44116	,88676
App 3 & 4	Varianzgleichheit angenommen	,174	,680	,318	32	,752	1,62760	5,11145	-8,78407	12,03928
	Varianzgleichheit nicht angenommen			,317	31,012	,753	1,62760	5,12922	-8,83335	12,08856
App 4 & 5	Varianzgleichheit angenommen	,243	,625	-,966	32	,341	-6,45689	6,68321	-20,07013	7,15636
	Varianzgleichheit nicht angenommen			-,983	31,035	,333	-6,45689	6,56544	-19,84658	6,93280
App 5 & 6	Varianzgleichheit angenommen	,033	,857	,833	32	,411	4,16696	5,00145	-6,02067	14,35458
	Varianzgleichheit nicht angenommen			,847	31,273	,403	4,16696	4,92021	-5,86434	14,19825
App 6 & 7	Varianzgleichheit angenommen	2,202	,148	-,364	32	,718	-6,02459	16,55878	-39,75373	27,70454
	Varianzgleichheit nicht angenommen			-,385	18,069	,705	-6,02459	15,63638	-38,86644	26,81725
App 7 & 8	Varianzgleichheit angenommen	2,209	,147	,910	32	,370	11,80006	12,96848	-14,61586	38,21598
	Varianzgleichheit nicht angenommen			,964	17,943	,348	11,80006	12,24142	-13,92401	37,52413

Tabelle 63 *T-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppen A und C*

Test bei unabhängigen Stichproben										
		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	95 % Konfidenzintervall der Differenz	
									Unterer	Oberer
App 1 & 2	Varianzgleichheit angenommen	,000	,991	-,842	36	,406	-3,23704	3,84577	-11,03663	4,56255
	Varianzgleichheit nicht angenommen			-,844	35,832	,405	-3,23704	3,83747	-11,02106	4,54699
App 2 & 3	Varianzgleichheit angenommen	1,207	,279	-,094	36	,925	-,41782	4,43662	-9,41570	8,58005
	Varianzgleichheit nicht angenommen			-,097	27,783	,923	-,41782	4,28775	-9,20397	8,36832
App 3 & 4	Varianzgleichheit angenommen	,254	,617	-,696	36	,491	-4,12292	5,92153	-16,13234	7,88651
	Varianzgleichheit nicht angenommen			-,710	33,799	,483	-4,12292	5,80828	-15,92934	7,68351
App 4 & 5	Varianzgleichheit angenommen	,223	,640	,300	36	,766	3,13426	10,44411	-18,04739	24,31590
	Varianzgleichheit nicht angenommen			,309	30,442	,760	3,13426	10,15370	-17,58975	23,85827
App 5 & 6	Varianzgleichheit angenommen	,129	,721	1,125	36	,268	4,93727	4,38971	-3,96548	13,84002
	Varianzgleichheit nicht angenommen			1,100	28,451	,281	4,93727	4,48973	-4,25297	14,12751
App 6 & 7	Varianzgleichheit angenommen	2,005	,165	-,551	36	,585	-8,25949	14,97739	-38,63505	22,11607
	Varianzgleichheit nicht angenommen			-,525	18,502	,606	-8,25949	15,73174	-41,24646	24,72748
App 7 & 8	Varianzgleichheit angenommen	,487	,490	,381	36	,705	5,27662	13,84776	-22,80794	33,36118
	Varianzgleichheit nicht angenommen			,373	28,554	,712	5,27662	14,15974	-23,70298	34,25622

Tabelle 64 *T-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppen A und D*

Test bei unabhängigen Stichproben										
		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	95 % Konfidenzintervall der Differenz	
									Unterer	Oberer
App 1 & 2	Varianzgleichheit angenommen	3,003	,092	1,543	34	,132	12,12731	7,86182	-3,84982	28,10445
	Varianzgleichheit nicht angenommen			1,543	21,578	,137	12,12731	7,86182	-4,19559	28,45022
App 2 & 3	Varianzgleichheit angenommen	4,606	,039	-1,264	34	,215	-9,15972	7,24938	-23,89224	5,57280
	Varianzgleichheit nicht angenommen			-1,264	19,553	,221	-9,15972	7,24938	-24,30386	5,98441
App 3 & 4	Varianzgleichheit angenommen	,420	,521	-1,722	34	,094	-9,13194	5,30283	-19,90859	1,64470
	Varianzgleichheit nicht angenommen			-1,722	33,016	,094	-9,13194	5,30283	-19,92043	1,65654
App 4 & 5	Varianzgleichheit angenommen	,861	,360	,888	34	,381	7,15741	8,05631	-9,21499	23,52981
	Varianzgleichheit nicht angenommen			,888	32,962	,381	7,15741	8,05631	-9,23401	23,54883
App 5 & 6	Varianzgleichheit angenommen	2,850	,101	,740	34	,464	7,63889	10,32398	-13,34196	28,61974
	Varianzgleichheit nicht angenommen			,740	22,305	,467	7,63889	10,32398	-13,75479	29,03256
App 6 & 7	Varianzgleichheit angenommen	,007	,934	-1,175	34	,248	-22,44907	19,11290	-61,29117	16,39302
	Varianzgleichheit nicht angenommen			-1,175	31,233	,249	-22,44907	19,11290	-61,41834	16,52019
App 7 & 8	Varianzgleichheit angenommen	2,732	,108	1,036	34	,307	12,62963	12,18931	-12,14202	37,40128
	Varianzgleichheit nicht angenommen			1,036	17,649	,314	12,62963	12,18931	-13,01572	38,27498

Tabelle 65 *T-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppen B und C*

Test bei unabhängigen Stichproben										
		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	95 % Konfidenzintervall der Differenz	
									Unterer	Oberer
App 1 & 2	Varianzgleichheit angenommen	7,573	,009	1,829	34	,076	12,11771	6,62589	-1,34771	25,58313
	Varianzgleichheit nicht angenommen			1,696	19,961	,105	12,11771	7,14450	-2,78733	27,02275
App 2 & 3	Varianzgleichheit angenommen	1,399	,245	,936	34	,356	4,35937	4,65621	-5,10319	13,82194
	Varianzgleichheit nicht angenommen			1,007	28,176	,322	4,35937	4,32774	-4,50310	13,22185
App 3 & 4	Varianzgleichheit angenommen	,035	,853	-,916	34	,366	-5,75052	6,28057	-18,51417	7,01313
	Varianzgleichheit nicht angenommen			-,948	33,757	,350	-5,75052	6,06455	-18,07844	6,57740
App 4 & 5	Varianzgleichheit angenommen	,531	,471	,918	34	,365	9,59115	10,44517	-11,63600	30,81830
	Varianzgleichheit nicht angenommen			,996	26,491	,328	9,59115	9,63419	-10,19436	29,37666
App 5 & 6	Varianzgleichheit angenommen	,041	,841	,203	34	,840	,77031	3,79578	-6,94363	8,48426
	Varianzgleichheit nicht angenommen			,199	29,489	,844	,77031	3,86796	-7,13486	8,67549
App 6 & 7	Varianzgleichheit angenommen	,966	,333	-,511	34	,612	-2,23490	4,36987	-11,11554	6,64575
	Varianzgleichheit nicht angenommen			-,528	33,917	,601	-2,23490	4,23571	-10,84366	6,37387
App 7 & 8	Varianzgleichheit angenommen	1,253	,271	-,769	34	,447	-6,52344	8,48541	-23,76787	10,72100
	Varianzgleichheit nicht angenommen			-,851	21,771	,404	-6,52344	7,66548	-22,43037	9,38350

Tabelle 66 *T-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppen B und D*

Test bei unabhängigen Stichproben										
		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	95 % Konfidenzintervall der Differenz	
									Unterer	Oberer
App 1 & 2	Varianzgleichheit angenommen	,025	,875	2,747	32	,010	27,48206	10,00582	7,10088	47,86324
	Varianzgleichheit nicht angenommen			2,774	31,934	,009	27,48206	9,90585	7,30287	47,66125
App 2 & 3	Varianzgleichheit angenommen	4,452	,043	-,572	32	,571	-4,38252	7,66385	-19,99327	11,22823
	Varianzgleichheit nicht angenommen			-,603	19,771	,554	-4,38252	7,27311	-19,56525	10,80021
App 3 & 4	Varianzgleichheit angenommen	,064	,802	-1,914	32	,065	-10,75955	5,62195	-22,21109	,69199
	Varianzgleichheit nicht angenommen			-1,927	31,999	,063	-10,75955	5,58235	-22,13044	,61134
App 4 & 5	Varianzgleichheit angenommen	2,339	,136	1,793	32	,082	13,61429	7,59403	-1,85424	29,08283
	Varianzgleichheit nicht angenommen			1,842	28,732	,076	13,61429	7,39082	-1,50775	28,73633
App 5 & 6	Varianzgleichheit angenommen	3,042	,091	,328	32	,745	3,47193	10,58975	-18,09869	25,04256
	Varianzgleichheit nicht angenommen			,345	20,451	,734	3,47193	10,06916	-17,50228	24,44615
App 6 & 7	Varianzgleichheit angenommen	4,228	,048	-1,335	32	,191	-16,42448	12,30595	-41,49089	8,64193
	Varianzgleichheit nicht angenommen			-1,410	18,966	,175	-16,42448	11,65147	-40,81425	7,96529
App 7 & 8	Varianzgleichheit angenommen	,206	,653	,320	32	,751	,82957	2,59512	-4,45652	6,11566
	Varianzgleichheit nicht angenommen			,317	30,131	,753	,82957	2,61547	-4,51095	6,17010

Tabelle 67 *T-Test Vergleich der Differenzen der Entscheidungszeiten der chronologisch-sortierten Applikationen zwischen den Gruppen C und D*

Test bei unabhängigen Stichproben

		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	95 % Konfidenzintervall der Differenz	
									Unterer	Oberer
App 1 & 2	Varianzgleichheit angenommen	3,265	,079	2,037	36	,049	15,36435	7,54088	,07073	30,65797
	Varianzgleichheit nicht angenommen			1,957	21,507	,063	15,36435	7,84990	-,93699	31,66569
App 2 & 3	Varianzgleichheit angenommen	1,812	,187	-1,127	36	,267	-8,74190	7,75976	-24,47943	6,99563
	Varianzgleichheit nicht angenommen			-1,097	26,609	,283	-8,74190	7,97232	-25,11101	7,62721
App 3 & 4	Varianzgleichheit angenommen	,000	,993	-,798	36	,430	-5,00903	6,27849	-17,74240	7,72435
	Varianzgleichheit nicht angenommen			-,806	35,710	,425	-5,00903	6,21207	-17,61125	7,59319
App 4 & 5	Varianzgleichheit angenommen	,010	,920	,368	36	,715	4,02315	10,92771	-18,13927	26,18557
	Varianzgleichheit nicht angenommen			,376	33,416	,709	4,02315	10,70593	-17,74793	25,79423
App 5 & 6	Varianzgleichheit angenommen	4,152	,049	,287	36	,776	2,70162	9,40833	-16,37936	21,78260
	Varianzgleichheit nicht angenommen			,274	19,019	,787	2,70162	9,86596	-17,94670	23,34995
App 6 & 7	Varianzgleichheit angenommen	3,694	,063	-1,260	36	,216	-14,18958	11,25872	-37,02332	8,64415
	Varianzgleichheit nicht angenommen			-1,205	19,769	,243	-14,18958	11,77913	-38,77881	10,39964
App 7 & 8	Varianzgleichheit angenommen	1,693	,201	,923	36	,362	7,35301	7,96538	-8,80154	23,50755
	Varianzgleichheit nicht angenommen			,970	20,922	,343	7,35301	7,58199	-8,41815	23,12417

Tabelle 68 *Fixationszeiten auf Symbol, Text und Skala nach Gruppen*

Fixationszeiten auf die jeweiligen Gebiete nach Gruppen															
	Gruppe A			Gruppe B			Gruppe C			Gruppe D			Gesamt		
Gebiet	M	SD	NV	M	SD	NV	M	SD	NV	M	SD	NV	M	SD	NV
Symbol	22,10	16,55	0,104	16,25	12,04	0,045	14,89	20,32	0	19,78	25,60	0,001	18,22	19,29	0
Text	34,54	25,27	0,041	44,47	26,97	0,108	50,58	23,87	0,161	46,37	30,17	0,2	44,16	26,71	0,008
Skala	12,46	12,06	0,11	12,41	10,28	0,2	12,44	8,49	0,2				12,44	10,29	0

Anmerkung. Fixationszeiten auf die jeweiligen Gebiete verglichen unter den Gruppen farblich in aufsteigender Reihenfolge markiert: rot, orange, gelb, grün.

Tabelle 69 *Kruskal-Wallis-Test Vergleich der Fixationszeiten auf Symbol, Text und Skala zwischen den Gruppen*

Ränge			
Gebiet	Gruppe	H	Mittlerer Rang
Symbol	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	43,31
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	39,13
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	29,43
	D: Keine Datenschutzskala	18	35,22
	Gesamtsumme	72	
Text	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	27,58
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	36,25
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	43,53
	D: Keine Datenschutzskala	18	37,83
	Gesamtsumme	72	
Skala	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	43,72
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	45,25
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	46,85
	D: Keine Datenschutzskala	18	10,00
	Gesamtsumme	72	

Fortsetzung Tabelle 69

Teststatistiken[a,b]			
	Symbol	Text	Skala
Chi-Quadrat	4,508	5,596	39,415
df	3	3	3
Asymp. Sig.	,212	,133	,000

a. Kruskal-Wallis-Test

b. Gruppierungsvariable: Gruppe

Tabelle 70 *Mann-Whitney-U-Test Vergleich der Fixationszeiten zwischen Gruppe A und B*

Ränge

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Symbol	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,78	338,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	16,06	257,00
	Gesamtsumme	34		
Text	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	15,39	277,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	19,88	318,00
	Gesamtsumme	34		
Skala	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,06	307,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	18,00	288,00
	Gesamtsumme	34		

Fortsetzung Tabelle 70

Teststatistiken[a]			
	Symbol	Text	Skala
Mann-Whitney-U-Test	121,000	106,000	136,000
Wilcoxon-W	257,000	277,000	307,000
z	-,794	-1,311	-,276
Asymp. Sig. (2-seitig)	,427	,190	,783
Exakte Sig. [2*(1-seitige Sig.)]	,443[b]	,198[b]	,798[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 71 *Mann-Whitney-U-Test Vergleich der Fixationszeiten zwischen Gruppe A und C*

Ränge				
Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Symbol	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	23,17	417,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	16,20	324,00
	Gesamtsumme	38		
Text	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	14,86	267,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	23,68	473,50
	Gesamtsumme	38		
Skala	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,67	336,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,25	405,00
	Gesamtsumme	38		

Teststatistiken[a]			
	Symbol	Text	Skala
Mann-Whitney-U-Test	114,000	96,500	165,000
Wilcoxon-W	324,000	267,500	336,000
z	-1,930	-2,441	-,439
Asymp. Sig. (2-seitig)	,054	,015	,661
Exakte Sig. [2*(1-seitige Sig.)]	,055[b]	,013[b]	,675[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 72 *Mann-Whitney-U-Test Vergleich der Fixationszeiten zwischen Gruppe A und D*

Ränge

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Symbol	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	20,36	366,50
	D: Keine Datenschutzskala	18	16,64	299,50
	Gesamtsumme	36		
Text	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	16,33	294,00
	D: Keine Datenschutzskala	18	20,67	372,00
	Gesamtsumme	36		
Skala	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	27,00	486,00
	D: Keine Datenschutzskala	18	10,00	180,00
	Gesamtsumme	36		

Teststatistiken[a]

	Symbol	Text	Skala
Mann-Whitney-U-Test	128,500	123,000	9,000
Wilcoxon-W	299,500	294,000	180,000
z	-1,060	-1,234	-5,241
Asymp. Sig. (2-seitig)	,289	,217	,000
Exakte Sig. [2*(1-seitige Sig.)]	,293[b]	,226[b]	,000[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 73 *Mann-Whitney-U-Test Vergleich der Fixationszeiten zwischen Gruppe B und C*

Ränge

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Symbol	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	21,31	341,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	16,25	325,00
	Gesamtsumme	36		
Text	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	16,44	263,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,15	403,00
	Gesamtsumme	36		
Skala	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	17,75	284,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,10	382,00
	Gesamtsumme	36		

Teststatistiken[a]

	Symbol	Text	Skala
Mann-Whitney-U-Test	115,000	127,000	148,000
Wilcoxon-W	325,000	263,000	284,000
z	-1,433	-1,051	-,382
Asymp. Sig. (2-seitig)	,152	,293	,702
Exakte Sig. [2*(1-seitige Sig.)]	,158[b]	,305[b]	,718[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 74 *Mann-Whitney-U-Test Vergleich der Fixationszeiten zwischen Gruppe B und D*

Ränge

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Symbol	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	18,75	300,00
	D: Keine Datenschutzskala	18	16,39	295,00
	Gesamtsumme	34		
Text	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	16,94	271,00
	D: Keine Datenschutzskala	18	18,00	324,00
	Gesamtsumme	34		
Skala	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	26,50	424,00
	D: Keine Datenschutzskala	18	9,50	171,00
	Gesamtsumme	34		

Teststatistiken[a]

	Symbol	Text	Skala
Mann-Whitney-U-Test	124,000	135,000	,000
Wilcoxon-W	295,000	271,000	171,000
z	-,690	-,311	-5,383
Asymp. Sig. (2-seitig)	,490	,756	,000
Exakte Sig. [2*(1-seitige Sig.)]	,506[b]	,772[b]	,000[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 75 *Mann-Whitney-U-Test Vergleich der Fixationszeiten zwischen Gruppe C und D*

Ränge

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Symbol	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	17,98	359,50
	D: Keine Datenschutzskala	18	21,19	381,50
	Gesamtsumme	38		
Text	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,70	414,00
	D: Keine Datenschutzskala	18	18,17	327,00
	Gesamtsumme	38		
Skala	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	28,50	570,00
	D: Keine Datenschutzskala	18	9,50	171,00
	Gesamtsumme	38		

Teststatistiken[a]

	Symbol	Text	Skala
Mann-Whitney-U-Test	149,500	156,000	,000
Wilcoxon-W	359,500	327,000	171,000
z	-,892	-,702	-5,566
Asymp. Sig. (2-seitig)	,373	,483	,000
Exakte Sig. [2*(1-seitige Sig.)]	,377[b]	,496[b]	,000[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 76 *Fixationszeiten auf die jeweiligen Gebiete nach Gruppen*

Fixationszeiten auf die jeweiligen Gebiete nach Gruppen

Gebiet	Gruppe A			Gruppe B			Gruppe C			Gruppe D			Gesamt		
	M	SD	NV	M	SD	NV	M	SD	NV	M	SD	NV	M	SD	NV
Kein Signal	5,58	17,25	0	5,32	7,15	0	2,06	5,30	0	6,25	11,39	0	4,71	11,11	
Eingabe	35,08	12,69	0,20	52,36	49,55	0,00	44,98	19,78	0,20	55,83	27,96	0,20	46,86	30,03	0,2
Leerlauf	9,87	8,66	0,02	4,79	6,61	0	9,99	10,82	0	5,36	8,55	0,002	7,65	9,05	0
Suchzeile	5,51	5,64	0,018	6,38	4,72	0,2	6,48	14,31	0	7,41	9,29	0,004	6,45	9,40	0
Zurücktaste	0,24	0,45	0	0,37	0,81	0	1,34	3,70	0	0,00	0,01	0	0,51	2,04	0
Apptaste	0,20	0,76	0	0,15	0,28	0	0,48	1,45	0	0,01	0,03	0	0,22	0,87	0
Hometaste	0,50	1,71	0	0,14	0,36	0	0,60	1,37	0	0,01	0,05	0	0,32	1,14	0
Tastatur	1,16	3,58	0	1,86	3,65	0	0,26	0,69	0	2,41	5,94	0	1,38	3,89	0
Diagramm	13,08	38,47	0	5,13	8,36	0	0,51	2,26	0	0,00	0,00		4,55	19,97	0
Auswahl der App	44,22	23,33	0,007	53,67	53,60	0	52,35	58,87	0	57,44	31,56	0,01	51,88	43,89	0
Bilder	6,66	9,88	0	8,13	17,51	0	12,75	20,38	0,001	9,50	13,06	0,001	9,39	15,67	
Rezension/Bewertung	25,37	77,05	0	7,94	18,04	0	32,66	101,33	0	32,31	74,45	0	25,25	75,24	0
Rest	738,05	133,60	0,2	757,42	208,34	0,2	818,38	151,66	0,09	858,28	194,81	0,2	794,73	176,06	0,2

Anmerkung. Fixationszeiten auf die jeweiligen Gebiete verglichen unter den Gruppen farblich in aufsteigender Reihenfolge markiert: rot, orange, gelb, grün.

Tabelle 77 *Kruskal-Wallis-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen*

Ränge

Gebiet	Gruppe	H	Mittlerer Rang
Kein Signal	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	28,72
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	46,56
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	30,75
	D: Keine Datenschutzskala	18	41,72
	Gesamtsumme	72	

Fortsetzung Tabelle 77

Gebiet	Gruppe	H	Mittlerer Rang
Eingabe	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	29,22
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	38,94
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	36,35
	D: Keine Datenschutzskala	18	41,78
	Gesamtsumme	72	
Leerlauf	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	45,56
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	28,31
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	42,60
	D: Keine Datenschutzskala	18	27,94
	Gesamtsumme	72	
Suchzeile	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	36,67
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	44,94
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	29,05
	D: Keine Datenschutzskala	18	37,11
	Gesamtsumme	72	
Zurücktaste	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	41,89
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	34,34
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	41,05
	D: Keine Datenschutzskala	18	27,97
	Gesamtsumme	72	
Apptaste	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	34,25
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	39,78
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	41,58
	D: Keine Datenschutzskala	18	30,19
	Gesamtsumme	72	

Fortsetzung Tabelle 77

Gebiet	Gruppe	H	Mittlerer Rang
Hometaste	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	40,56
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	35,69
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	38,65
	D: Keine Datenschutzskala	18	30,78
	Gesamtsumme	72	
Tastatur	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	33,75
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	42,13
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	29,90
	D: Keine Datenschutzskala	18	41,58
	Gesamtsumme	72	
Diagramm	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	39,22
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	44,44
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	32,65
	D: Keine Datenschutzskala	18	31,00
	Gesamtsumme	72	
Auswahl der App	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	35,94
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	36,81
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	30,60
	D: Keine Datenschutzskala	18	43,33
	Gesamtsumme	72	
Bilder	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	36,17
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	34,26
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	40,38
	D: Keine Datenschutzskala	18	36,89
	Gesamtsumme	72	

Fortsetzung Tabelle 77

Gebiet	Gruppe	H	Mittlerer Rang
Rezension / Bewertung	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	40,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	28,13
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	40,65
	D: Keine Datenschutzskala	18	35,83
	Gesamtsumme	72	
Rest	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	35,33
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	32,63
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	38,25
	D: Keine Datenschutzskala	18	39,17
	Gesamtsumme	72	

Fortsetzung Tabelle 77

Teststatistiken[a,b]

	Kein Signal	Eingabe	Leerlauf	Suchzeile	Zurücktaste	Apptaste	Hometaste	Tastatur	Diagramm	Auswahl der App	Bilder	Rezension / Bewertung	Rest
Chi-Quadrat	9,112	3,540	10,530	5,248	8,498	6,442	4,479	6,111	11,548	3,525	1,583	4,001	1,037
df	3	3	3	3	3	3	3	3	3	3	3	3	3
Asymp. Sig.	,028	,316	,015	,155	,037	,092	,214	,106	,009	,318	,663	,261	,792

a. Kruskal-Wallis-Test

b. Gruppierungsvariable: Gruppe

Tabelle 78 *Anzahl der Fixationswechsel auf die jeweiligen Gebiete nach Gruppen*

Anzahl der Fixationswechsel auf die jeweiligen Gebiete nach Gruppen

Gebiet	Gruppe A			Gruppe B			Gruppe C			Gruppe D			Gesamt		
	M	SD	NV	M	SD	NV	M	SD	NV	M	SD	NV	M	SD	NV
Symbol	39,94	24,73	0,2	30,47	16,55	0,2	31,50	30,95	0,086	22,17	13,23	0,2	30,71	23,20	0,008
Text	54,56	35,27	0	61,24	38,05	0,057	60,70	31,75	0,003	31,06	11,34	0,2	50,56	30,41	0
Skala	24,78	20,13	0,2	27,71	20,64	0,069	26,80	17,54	0,098				19,54	20,00	0
Kein Signal	9, 28	23,34	0	9,35	7,66	0,2	5,4	7,86	0,003	7,67	8,37	0,009	7,88	13,40	0
Eingabe	7,83	0,71	0	7,82	0,73	0	8,15	0,75	,000	8,11	0,32	0	7,99	0,66	0
Leerlauf	23,89	28,74	0	14,24	16,10	0	23,35	22,50	0,012	8,61	10,15	0,031	17,92	21,36	0
Suchzeile	8,11	7,05	0,096	8,29	5,31	0,2	6,25	8,63	0,001	8,67	8,93	0,057	7,89	7,58	0
Zurücktaste	0,72	1,02	0	0,76	1,48	0	4,35	11,71	0	0,06	0,24	0	1,56	6,37	0
Apptaste	0,83	3,05	0	0,53	0,87	0	1,55	4,67	0	0,06	0,24	0	0,76	2,93	0
Hometaste	1,50	4,67	0	0,35	0,86	0	1,65	4,02	0	0,06	0,24	0	0,93	3,19	0
Tastatur	0,94	2,60	0	2,06	2,33	0,001	0,50	1,15	0	2,17	3,93	0	1,33	2,69	0
Diagramm	1,11	3,07	0	0,53	1,01	0	0,05	0,22	0				0,42	1,64	0
Appwahl	16,39	7,51	0,046	18,94	28,01	0	17,50	7,21	0,08	18,50	11,79	0,098	16,31	8,44	0
Bilder	7,61	6,39	0,06	7,29	19,67	0	8,80	7,94	0,005	6,61	6,45	0,006	6,57	6,59	0
Rezension	7,94	6,25	0,2	2,35	3,02	0,005	11,70	12,13	0,012	6,61	8,35	0,004	7,39	8,88	0
Rest	7,89	0,58	0	7,76	0,83	0	8,20	0,89	0	8,00	0,00	0	7,97	0,69	0

Anmerkung. Anzahl der Fixationswechsel auf die jeweiligen Gebiete verglichen unter den Gruppen farblich in absteigender Reihenfolge markiert: rot, orange, gelb, grün.

Tabelle 79 *Kruskal-Wallis-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen*

Ränge

Gebiet	Gruppe	H	Mittlerer Rang
Kein Signal	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	26,83
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	46,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	34,10
	D: Keine Datenschutzskala	18	41,89
	Gesamtsumme	73	

Fortsetzung Tabelle 79

Gebiet	Gruppe	H	Mittlerer Rang
Eingabe	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	33,75
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	33,53
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	39,28
	D: Keine Datenschutzskala	18	41,00
	Gesamtsumme	73	
Symbol	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	46,89
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	38,91
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	33,60
	D: Keine Datenschutzskala	18	29,08
	Gesamtsumme	73	
Text	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	40,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	42,85
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	43,50
	D: Keine Datenschutzskala	18	20,75
	Gesamtsumme	73	
Skala	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	43,92
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	46,59
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	46,93
	D: Keine Datenschutzskala	18	10,00
	Gesamtsumme	73	
Leerlauf	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	43,61
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	33,74
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	44,40
	D: Keine Datenschutzskala	18	25,25
	Gesamtsumme	73	

Fortsetzung Tabelle 79

Gebiet	Gruppe	H	Mittlerer Rang
Suchzeile	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	38,69
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	41,53
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	30,10
	D: Keine Datenschutzskala	18	38,69
	Gesamtsumme	73	
Zurücktaste	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	41,42
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	36,24
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	41,63
	D: Keine Datenschutzskala	18	28,17
	Gesamtsumme	73	
Apptaste	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	34,64
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	41,15
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	41,58
	D: Keine Datenschutzskala	18	30,36
	Gesamtsumme	73	
Hometaste	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	41,36
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	35,88
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	39,18
	D: Keine Datenschutzskala	18	31,28
	Gesamtsumme	73	
Tastatur	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	32,69
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	44,44
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	30,30
	D: Keine Datenschutzskala	18	41,72
	Gesamtsumme	73	

Fortsetzung Tabelle 79

Gebiet	Gruppe	H	Mittlerer Rang
Diagramm	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	39,94
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	44,12
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	33,25
	D: Keine Datenschutzskala	18	31,50
	Gesamtsumme	73	
Auswahl der App	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	38,61
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	28,15
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	41,65
	D: Keine Datenschutzskala	18	38,58
	Gesamtsumme	73	
Bilder	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	41,44
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	25,82
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	42,03
	D: Keine Datenschutzskala	18	37,53
	Gesamtsumme	73	
Rezension/Bewertung	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	42,67
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	24,79
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	44,55
	D: Keine Datenschutzskala	18	34,47
	Gesamtsumme	73	
Rest	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	35,97
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	33,79
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	39,75
	D: Keine Datenschutzskala	18	38,00
	Gesamtsumme	73	

Fortsetzung Tabelle 79

Teststatistiken[a,b]

Gebiet	Chi-Quadrat	df	Asymp. Sig.
Kein Signal	8,850	3	,031
Eingabe	3,194	3	,363
Symbol	7,073	3	,070
Text	14,229	3	,003
Skala	39,643	3	,000
Leerlauf	10,124	3	,018
Suchzeile	3,189	3	,363
Zurücktaste	7,651	3	,054
Apptaste	6,539	3	,088
Hometaste	4,675	3	,197
Tastatur	7,644	3	,054
Diagramm	10,604	3	,014
Appauswahl	4,147	3	,246
Bilder	6,696	3	,082
Berwertung	10,027	3	,018
Rest	2,743	3	,433

a. Kruskal-Wallis-Test

b. Gruppierungsvariable: Gruppe

Tabelle 80 *Mann-Whitney-U-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen A und B*

Ränge				
Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Kein Signal	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	13,67	246,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	21,81	349,00
	Gesamtsumme	34		
Eingabe	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,61	317,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	17,38	278,00
	Gesamtsumme	34		
Symbol	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	20,00	360,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	14,69	235,00
	Gesamtsumme	34		
Text	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,11	308,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	17,94	287,00
	Gesamtsumme	34		
Skala	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,08	307,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	17,97	287,50
	Gesamtsumme	34		
Leerlauf	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	19,56	352,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	15,19	243,00
	Gesamtsumme	34		

Fortsetzung Tabelle 80

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Suchzeile	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	16,89	304,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	18,19	291,00
	Gesamtsumme	34		
Zurücktaste	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,94	341,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	15,88	254,00
	Gesamtsumme	34		
Apptaste	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	16,36	294,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	18,78	300,50
	Gesamtsumme	34		
Hometaste	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,58	334,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	16,28	260,50
	Gesamtsumme	34		
Tastatur	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	15,22	274,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	20,06	321,00
	Gesamtsumme	34		
Diagramm	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	16,56	298,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	18,56	297,00
	Gesamtsumme	34		
Auswah der lApp	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	20,53	369,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	14,09	225,50
	Gesamtsumme	34		

Fortsetzung Tabelle 80

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Bilder	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	21,89	394,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	12,56	201,00
	Gesamtsumme	34		
Rezension/Berwertung	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	21,97	395,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	12,47	199,50
	Gesamtsumme	34		
Rest	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,03	324,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	16,91	270,50
	Gesamtsumme	34		

Fortsetzung Tabelle 80

Teststatistiken[a]

Gebiet	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)	Exakte Sig. [2*(1-seitige Sig.)]
Kein Signal	75,000	246,000	-2,469	,014	,017[b]
Eingabe	142,000	278,000	-,081	,935	,959[b]
Symbol	99,000	235,000	-1,553	,120	,126[b]
Text	137,000	308,000	-,242	,809	,825[b]
Skala	136,500	307,500	-,259	,796	,798[b]
Leerlauf	107,000	243,000	-1,279	,201	,211[b]
Suchzeile	133,000	304,000	-,381	,703	,721[b]
Zurücktaste	118,000	254,000	-1,082	,279	,384[b]
Apptaste	123,500	294,500	-,954	,340	,484[b]
Hometaste	124,500	260,500	-,868	,385	,506[b]
Tastatur	103,000	274,000	-1,621	,105	,164[b]
Diagramm	127,000	298,000	-,733	,463	,574[b]
Appauswahl	89,500	225,500	-1,886	,059	,059[b]
Bilder	65,000	201,000	-2,744	,006	,006[b]
Berwertung	63,500	199,500	-2,843	,004	,004[b]
Rest	134,500	270,500	-,464	,643	,746[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert

Tabelle 81 *Mann-Whitney-U-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen A und C*

Ränge

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Kein Signal	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,25	310,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	21,53	430,50
	Gesamtsumme	38		
Eingabe	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,97	323,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,88	417,50
	Gesamtsumme	38		
Symbol	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	22,61	407,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	16,70	334,00
	Gesamtsumme	38		
Text	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,67	336,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,25	405,00
	Gesamtsumme	38		
Skala	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,69	336,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,23	404,50
	Gesamtsumme	38		
Leerlauf	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	19,11	344,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,85	397,00
	Gesamtsumme	38		
Suchzeile	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	21,86	393,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	17,38	347,50
	Gesamtsumme	38		
Zurücktaste	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	19,25	346,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,73	394,50
	Gesamtsumme	38		
Apptaste	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	17,64	317,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	21,18	423,50
	Gesamtsumme	38		

Fortsetzung Tabelle 81

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Hometaste	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	20,03	360,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,03	380,50
	Gesamtsumme	38		
Tastatur	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	20,17	363,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	18,90	378,00
	Gesamtsumme	38		
Diagramm	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	21,28	383,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	17,90	358,00
	Gesamtsumme	38		
Auswahl der App	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,64	335,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,28	405,50
	Gesamtsumme	38		
Bilder	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	19,19	345,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,78	395,50
	Gesamtsumme	38		
Rezension/ Bewertung	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,86	339,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,08	401,50
	Gesamtsumme	38		
Rest	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,47	332,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,43	408,50
	Gesamtsumme	38		

Fortsetzung Tabelle 81

Teststatistiken[a]					
Gebiet	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)	Exakte Sig. [2*(1-seitige Sig.)]
Kein Signal	139,500	310,500	-1,253	,210	,239[b]
Eingabe	152,500	323,500	-1,080	,280	,426[b]
Symbol	124,000	334,000	-1,638	,101	,105[b]
Text	165,000	336,000	-,439	,661	,675[b]
Skala	165,500	336,500	-,424	,671	,675[b]
Leerlauf	173,000	344,000	-,205	,838	,851[b]
Suchzeile	137,500	347,500	-1,283	,199	,217[b]
Zurücktaste	175,500	346,500	-,147	,883	,897[b]
Apptaste	146,500	317,500	-1,268	,205	,331[b]
Hometaste	170,500	380,500	-,347	,728	,784[b]
Tastatur	168,000	378,000	-,471	,638	,740[b]
Diagramm	148,000	358,000	-1,593	,111	,361[b]
Appauswahl	164,500	335,500	-,454	,650	,654[b]
Bilder	174,500	345,500	-,161	,872	,874[b]
Berwertung	168,500	339,500	-,338	,735	,740[b]
Rest	161,500	332,500	-1,015	,310	,593[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert

Tabelle 82 *Mann-Whitney-U-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen A und D*

Ränge

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Kein Signal	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	14,69	264,50
	D: Keine Datenschutzskala	18	22,31	401,50
	Gesamtsumme	36		
Eingabe	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	16,72	301,00
	D: Keine Datenschutzskala	18	20,28	365,00
	Gesamtsumme	36		
Symbol	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	22,94	413,00
	D: Keine Datenschutzskala	18	14,06	253,00
	Gesamtsumme	36		
Text	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	23,67	426,00
	D: Keine Datenschutzskala	18	13,33	240,00
	Gesamtsumme	36		
Skala	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	27,00	486,00
	D: Keine Datenschutzskala	18	10,00	180,00
	Gesamtsumme	36		
Leerlauf	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	23,00	414,00
	D: Keine Datenschutzskala	18	14,00	252,00
	Gesamtsumme	36		
Suchzeile	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,08	325,50
	D: Keine Datenschutzskala	18	18,92	340,50
	Gesamtsumme	36		
Zurücktaste	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	22,08	397,50
	D: Keine Datenschutzskala	18	14,92	268,50
	Gesamtsumme	36		
Apptaste	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	19,53	351,50
	D: Keine Datenschutzskala	18	17,47	314,50
	Gesamtsumme	36		

Fortsetzung Tabelle 82

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Hometaste	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	21,08	379,50
	D: Keine Datenschutzskala	18	15,92	286,50
	Gesamtsumme	36		
Tastatur	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	16,25	292,50
	D: Keine Datenschutzskala	18	20,75	373,50
	Gesamtsumme	36		
Diagramm	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	20,50	369,00
	D: Keine Datenschutzskala	18	16,50	297,00
	Gesamtsumme	36		
AuswahlApp	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,44	332,00
	D: Keine Datenschutzskala	18	18,56	334,00
	Gesamtsumme	36		
Bilder	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	19,36	348,50
	D: Keine Datenschutzskala	18	17,64	317,50
	Gesamtsumme	36		
Rezension/Bewertung	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	20,11	362,00
	D: Keine Datenschutzskala	18	16,89	304,00
	Gesamtsumme	36		
Rest	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	18,00	324,00
	D: Keine Datenschutzskala	18	19,00	342,00
	Gesamtsumme	36		

Fortsetzung Tabelle 82

Teststatistiken[a]

Gebiet	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)	Exakte Sig. [2*(1-seitige Sig.)]
Kein Signal	93,500	264,500	-2,235	,025	,029[b]
Eingabe	130,000	301,000	-1,393	,163	,323[b]
Symbol	82,000	253,000	-2,533	,011	,011[b]
Text	69,000	240,000	-2,944	,003	,003[b]
Skala	9,000	180,000	-5,243	,000	,000[b]
Leerlauf	81,000	252,000	-2,568	,010	,010[b]
Suchzeile	154,500	325,500	-,239	,811	,815[b]
Zurücktaste	97,500	268,500	-2,694	,007	,040[b]
Apptaste	143,500	314,500	-1,073	,283	,563[b]
Hometaste	115,500	286,500	-2,132	,033	,143[b]
Tastatur	121,500	292,500	-1,462	,144	,203[b]
Diagramm	126,000	297,000	-2,088	,037	,265[b]
Appauswahl	161,000	332,000	-,032	,975	,988[b]
Bilder	146,500	317,500	-,493	,622	,628[b]
Bewertung	133,000	304,000	-,932	,351	,372[b]
Rest	153,000	324,000	-,594	,553	,791[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert

Tabelle 83 *Mann-Whitney-U-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen B und C*

Ränge

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Kein Signal	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	22,35	380,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	16,15	323,00
	Gesamtsumme	37		
Eingabe	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	17,41	296,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,35	407,00
	Gesamtsumme	37		
Symbol	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	20,56	349,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	17,68	353,50
	Gesamtsumme	37		
Text	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	18,82	320,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,15	383,00
	Gesamtsumme	37		
Skala	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	18,76	319,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,20	384,00
	Gesamtsumme	37		
Leerlauf	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	15,97	271,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	21,58	431,50
	Gesamtsumme	37		
Suchzeile	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	22,38	380,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	16,13	322,50
	Gesamtsumme	37		

Fortsetzung Tabelle 83

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Zurücktaste	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	17,65	300,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,15	403,00
	Gesamtsumme	37		
Apptaste	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	18,79	319,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,18	383,50
	Gesamtsumme	37		
Hometaste	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	18,06	307,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,80	396,00
	Gesamtsumme	37		
Tastatur	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	22,79	387,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	15,78	315,50
	Gesamtsumme	37		
Diagramm	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	22,06	375,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	16,40	328,00
	Gesamtsumme	37		
AuswahlApp	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	15,09	256,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	22,33	446,50
	Gesamtsumme	37		
Bilder	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	14,79	251,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	22,58	451,50
	Gesamtsumme	37		

Fortsetzung Tabelle 83

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Rezension/Bewertung	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	13,68	232,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	23,53	470,50
	Gesamtsumme	37		
Rest	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	17,38	295,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,38	407,50
	Gesamtsumme	37		

Teststatistiken[a]

Gebiet	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)	Exakte Sig. [2*(1-seitige Sig.)]
Kein Signal	113,000	323,000	-1,757	,079	,085[b]
Eingabe	143,000	296,000	-1,095	,274	,424[b]
Symbol	143,500	353,500	-,808	,419	,424[b]
Text	167,000	320,000	-,091	,927	,940[b]
Skala	166,000	319,000	-,122	,903	,916[b]
Leerlauf	118,500	271,500	-1,572	,116	,117[b]
Suchzeile	112,500	322,500	-1,778	,075	,080[b]
Zurücktaste	147,000	300,000	-,844	,399	,497[b]
Apptaste	166,500	319,500	-,126	,900	,916[b]
Hometaste	154,000	307,000	-,677	,498	,641[b]
Tastatur	105,500	315,500	-2,307	,021	,048[b]
Diagramm	118,000	328,000	-2,329	,020	,117[b]
Appauswahl	103,500	256,500	-2,033	,042	,042[b]
Bilder	98,500	251,500	-2,193	,028	,028[b]
Bewertung	79,500	232,500	-2,809	,005	,005[b]
Rest	142,500	295,500	-1,410	,158	,407[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert

Tabelle 84 *Mann-Whitney-U-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen B und D*

Ränge

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Kein Signal	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	19,29	328,00
	D: Keine Datenschutzskala	18	16,78	302,00
	Gesamtsumme	35		
Eingabe	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	16,18	275,00
	D: Keine Datenschutzskala	18	19,72	355,00
	Gesamtsumme	35		
Symbol	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	20,82	354,00
	D: Keine Datenschutzskala	18	15,33	276,00
	Gesamtsumme	35		
Text	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	23,15	393,50
	D: Keine Datenschutzskala	18	13,14	236,50
	Gesamtsumme	35		
Skala	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	27,00	459,00
	D: Keine Datenschutzskala	18	9,50	171,00
	Gesamtsumme	35		
Leerlauf	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	20,41	347,00
	D: Keine Datenschutzskala	18	15,72	283,00
	Gesamtsumme	35		
Suchzeile	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	18,88	321,00
	D: Keine Datenschutzskala	18	17,17	309,00
	Gesamtsumme	35		

Fortsetzung Tabelle 84

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Zurücktaste	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	19,74	335,50
	D: Keine Datenschutzskala	18	16,36	294,50
	Gesamtsumme	35		
Apptaste	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	20,74	352,50
	D: Keine Datenschutzskala	18	15,42	277,50
	Gesamtsumme	35		
Hometaste	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	19,15	325,50
	D: Keine Datenschutzskala	18	16,92	304,50
	Gesamtsumme	35		
Tastatur	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	18,76	319,00
	D: Keine Datenschutzskala	18	17,28	311,00
	Gesamtsumme	35		
Diagramm	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	21,18	360,00
	D: Keine Datenschutzskala	18	15,00	270,00
	Gesamtsumme	35		
Auswahl App	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	15,74	267,50
	D: Keine Datenschutzskala	18	20,14	362,50
	Gesamtsumme	35		
Bilder	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	15,15	257,50
	D: Keine Datenschutzskala	18	20,69	372,50
	Gesamtsumme	35		

Fortsetzung Tabelle 84

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Rezension/ Bewertung	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	16,09	273,50
	D: Keine Datenschutzskala	18	19,81	356,50
	Gesamtsumme	35		
Rest	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	16,94	288,00
	D: Keine Datenschutzskala	18	19,00	342,00
	Gesamtsumme	35		

Teststatistiken[a]

Gebiet	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)	Exakte Sig. [2*(1-seitige Sig.)]
Kein Signal	131	302	-0,729	0,466	,483b
Eingabe	122	275	-1,393	0,164	,318b
Symbol	105	276	-1,585	0,113	,118b
Text	65,5	236,5	-2,891	0,004	,003b
Skala	0	171	-5,432	0	,000b
Leerlauf	112	283	-1,358	0,174	,184b
Suchzeile	138	309	-0,497	0,619	,636b
Zurücktaste	123,5	294,5	-1,6	0,11	,335b
Apptaste	106,5	277,5	-2,203	0,028	,126b
Hometaste	133,5	304,5	-1,165	0,244	,525b
Tastatur	140	311	-0,457	0,648	,684b
Diagramm	99	270	-2,722	0,006	,077b
Appauswahl	114,5	267,5	-1,277	0,201	,207b
Bilder	104,5	257,5	-1,618	0,106	,110b
Berwertung	120,5	273,5	-1,118	0,264	,287b
Rest	135	288	-1,075	0,282	,568b

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert

Tabelle 85 *Mann-Whitney-U-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen C und D*

Ränge

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Kein Signal	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	17,43	348,50
	D: Keine Datenschutzskala	18	21,81	392,50
	Gesamtsumme	38		
Eingabe	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,05	381,00
	D: Keine Datenschutzskala	18	20,00	360,00
	Gesamtsumme	38		
Symbol	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,23	404,50
	D: Keine Datenschutzskala	18	18,69	336,50
	Gesamtsumme	38		
Text	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	25,10	502,00
	D: Keine Datenschutzskala	18	13,28	239,00
	Gesamtsumme	38		
Skala	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	28,50	570,00
	D: Keine Datenschutzskala	18	9,50	171,00
	Gesamtsumme	38		
Leerlauf	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	23,98	479,50
	D: Keine Datenschutzskala	18	14,53	261,50
	Gesamtsumme	38		
Suchzeile	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	17,60	352,00
	D: Keine Datenschutzskala	18	21,61	389,00
	Gesamtsumme	38		
Zurücktaste	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	22,75	455,00
	D: Keine Datenschutzskala	18	15,89	286,00
	Gesamtsumme	38		
Apptaste	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	22,23	444,50
	D: Keine Datenschutzskala	18	16,47	296,50
	Gesamtsumme	38		
Hometaste	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	21,35	427,00
	D: Keine Datenschutzskala	18	17,44	314,00
	Gesamtsumme	38		

Fortsetzung Tabelle 85

Gebiet	Gruppe	H	Mittlerer Rang	Summe der Ränge
Tastatur	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	16,63	332,50
	D: Keine Datenschutzskala	18	22,69	408,50
	Gesamtsumme	38		
Diagramm	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,95	399,00
	D: Keine Datenschutzskala	18	19,00	342,00
	Gesamtsumme	38		
Auswahl der App	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,05	401,00
	D: Keine Datenschutzskala	18	18,89	340,00
	Gesamtsumme	38		
Bilder	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	20,68	413,50
	D: Keine Datenschutzskala	18	18,19	327,50
	Gesamtsumme	38		
Rezension/Bewertung	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	21,95	439,00
	D: Keine Datenschutzskala	18	16,78	302,00
	Gesamtsumme	38		
Rest	C: Datenschutzskala ohne eine detaillierte Beschreibung	20	19,95	399,00
	D: Keine Datenschutzskala	18	19,00	342,00
	Gesamtsumme	38		

Fortsetzung Tabelle 85

Teststatistiken[a]

Gebiet	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)	Exakte Sig. [2*(1-seitige Sig.)]
Kein Signal	138,500	348,500	-1,227	0,22	,228b
Eingabe	171,000	381,000	-,448	0,654	,806b
Symbol	165,500	336,500	-0,424	0,672	,675b
Text	68,000	239,000	-3,277	0,001	,001b
Skala	,000	171,000	-5,567	0	,000b
Leerlauf	90,500	261,500	-2,62	0,009	,008b
Suchzeile	142,000	352,000	-1,141	0,254	,276b
Zurücktaste	115,000	286,000	-2,551	0,011	,059b
Apptaste	125,500	296,500	-2,24	0,025	,112b
Hometaste	143,000	314,000	-1,704	0,088	,290b
Tastatur	122,500	332,500	-1,99	0,047	,093b
Diagramm	171,000	342,000	-0,949	0,343	,806b
Appauswahl	169,000	340,000	-0,323	0,747	,762b
Bilder	156,500	327,500	-0,689	0,491	,496b
Bewertung	131,000	302,000	-1,452	0,147	,158b
Rest	171,000	342,000	-0,949	0,343	, 806b

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert

Tabelle 86 *T-Test Vergleich der Fixationszeiten auf verschiedene Gebiete zwischen den Gruppen*

Test bei unabhängigen Stichproben

Anzahl an Wechsel Gruppe A und B		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Symbol	Varianzgleichheit angenommen	1,278	,266	1,324	33	,195	9,47386	7,15766	-5,08851	24,03622
	Varianzgleichheit nicht angenommen			1,339	29,819	,191	9,47386	7,07776	-4,98453	23,93224
Suchzeit	Varianzgleichheit angenommen	4,655	,038	-,086	33	,932	-,18301	2,12050	-4,49719	4,13118
	Varianzgleichheit nicht angenommen			-,087	31,485	,931	-,18301	2,10333	-4,47011	4,10409

Fortsetzung Tabelle 86

Test bei unabhängigen Stichproben										
Anzahl an Wechsel Gruppe A und C		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Symbol	Varianzgleichheit angenommen	,457	,503	,922	36	,363	8,44444	9,15739	-10,12761	27,01650
	Varianzgleichheit nicht angenommen			,933	35,534	,357	8,44444	9,04880	-9,91574	26,80463
Skala	Varianzgleichheit angenommen	,245	,624	-,331	36	,743	-2,02222	6,11002	-14,41393	10,36948
	Varianzgleichheit nicht angenommen			-,329	33,973	,745	-2,02222	6,15551	-14,53209	10,48764

Fortsetzung Tabelle 86

Test bei unabhängigen Stichproben

Anzahl an Wechsel Gruppe B und C		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Symbol	Varianzgleichheit angenommen	2,800	,103	-,123	35	,903	-1,02941	8,37955	-18,04079	15,98197
	Varianzgleichheit nicht angenommen			-,129	29,913	,898	-1,02941	8,00053	-17,37068	15,31186
Skala	Varianzgleichheit angenommen	,471	,497	,144	35	,886	,90588	6,27319	-11,82936	13,64113
	Varianzgleichheit nicht angenommen			,142	31,634	,888	,90588	6,35819	-12,05120	13,86297

Fortsetzung Tabelle 86

Test bei unabhängigen Stichproben										
Anzahl an Wechsel Gruppe A und D		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Symbol	Varianzgleichheit angenommen	3,434	,073	2,689	34	,011	17,77778	6,61091	4,34280	31,21275
	Varianzgleichheit nicht angenommen			2,689	25,990	,012	17,77778	6,61091	4,18861	31,36695
Suchzeile	Varianzgleichheit angenommen	,841	,366	-,207	34	,837	-,55556	2,68242	-6,00688	4,89577
	Varianzgleichheit nicht angenommen			-,207	32,267	,837	-,55556	2,68242	-6,01768	4,90657

Fortsetzung Tabelle 86

Anzahl an Wechsel Gruppe C und D		Test bei unabhängigen Stichproben								
		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Auswahl der App	Varianzgleichheit angenommen	2,172	,149	-,319	36	,751	-1,00000	3,13386	-7,35576	5,35576
	Varianzgleichheit nicht angenommen			-,311	27,570	,758	-1,00000	3,21216	-7,58443	5,58443

Fortsetzung Tabelle 86

Test bei unabhängigen Stichproben

Anzahl an Wechsel Gruppe B und D		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Symbol	Varianzgleichheit angenommen	,938	,340	1,644	33	,110	8,30392	5,04962	-1,96961	18,57746
	Varianzgleichheit nicht angenommen			1,634	30,635	,113	8,30392	5,08249	-2,06690	18,67474
Text	Varianzgleichheit angenommen	10,313	,003	3,220	33	,003	30,17974	9,37321	11,10981	49,24967
	Varianzgleichheit nicht angenommen			3,141	18,675	,005	30,17974	9,60718	10,04796	50,31152
Suchzeile	Varianzgleichheit angenommen	5,990	,020	-,149	33	,883	-,37255	2,50299	-5,46492	4,71982
	Varianzgleichheit nicht angenommen			-,151	27,954	,881	-,37255	2,46808	-5,42855	4,68345

Tabelle 87 *Auflistung der ausgewählten Applikationen mit den entsprechenden Häufigkeiten*

Szenario	App	Anzahl	Prozent	Gesamtsumme	
				Anzahl	Prozent
Messenger	BiP Messenger	5	6,1	82	100
	Hangouts	0	0		
	Facebook Messenger	9	11		
	Kik	1	1,2		
	Threema	2	2,4		
	Signal	3	3,7		
	Wire	0	0		
	WhatsApp	52	63,4		
	Telegram	7	8,5		
	Line	0	0		
	Forbis Messenger	3	3,7		
Videokonferenz	Skype	59	72	82	100
	Imo	1	1,2		
	TrueConf	2	2,4		
	Viber	14	17,1		
	JusTalk	1	1,2		
	ZOOM	0	0		
	Glide	0	0		
	Tango	0	0		
	Google Duo	0	0		
	VideoCall Free	0	0		
	Facebook Messenger	2	2,4		
	Kik	1	1,2		
	Hangouts	2	2,4		
Wetter	Yr	1	1,2	82	100
	Weatherzone	2	2,4		
	Wetter.de	18	22		
	Wetter.com	21	25,6		
	Wetter-Online	22	26,8		
	Morecast (UBIMET)	16	19,5		
	Yahoo Wetter	0	0		
	AccuWeather	0	0		
	Bayer Agrar Wetter	2	2,4		
	Weather Live	0	0		
	Windy.com	0	0		

Fortsetzung Tabelle 87

Szenario	App	Anzahl	Prozent	Gesamtsumme Anzahl	Gesamtsumme Prozent
E-Mail	Outlook	40	48,8	82	100
	Blue Mail	4	4,9		
	Spark	9	11		
	E-Mail für Outlook und andere	3	3,7		
	myMail	0	0		
	Nine	1	1,2		
	Open Mail	18	22		
	MailDroid	0	0		
	K-9 Mail	4	4,9		
	E-Mail-Mailchecker	3	3,7		
Music	Spotify	61	74,4	82	100
	Free Music	0	0		
	Deezer	1	1,2		
	Google Play	0	0		
	Gratis Musik/ Free Musik (Notenschlüssel Bild)*	1	1,2		
	Soundcloud	18	22		
	Freie Musik MH Musik	1	1,2		
	SongFlip	0	0		
	Audiomack	0	0		
	Musikspieler	0	0		
Fitness	Schrittzähler- Gratis Pedometer & Kalorienzähler*	32	39	81	98,8
	Wandern Schrittzähler Diät	2	2,4		
	Google Fit	6	7,3		
	Strava Training	4	4,9		
	Sportractive workout	7	8,5		
	Pacer Health Schrittzähler & Abnehm-trainer	2	2,4		
	Laufen zur Gewichtsabnahme	1	1,2		
	Fitbit	25	30,5		
	Endomondo	2	2,4		

Fortsetzung Tabelle 86

Szenario	App	Anzahl	Prozent	Gesamtsumme	
				Anzahl	Prozent
Spiele	Sudoku classic (Quarzo Apps)	21	25,6	82	100
	Sudoku 2 (Magma Mobile)	1	1,2		
	Sudoku (Volcano Entertainment)	2	2,4		
	Sudoku Free (Titan Inc Geduldsspiele)	3	3,7		
	Sudoku (Card Games)*	38	46,3		
	Sudoku Master (Dat Viet Entertainment)	6	7,3		
	Sudoku (Timeglass Works)	1	1,2		
	Sudoku puzzle	0	0		
	Material Sudoku (OkayCode)	1	1,2		
	Sudoku kostenlos deutsch (Marco Meyer)	9	11		
Nachrichten	Microsoft News	6	7,3	82	100
	BBC News	8	9,8		
	CNN Braking News	6	7,3		
	News Suite	0	0		
	Zeit	51	62,2		
	SQUID	0	0		
	FlipBoard	1	1,2		
	Euronews	6	7,3		
	RT News	4	4,9		
	Google News	0	0		

Tabelle 88 *Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Gruppen*

Gruppe		Score							
		Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
A	M	3,10	4,24	4,00	4,10	4,05	4,71	4,38	4,86
	SD	0,94	0,54	1,00	0,94	0,22	0,64	1,07	0,65
	NV (p)	0	0	0,008	0,001	0	0	0	0
	N	21	21	21	21	21	21	21	21
B	M	3,00	3,79	3,58	3,32	4,58	4,83	4,47	4,58
	SD	1,05	0,79	1,02	1,34	0,51	0,71	1,07	1,07
	NV (p)	0	0	0,072	0,003	0	0	0	0
	N	19	19	19	19	19	18	19	19
C	M	2,61	4,04	3,39	3,43	4,00	4,30	4,35	3,96
	SD	1,08	0,93	1,27	1,31	0,90	1,18	1,11	1,52
	NV (p)	0	0	0,093	0,001	0	0	0	0
	N	23	23	23	23	23	23	23	23
D	M	2,95	3,95	2,63	3,00	3,89	3,21	3,05	3,00
	SD	0,71	0,62	0,96	0,67	0,74	1,58	1,03	1,49
	NV (p)	0	0	0,017	0	0	0,006	0	0,001
	N	19	19	19	19	19	19	19	19

Anmerkung. Bekanntheit der ausgewählten Applikation verglichen unter den Gruppen: niedrigster Mittelwert (rot) und höchster Mittelwert (grün).

Tabelle 89 *Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala*

Datenschutzskala		Score							
		Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Ja (Gruppe A – C)	N	62,000	62,000	62,000	62,000	62,000	61,000	62,000	62,000
	M	3,629	2,887	4,081	3,661	4,194	4,590	4,452	4,435
	SD	1,244	1,042	0,685	1,130	0,674	0,920	0,986	1,210
	NV (p)	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Nein (Gruppe D)	N	20,000	20,000	20,000	20,000	20,000	20,000	20,000	20,000
	M	3,000	2,950	3,800	2,650	3,900	3,300	2,950	3,100
	SD	0,649	0,686	0,894	0,933	0,718	1,593	1,099	1,518
	NV (p)	0	0	0,025	0	0	0,001	0	0,001

Anmerkung. Angemessenheit der ausgewählten Applikation verglichen zwischen den Gruppen, denen eine Datenschutzskala präsentiert wurde und der Gruppe, die keine Datenschutzskala vorgefunden hat: niedrigster Mittelwert (rot) und höchster Mittelwert (grün).

Tabelle 90 *Kruskal-Wallis-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen*

(Zeile 53-60)

Ränge

Score	Gruppe	H	Mittlerer Rang
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	45,83
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	42,29
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	34,67
	D: Keine Datenschutzskala	19	44,18
	Gesamtsumme	82	
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	47,07
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	34,71
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	44,57
	D: Keine Datenschutzskala	19	38,42
	Gesamtsumme	82	
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	53,12
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	44,45
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	41,11
	D: Keine Datenschutzskala	19	26,18
	Gesamtsumme	82	
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	53,90
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	39,26
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	41,22
	D: Keine Datenschutzskala	19	30,37
	Gesamtsumme	82	
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	35,88
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	56,87
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	39,83
	D: Keine Datenschutzskala	19	34,37
	Gesamtsumme	82	

Fortsetzung Tabelle 90

Score	Gruppe	H	Mittlerer Rang
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	46,57
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	50,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	41,09
	D: Keine Datenschutzskala	19	25,74
	Gesamtsumme	81	
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	46,74
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	48,97
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	46,59
	D: Keine Datenschutzskala	19	22,08
	Gesamtsumme	82	
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	52,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	47,95
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	39,48
	D: Keine Datenschutzskala	19	25,89
	Gesamtsumme	82	

Teststatistiken[a,b]

	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Chi-Quadrat	4,013	5,459	13,952	11,871	18,862	18,649	20,925	20,926
df	3	3	3	3	3	3	3	3
Asymp. Sig.	,260	,141	,003	,008	,000	,000	,000	,000

a. Kruskal-Wallis-Test

b. Gruppierungsvariable: Gruppe

Tabelle 91 *Mann-Whitney-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen A, B, C (mit Datenschutzskala) und D (ohne Datenschutzskala)*

Ränge				
Score	Datenschutzskala	H	Mittlerer Rang	Summe der Ränge
Messenger	Ja	62	40,60	2517,00
	Nein	20	44,30	886,00
	Gesamtsumme	82		
Videokonferenz	Ja	62	43,09	2671,50
	Nein	20	36,58	731,50
	Gesamtsumme	82		
Wetter	Ja	62	46,35	2873,50
	Nein	20	26,48	529,50
	Gesamtsumme	82		
E-Mail	Ja	62	45,10	2796,50
	Nein	20	30,33	606,50
	Gesamtsumme	82		
Musik	Ja	62	43,81	2716,00
	Nein	20	34,35	687,00
	Gesamtsumme	82		
Fitness	Ja	61	45,56	2779,00
	Nein	20	27,10	542,00
	Gesamtsumme	81		
Spiele	Ja	62	48,08	2981,00
	Nein	20	21,10	422,00
	Gesamtsumme	82		
Nachrichten	Ja	62	46,08	2857,00
	Nein	20	27,30	546,00
	Gesamtsumme	82		

Fortsetzung Tabelle 91

Teststatistiken[a]

	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	564,000	521,500	319,500	396,500	477,000	332,000	212,000	336,000
Wilcoxon-W	2517,000	731,500	529,500	606,500	687,000	542,000	422,000	546,000
z	-,718	-1,349	-3,342	-2,627	-2,031	-3,778	-4,951	-3,776
Asymp. Sig. (2-seitig)	,473	,177	,001	,009	,042	,000	,000	,000

a. Gruppierungsvariable: Datenschutzskala

Tabelle 92 Mann-Whitney-U-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen A und B

Ränge

Score	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	21,31	447,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	19,61	372,50
	Gesamtsumme	40		
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	23,38	491,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	17,32	329,00
	Gesamtsumme	40		
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	22,76	478,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	18,00	342,00
	Gesamtsumme	40		
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	23,71	498,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	16,95	322,00
	Gesamtsumme	40		

Fortsetzung Tabelle 92

Score	Gruppe	H	Mittlerer Rang	Summe der Ränge
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	15,45	324,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	26,08	495,50
	Gesamtsumme	40		
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	18,88	396,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	21,31	383,50
	Gesamtsumme	39		
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,88	417,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	21,18	402,50
	Gesamtsumme	40		
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	21,52	452,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	19,37	368,00
	Gesamtsumme	40		

Teststatistiken[ab]

	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	182,500	139,000	152,000	132,000	93,500	165,500	186,500	178,000
Wilcoxon-W	372,500	329,000	342,000	322,000	324,500	396,500	417,500	368,000
z	-,543	-2,092	-1,340	-1,920	-3,616	-1,140	-,436	-1,119
Asymp. Sig. (2-seitig)	,587	,036	,180	,055	,000	,254	,663	,263
Exakte Sig. [2*(1-seitige Sig.)]	,649[b]	,105[b]	,205[b]	,069[b]	,003[b]	,512[b]	,728[b]	,573[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 93 *Mann-Whitney-U-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen A und C*

Ränge

Score	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	25,57	537,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,70	453,00
	Gesamtsumme	44		
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	23,14	486,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,91	504,00
	Gesamtsumme	44		
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	25,64	538,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,63	451,50
	Gesamtsumme	44		
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	25,81	542,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,48	448,00
	Gesamtsumme	44		
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	21,50	451,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	23,41	538,50
	Gesamtsumme	44		
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	24,14	507,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,00	483,00
	Gesamtsumme	44		
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	22,45	471,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,54	518,50
	Gesamtsumme	44		

Fortsetzung Tabelle 93

Score	Gruppe	H	Mittlerer Rang	Summe der Ränge
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	25,95	545,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,35	445,00
	Gesamtsumme	44		

Teststatistiken[a]

	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	177,000	228,000	175,500	172,000	220,500	207,000	240,500	169,000
Wilcoxon-W	453,000	504,000	451,500	448,000	451,500	483,000	471,500	445,000
z	-1,736	-,381	-1,605	-1,723	-,736	-1,069	-,029	-2,421
Asymp. Sig. (2-seitig)	,083	,703	,108	,085	,462	,285	,977	,015

a. Gruppierungsvariable: Gruppe

Tabelle 94 *Mann-Whitney-U-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen A und D*

Ränge

Score	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	20,95	440,00
	D: Keine Datenschutzskala	19	20,00	380,00
	Gesamtsumme	40		
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	22,55	473,50
	D: Keine Datenschutzskala	19	18,24	346,50
	Gesamtsumme	40		

Fortsetzung Tabelle 94

Score	Gruppe	H	Mittlerer Rang	Summe der Ränge
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	26,71	561,00
	D: Keine Datenschutzskala	19	13,63	259,00
	Gesamtsumme	40		
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	26,38	554,00
	D: Keine Datenschutzskala	19	14,00	266,00
	Gesamtsumme	40		
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	20,93	439,50
	D: Keine Datenschutzskala	19	20,03	380,50
	Gesamtsumme	40		
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	25,55	536,50
	D: Keine Datenschutzskala	19	14,92	283,50
	Gesamtsumme	40		
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	26,40	554,50
	D: Keine Datenschutzskala	19	13,97	265,50
	Gesamtsumme	40		
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	26,52	557,00
	D: Keine Datenschutzskala	19	13,84	263,00
	Gesamtsumme	40		

Teststatistiken[a]

	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	190,000	156,500	69,000	76,000	190,500	93,500	75,500	73,000
Wilcoxon-W	380,000	346,500	259,000	266,000	380,500	283,500	265,500	263,000
z	-,352	-1,490	-3,637	-3,705	-,534	-3,251	-3,600	-4,055
Asymp. Sig. (2-seitig)	,725	,136	,000	,000	,593	,001	,000	,000
Exakte Sig. [2*(1-seitige Sig.)]	,810[b]	,247[b]	,000[b]	,001[b]	,810[b]	,003[b]	,000[b]	,000[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 95 *Mann-Whitney-U-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen B und C*

Ränge

Score	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	23,63	449,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,74	454,00
	Gesamtsumme	42		
Videokonferenz	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	18,79	357,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	23,74	546,00
	Gesamtsumme	42		
Wetter	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	22,42	426,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,74	477,00
	Gesamtsumme	42		
E-Mail	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	20,97	398,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,93	504,50
	Gesamtsumme	42		
Musik	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	26,08	495,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	17,72	407,50
	Gesamtsumme	42		
Fitness	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	23,75	427,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,85	433,50
	Gesamtsumme	41		
Spiele	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	22,13	420,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,98	482,50
	Gesamtsumme	42		

Fortsetzung Tabelle 95

Score	Gruppe	H	Mittlerer Rang	Summe der Ränge
Nachrichten	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	23,84	453,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,57	450,00
	Gesamtsumme	42		

Teststatistiken[a]

	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	178,000	167,000	201,000	208,500	131,500	157,500	206,500	174,000
Wilcoxon-W	454,000	357,000	477,000	398,500	407,500	433,500	482,500	450,000
z	-1,128	-1,638	-,456	-,272	-2,524	-1,881	-,382	-1,456
Asymp. Sig. (2-seitig)	,259	,101	,649	,786	,012	,060	,703	,145

a. Gruppierungsvariable: Gruppe

Tabelle 96 *Mann-Whitney-U-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen B und D*

Ränge

Score	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	19,05	362,00
	D: Keine Datenschutzskala	19	19,95	379,00
	Gesamtsumme	38		
Videokonferenz	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	18,61	353,50
	D: Keine Datenschutzskala	19	20,39	387,50
	Gesamtsumme	38		
Wetter	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	24,03	456,50
	D: Keine Datenschutzskala	19	14,97	284,50
	Gesamtsumme	38		

Fortsetzung Tabelle 96

Score	Gruppe	H	Mittlerer Rang	Summe der Ränge
E-Mail	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	21,34	405,50
	D: Keine Datenschutzskala	19	17,66	335,50
	Gesamtsumme	38		
Musik	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	24,71	469,50
	D: Keine Datenschutzskala	19	14,29	271,50
	Gesamtsumme	38		
Fitness	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	24,44	440,00
	D: Keine Datenschutzskala	19	13,84	263,00
	Gesamtsumme	37		
Spiele	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	25,66	487,50
	D: Keine Datenschutzskala	19	13,34	253,50
	Gesamtsumme	38		
Nachrichten	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	24,74	470,00
	D: Keine Datenschutzskala	19	14,26	271,00
	Gesamtsumme	38		

Teststatistiken[a.b.]

	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	172,000	163,500	94,500	145,500	81,500	73,000	63,500	81,000
Wilcoxon-W	362,000	353,500	284,500	335,500	271,500	263,000	253,500	271,000
z	-,311	-,697	-2,602	-1,244	-3,494	-3,504	-3,683	-3,259
Asymp. Sig. (2-seitig)	,756	,486	,009	,214	,000	,000	,000	,001
Exakte Sig. [2*(1-seitige Sig.)]	,817[b]	,624[b]	,011[b]	,311[b]	,003[b]	,002[b]	,000[b]	,003[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 97 *Mann-Whitney-U-Test Vergleich der Angemessenheit der Applikationsauswahl (Datenschutzscore) nach Datenschutzskala zwischen den Gruppen C und D*

Ränge

Score	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,24	442,50
	D: Keine Datenschutzskala	19	24,24	460,50
	Gesamtsumme	42		
Videokonferenz	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,91	527,00
	D: Keine Datenschutzskala	19	19,79	376,00
	Gesamtsumme	42		
Wetter	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	24,74	569,00
	D: Keine Datenschutzskala	19	17,58	334,00
	Gesamtsumme	42		
E-Mail	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	23,80	547,50
	D: Keine Datenschutzskala	19	18,71	355,50
	Gesamtsumme	42		
Musik	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,70	522,00
	D: Keine Datenschutzskala	19	20,05	381,00
	Gesamtsumme	42		
Fitness	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	25,24	580,50
	D: Keine Datenschutzskala	19	16,97	322,50
	Gesamtsumme	42		
Spiele	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	27,07	622,50
	D: Keine Datenschutzskala	19	14,76	280,50
	Gesamtsumme	42		
Nachrichten	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	24,57	565,00
	D: Keine Datenschutzskala	19	17,79	338,00
	Gesamtsumme	42		

Fortsetzung Tabelle 97

Teststatistiken[a]								
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	166,500	186,000	144,000	165,500	191,000	132,500	90,500	148,000
Wilcoxon-W	442,500	376,000	334,000	355,500	381,000	322,500	280,500	338,000
z	-1,572	-1,036	-1,942	-1,605	-,971	-2,389	-3,527	-1,933
Asymp. Sig. (2-seitig)	,116	,300	,052	,108	,332	,017	,000	,053

a. Gruppierungsvariable: Gruppe

Tabelle 98 *Spearmann-Rho-Test zwischen den Datenschutzscore der Scenarios und des MUIPCs*

		Spearman-Rho							
		Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Technikaffinität	r	0,024	-0,003	0,008	0,104	0,1	0,139	-0,037	0,141
	Sig. (2-seitig)	0,835	0,977	0,941	0,354	0,374	0,217	0,744	0,208
	N	81	81	81	81	81	80	81	81

Tabelle 99 *Auswertung der Entscheidungsmotive über die gesamte Stichprobe*

	Messenger			Videokonferenz			Wetter			E-Mail			Musik			Fitness			Spiele			Nachrichten		
Gesamt	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang
Datenschutzskala	8	6	8	9	14	3	27	15	0	23	13	0	7	19	1	25	12	4	36	6	4	17	15	4
Bekannt aus eigener Nutzung	69	2	0	57	2	0	37	4	0	39	1	0	60	1	0	12	2	0	2	0	0	30	9	0
Bekannt aber nicht selbst genutzt	1	2	0	11	1	0	1	3	0	4	0	0	10	3	0	6	5	0	2	0	0	23	9	0
Verbreitung im Umfeld	3	34	0	1	8	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0
Reihenfolge im App-Markt	1	0	1	0	1	0	4	1	0	3	4	0	0	2	0	9	3	0	11	2	1	2	1	1
Symbolgestaltung	0	0	0	1	2	0	10	5	0	4	4	0	1	0	0	7	9	1	22	16	1	2	1	0
Interface-Gestaltung, Screenshots	0	0	0	0	1	0	0	1	0	1	1	0	0	0	0	0	3	1	1	1	1	0	2	1
Erwartete Funktionalität und Eigenschaften	0	1	1	1	2	1	2	4	1	3	6	2	1	5	1	16	12	5	1	17	2	6	9	3
Bewertungen	0	1	0	1	1	1	0	2	0	2	3	0	0	0	1	0	4	1	0	3	2	0	1	1
Anzahl der Downloads	0	0	0	0	0	0	0	1	0	1	0	0	0	1	0	0	1	0	0	1	0	0	0	0
Benennung der App	0	0	1	1	0	1	0	3	2	3	2	1	1	1	0	5	6	3	6	4	5	0	1	0
Datenschutz-Diagramme	0	0	0	0	1	0	0	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0
Summe	82	46	11	82	33	6	81	39	3	82	36	3	82	32	4	81	57	15	81	50	16	80	48	10

Tabelle 100 *Auswertung der Entscheidungsmotive sortiert nach Gruppe A*

Gruppe A	Messenger			Videokonferenz			Wetter			E-Mail			Musik			Fitness			Spiele			Nachrichten		
	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang
Datenschutzskala	2	5	3	4	7	3	10	6	0	12	4	0	2	9	0	11	5	1	13	2	3	7	7	1
Bekannt aus eigener Nutzung	17	0	0	14	1	0	10	1	0	5	0	0	17	0	0	2	1	0	0	0	0	5	3	1
Bekannt aber nicht selbst genutzt	0	2	0	3	1	0	0	1	0	0	0	0	2	1	0	1	2	0	1	0	0	9	3	0
Verbreitung im Umfeld	2	9	0	0	3	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Reihenfolge im App-Markt	0	0	1	0	0	0	1	0	0	1	1	0	0	1	0	2	1	0	0	1	0	0	0	0
Symbolgestaltung	0	0	0	0	0	0	0	1	0	1	2	0	0	0	0	1	2	0	3	5	0	0	0	0
Interface-Gestaltung, Screenshots	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Erwartete Funktionalität und Eigenschaften	0	0	1	0	1	1	0	2	0	1	1	1	0	1	1	3	4	2	0	1	5	0	4	2
Bewertungen	0	1	0	0	0	0	0	1	0	0	2	0	0	0	1	0	1	0	0	0	0	0	0	0
Anzahl der Downloads	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0
Benennung der App	0	0	1	0	0	0	0	0	1	1	0	1	0	0	0	0	1	2	4	1	2	0	0	0
Datenschutz-Diagramme	0	0	0	0	1	0	0	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0
Summe	21	17	6	21	14	4	21	13	1	21	12	2	21	13	3	21	18	5	21	16	6	21	17	4

Tabelle 101 *Auswertung der Entscheidungsmotive sortiert nach Gruppe B*

Gruppe B	Messenger			Videokonferenz			Wetter			E-Mail			Musik			Fitness			Spiele			Nachrichten		
	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang
Datenschutzskala	4	0	2	2	5	0	9	3	0	4	7	0	3	4	1	7	3	1	10	2	0	5	2	1
Bekannt aus eigener Nutzung	12	2	0	12	0	0	7	2	0	9	0	0	12	1	0	2	0	0	1	0	0	6	2	0
Bekannt aber nicht selbst genutzt	1	0	0	3	0	0	0	2	0	2	0	0	2	2	0	0	3	0	0	0	0	5	4	0
Verbreitung im Umfeld	1	8	0	0	2	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Reihenfolge im App-Markt	1	0	0	0	0	0	1	0	0	1	1	0	0	1	0	1	0	0	1	1	0	0	0	1
Symbolgestaltung	0	0	0	0	1	0	2	0	0	1	1	0	0	0	0	0	2	0	5	2	0	0	0	0
Interface-Gestaltung, Screenshots	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	1	0
Erwartete Funktionalität und Eigenschaften	0	1	0	1	1	0	0	2	0	0	3	0	0	1	0	7	4	0	0	5	0	2	1	1
Bewertungen	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1
Anzahl der Downloads	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Benennung der App	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	1	1	0	0	0
Datenschutz-Diagramme	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Summe	19	11	2	19	9	0	19	10	0	19	12	0	19	9	1	18	13	2	18	11	1	18	11	4

Tabelle 102 *Auswertung der Entscheidungsmotive sortiert nach Gruppe C*

Gruppe C	Messenger			Videokonferenz			Wetter			E-Mail			Musik			Fitness			Spiele			Nachrichten		
	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang
Datenschutzskala	2	1	3	3	2	0	8	6	0	7	2	0	2	6	0	7	4	2	13	2	1	5	6	2
Bekannt aus eigener Nutzung	21	0	0	16	0	0	7	1	0	11	0	0	15	0	0	5	0	0	0	0	0	9	4	0
Bekannt aber nicht selbst genutzt	0	0	0	3	0	0	1	0	0	1	0	0	3	0	0	1	0	0	0	0	0	6	1	0
Verbreitung im Umfeld	0	6	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Reihenfolge im App-Markt	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	4	2	0	4	0	1	0	0	0
Symbolgestaltung	0	0	0	0	1	0	4	2	0	1	0	0	1	0	0	1	2	0	5	6	1	1	1	0
Interface-Gestaltung, Screenshots	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1	0
Erwartete Funktionalität und Eigenschaften	0	0	0	0	0	0	2	0	0	0	2	0	1	0	0	3	2	0	0	2	0	2	0	0
Bewertungen	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Anzahl der Downloads	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Benennung der App	0	0	0	1	0	1	0	0	1	1	1	0	1	1	0	2	1	1	1	1	1	0	0	0
Datenschutz-Diagramme	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Summe	23	7	3	23	5	1	22	10	1	23	6	0	23	7	0	23	12	4	23	11	4	23	13	2

Tabelle 103 *Auswertung der Entscheidungsmotive sortiert nach Gruppe D*

Gruppe D	Messenger			Videokonferenz			Wetter			E-Mail			Musik			Fitness			Spiele			Nachrichten		
	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang	1.Rang	2.Rang	3.Rang
Datenschutzskala	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bekannt aus eigener Nutzung	19	0	0	15	1	0	13	0	0	14	1	0	16	0	0	3	1	0	1	0	0	10	0	0
Bekannt aber nicht selbst genutzt	0	0	0	2	0	0	0	0	0	1	0	0	3	0	0	4	0	0	1	0	0	3	1	0
Verbreitung im Umfeld	0	11	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Reihenfolge im App-Markt	0	0	0	0	1	0	2	0	0	0	1	0	0	0	0	2	0	0	6	0	0	2	1	0
Symbolgestaltung	0	0	0	1	0	0	4	2	0	1	1	0	0	0	0	5	3	1	9	3	0	1	0	0
Interface-Gestaltung, Screenshots	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0	0	0
Erwartete Funktionalität und Eigenschaften	0	0	0	0	0	0	0	0	1	2	0	1	0	3	0	3	2	3	1	5	1	2	4	0
Bewertungen	0	0	0	0	1	1	0	1	0	1	1	0	0	0	0	0	3	0	0	3	2	0	0	0
Anzahl der Downloads	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Benennung der App	0	0	0	0	0	0	0	3	0	0	1	0	0	0	0	2	4	0	1	1	1	0	1	0
Datenschutz-Diagramme	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Summe	19	11	0	19	5	1	19	6	1	19	6	1	19	3	0	19	14	4	19	12	5	18	7	0

Tabelle 104 *Kruskal-Wallis-Test Vergleich des App-Scores nach der Entscheidungsmotive zwischen den Gruppen*

Ränge			
Aussagen	Gruppe	H	Mittlerer Rang
Messenger	1: Datenschutzskala als wichtigstes Auswahlmotiv	8	70,1
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	14	42,7
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	60	37,4
	Gesamtsumme		
Videokonferenz	1: Datenschutzskala als wichtigstes Auswahlmotiv	9	70,9
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	17	40,2
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	56	37,2
	Gesamtsumme		
Wetter	1: Datenschutzskala als wichtigstes Auswahlmotiv	27	62,1
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	15	43,9
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	39	25,3
	Gesamtsumme		
E-Mail	1: Datenschutzskala als wichtigstes Auswahlmotiv	23	66,6
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	13	40,0
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	46	29,4
	Gesamtsumme		
Musik	1: Datenschutzskala als wichtigstes Auswahlmotiv	7	67,9
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	20	39,9
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	55	38,7
	Gesamtsumme		
Fitness	1: Datenschutzskala als wichtigstes Auswahlmotiv	25	53,0
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	16	44,1
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	40	32,3
	Gesamtsumme		
Spiele	1: Datenschutzskala als wichtigstes Auswahlmotiv	36	56,5
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	10	42,1
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	35	24,7
	Gesamtsumme		

Fortsetzung Tabelle 104

Aussagen	Gruppe	H	Mittlerer Rang
Nachrichten	1: Datenschutzskala als wichtigstes Auswahlmotiv	17	53,0
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	19	49,7
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	44	31,7
	Gesamtsumme		

Teststatistiken[a,b]

Aussage	Chi-Quadrat	df	Asymp. Sig.
Messenger	18,836	2	.000
Videokonferenz	25,110	2	.000
Wetter	41,565	2	.000
E-Mail	44,548	2	.000
Musik	16,289	2	.000
Fitness	18,905	2	.000
Spiele	41,237	2	.000
Nachrichten	21,281	2	.000

a. Kruskal-Wallis-Test

b. Gruppierungsvariable: Gruppe

Tabelle 105 *Mann-Whitney-U-Test Vergleich Gruppe 1 und 2*

Ränge

Score	Gruppe	H	Mittlerer Rang
Messenger	1: Datenschutzskala als wichtigstes Auswahlmotiv	8	16,50
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	14	8,64
	Gesamtsumme	22	
Videokonferenz	1: Datenschutzskala als wichtigstes Auswahlmotiv	9	20,56
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	17	9,76
	Gesamtsumme	26	
Wetter	1: Datenschutzskala als wichtigstes Auswahlmotiv	27	25,80
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	15	13,77
	Gesamtsumme	42	
E-Mail	1: Datenschutzskala als wichtigstes Auswahlmotiv	23	23,39
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	13	9, 85
	Gesamtsumme	36	
Musik	1: Datenschutzskala als wichtigstes Auswahlmotiv	7	21,07
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	20	11,53
	Gesamtsumme	27	
Fitness	1: Datenschutzskala als wichtigstes Auswahlmotiv	25	23,00
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	16	17,88
	Gesamtsumme	41	
Spiele	1: Datenschutzskala als wichtigstes Auswahlmotiv	36	25,78
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	10	15,30
	Gesamtsumme	46	
Nachrichten	1: Datenschutzskala als wichtigstes Auswahlmotiv	17	19,50
	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	19	17,61
	Gesamtsumme	36	

Fortsetzung Tabelle 105

Teststatistiken[a]								
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	16,00	13,00	86,50	37,00	20,50	150,00	98,00	144,50
z	-3,127	-4,150	-3,262	-4,032	-3,352	-2,596	-3,500	-1,357
Asymp. Sig. (2-seitig)	,003	,000	,002	,000	,001	,014	,001	,262

a. Gruppierungsvariable: Gruppe

Tabelle 106 *Mann-Whitney-U-Test Vergleich Gruppe 1 und 3*

Ränge			
Score	Gruppe	H	Mittlerer Rang
Messenger	1: Datenschutzskala als wichtigstes Auswahlmotiv	8	58,13
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	60	31,35
	Gesamtsumme	68	
Videokonferenz	1: Datenschutzskala als wichtigstes Auswahlmotiv	9	55,33
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	56	29,41
	Gesamtsumme		
Wetter	1: Datenschutzskala als wichtigstes Auswahlmotiv	27	50,26
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	39	21,90
	Gesamtsumme		
E-Mail	1: Datenschutzskala als wichtigstes Auswahlmotiv	23	55,24
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	46	24,88
	Gesamtsumme		
Musik	1: Datenschutzskala als wichtigstes Auswahlmotiv	7	50,79
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	55	29,05
	Gesamtsumme		
Fitness	1: Datenschutzskala als wichtigstes Auswahlmotiv	25	43,00
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	40	26,75
	Gesamtsumme	65	
Spiele	1: Datenschutzskala als wichtigstes Auswahlmotiv	36	49,25
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	35	22,37
	Gesamtsumme	71	

Fortsetzung Tabelle 106

Score	Gruppe	H	Mittlerer Rang
Nachrichten	1: Datenschutzskala als wichtigstes Auswahlmotiv	17	42,50
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	44	26,56
	Gesamtsumme		

Teststatistiken[a]

	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	51,00	51,00	74,00	63,50	57,50	250,00	153,00	178,50
z	-4,183	-4,562	-6,069	-6,375	-3,788	-4,132	-6,237	-3,637
Asymp. Sig. (2-seitig)	,000	,000	,000	,000	,000	,000	,000	,000

a. Gruppierungsvariable: Gruppe

Tabelle 107 *Mann-Whitney-U-Test Vergleich Gruppe 2 und 3*

Ränge

Score	Gruppe	H	Mittlerer Rang
Messenger	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	14	41,54
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	60	36,56
	Gesamtsumme	74	
Videokonferenz	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	17	39,41
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	56	36,27
	Gesamtsumme		
Wetter	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	15	38,10
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	39	23,42
	Gesamtsumme		
E-Mail	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	13	37,12
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	46	27,99
	Gesamtsumme		
Musik	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	20	38,90
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	55	37,67
	Gesamtsumme		

Fortsetzung Tabelle 107

Score	Gruppe	H	Mittlerer Rang
Fitness	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	16	34,69
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	40	26,03
	Gesamtsumme	56	
Spiele	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	10	32,75
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	35	20,36
	Gesamtsumme	45	
Nachrichten	2: Datenschutzskala als zweit- oder drittwichtigstes Auswahlmotiv	19	42,13
	3: Datenschutzskala hatte keinen Einfluss auf die Entscheidung	44	27,63
	Gesamtsumme		

Teststatistiken[a]

	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	363,50	435,00	133,00	206,50	532,00	221,00	82,50	225,50
z	-0,969	-0,759	-3,220	-2,120	-0,310	-1,999	-2,703	-3,285
Asymp. Sig. (2-seitig)	,499	,672	,002	,051	1,000	,068	,010	,002

a. Gruppierungsvariable: Gruppe

Tabelle 108 *Bekanntheit der ausgewählten Applikation*

Applikation	Bekanntheit der ausgewählten Applikation									
	installiert und bereits verwendet		installiert und noch nicht verwendet		bereits verwendet, derzeit jedoch nicht installiert		nicht installiert und noch nicht verwendet		keine Antwort	
	Anzahl	**Prozent**	**Anzahl**	**Prozent**	**Anzahl**	**Prozent**	**Anzahl**	**Prozent**	**Anzahl**	**Prozent**
Messenger	66	78,6	1	1,2	2	2,4	13	15,5	0	0
Videokonferenz	33	39,3	7	8,3	21	25	21	25	0	0
Wetter	14	16,7	2	2,4	17	20,2	29	34,5	20	23,8
E-Mail	18	21,4	2	2,4	12	14,3	37	44	13	15,5
Musik	41	48,8	4	4,8	11	13,1	24	28,6	2	2,4
Fitness	9	10,7	0	0	12	14,3	59	70,2	1	1,2
Spiele	2	2,4	0	0	2	2,4	78	92,9	0	0
Nachrichten	9	10,7	3	3,6	23	27,4	47	56	0	0

Tabelle 109 *Bekanntheit der ausgewählten Applikation nach Gruppen getrennt*

	Bekanntheit der ausgewählten Applikation	Gruppe							
		A		B		C		D	
		Anzahl	**Prozent**	**Anzahl**	**Prozent**	**Anzahl**	**Prozent**	**Anzahl**	**Prozent**
Messenger	installiert und bereits verwendet	18	85,70	13	68,40	19	82,60	16,00	84,20
	installiert und noch nicht verwendet	0		0		1	4,30	0	
	bereits verwendet, derzeit jedoch nicht installiert	0		0		0		2	10,50
	nicht installiert und noch nicht verwendet	3	14,29	6	31,60	3	13,00	1	5,30
	keine Antwort	0		0		0		0	
Videokonferenz	installiert und bereits verwendet	7	33,30	6	31,60	9	39,10	11	57,90
	installiert und noch nicht verwendet	3	14,30	2	10,50	1	4,30	1	5,30
	bereits verwendet, derzeit jedoch nicht installiert	6	28,60	6	31,60	7	30,40	2	10,50
	nicht installiert und noch nicht verwendet	5	23,80	5	26,30	6	26,10	5	26,30
	keine Antwort	0		0		0		0	

Fortsetzung Tabelle 109

	Bekanntheit der ausgewählten Applikation	Gruppe							
		A		B		C		D	
		Anzahl	Prozent	Anzahl	Prozent	Anzahl	Prozent	Anzahl	Prozent
Wetter	installiert und bereits verwendet	2	9,50	5	26,30	4	17,40	3	15,80
	installiert und noch nicht verwendet	1	4,80	0		1	4,30	0	
	bereits verwendet, derzeit jedoch nicht installiert	7	33,30	2	10,50	2	8,70	6	31,60
	nicht installiert und noch nicht verwendet	8	38,10	9	47,40	9	39,10	3	15,80
	keine Antwort	3	14,30	3	15,80	7	30,40	7	36,80
E-Mail	installiert und bereits verwendet	3	14,30	6	31,60	5	21,70	4	21,10
	installiert und noch nicht verwendet	0		0		0		2	10,50
	bereits verwendet, derzeit jedoch nicht installiert	1	4,80	2	10,50	4	17,40	5	26,30
	nicht installiert und noch nicht verwendet	9	42,90	8	42,10	12	52,20	8	42,10
	keine Antwort	8	38,10	3	15,80	2	8,70	0	
Musik	installiert und bereits verwendet	11	52,40	6	31,60	11	47,80	13	68,40
	installiert und noch nicht verwendet	1	4,80	1	5,30	1	4,30	1	5,30
	bereits verwendet, derzeit jedoch nicht installiert	4	19,00	4	21,10	2	8,70	1	5,30
	nicht installiert und noch nicht verwendet	4	19,00	8	42,10	8	34,80	4	21,10
	keine Antwort	1	4,80	0		1	4,30	0	
Fitness	installiert und bereits verwendet	3	14,3	2	10,50	3	13,00	1	5,30
	installiert und noch nicht verwendet	0		0		0		0	
	bereits verwendet, derzeit jedoch nicht installiert	3	14,3	3	15,80	3	13,00	3	15,80
	nicht installiert und noch nicht verwendet	15	71,4	13	68,40	16	69,60	15	78,90
	keine Antwort	0		0		1	4,30	0	
Spiele	installiert und bereits verwendet	1	4,80	0		1	4,30	0	
	installiert und noch nicht verwendet	0		0		0		0	
	bereits verwendet, derzeit jedoch nicht installiert	1	4,80	0		0		1	5,30
	nicht installiert und noch nicht verwendet	19	90,50	19	100,00	22	95,70	18	94,70
	keine Antwort	0		0		0		0	

Fortsetzung Tabelle 109

	Bekanntheit der ausgewählten Applikation	Gruppe							
		A		B		C		D	
		Anzahl	Prozent	Anzahl	Prozent	Anzahl	Prozent	Anzahl	Prozent
Nachrichten	installiert und bereits verwendet	2	9,50	1	5,30	3	13,00	3	15,80
	installiert und noch nicht verwendet	1	4,80	0		1	4,30	1	5,30
	bereits verwendet, derzeit jedoch nicht installiert	6	28,60	6	31,60	6	26,10	5	26,30
	nicht installiert und noch nicht verwendet	12	57,10	12	63,2	13	56,5	10	52,6
	keine Antwort	0		0		0		0	

Anmerkung. Bekanntheit der ausgewählten Applikation verglichen unter den Gruppen farblich in absteigender Reihenfolge markiert: orange, gelb, hellgrün, dunkelgrün.

Tabelle 110 *Bewertung der Datenschutzskala*

Attribut	Gruppe A				Gruppe B				Gruppe C				Gesamt			
	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV
Vertrauenswürdig	21	5,67	1,317	0,082	18	5,5	1,043	0	22	5	1,272	0	61	5,38	1,24	0
Gut	21	6,1	0,889	0	17	5,94	0,966	0,033	22	5,91	0,868	0,006	60	5,98	0,892	0
Verständlich	21	6,33	0,913	0	18	6	0,84	0,001	23	6,13	0,869	0,002	62	6,16	0,872	0
Intuitiv	21	5,48	1,632	0	18	5,72	1,364	0,005	23	5,74	1,054	0,001	62	5,65	1,344	0
Gültig	21	5,43	1,326	0,045	16	5,25	1,065	0,098	23	4,74	1,322	0,003	60	5,12	1,277	0
Zuverlässig	21	5,43	1,248	0,002	17	5,18	1,237	0,031	23	4,96	1,331	0,001	61	5,18	1,272	0
Auswirkungen Applikationsauswhal	21	5,86	1,558	0	18	5,39	1,461	0	23	4,78	1,833	0,001	62	5,32	1,677	0
Verwirrend	21	2,1	1,136	0,001	18	2,22	1,665	0,001	23	2,17	1,029	0,051	62	2,16	1,257	0
Nicht genug	21	3,05	1,687	0,2	18	3,11	1,41	0,013	23	4,48	1,855	0,005	62	3,6	1,788	0,002
Erhöht Privatsphäregefühl	21	5,86	1,315	0	18	5,83	1,2	0,001	23	5,65	1,641	0	62	5,77	1,396	0
Möchte Skalen in App-Markt	20	5,8	1,609	0,002	18	5,56	1,653	0,001	23	5,7	1,636	0,004	61	5,69	1,608	0
Komplex	21	2,1	1,3	0	18	2,56	1,886	0,001	23	2,04	1,492	0,001	62	2,21	1,549	0
Aktivieren Erhöhung	21	6,24	1,261	0	18	5,78	1,592	0,018	23	5,74	1,839	0	62	5,92	1,582	0
Vertrauenswürdigkeit der Applikation	21	6,24	0,944	0	18	6,06	1,392	0	23	5,83	1,302	0	62	6,03	1,214	0

Anmerkung. Bewertung der Datenschutzskala verglichen zwischen den Gruppen: höchster Mittelwert (rot) und niedrigster Mittelwert (grün).

Tabelle 111 *Kruskal-Wallis-Test Vergleich der Bewertung der Datenschutzskala zwischen den Gruppen*

Ränge

Aussagen	Gruppe	H	Mittlerer Rang
Die Privatsphäreskala ist vertrauenswürdig.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	35,21
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	32,78
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	25,52
	Gesamtsumme	61	
Die Benutzerfreundlichkeit der Privatsphäreskala ist gut.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	32,93
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	29,76
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	28,75
	Gesamtsumme	60	
Die Privatsphäreskala ist leicht zu verstehen.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	35,55
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	27,78
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	30,72
	Gesamtsumme	62	
Die Privatsphäreskala ist intuitiv.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	30,67
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	32,78
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	31,26
	Gesamtsumme	62	
Die Privatsphäreskala ist gültig.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	34,93
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	31,28
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	25,91
	Gesamtsumme	60	

Fortsetzung Tabelle 111

Aussagen	Gruppe	H	Mittlerer Rang
Die Privatsphäreskala ist zuverlässig.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	34,48
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	30,71
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	28,04
	Gesamtsumme	61	
Die Privatsphäreskala hatte Auswirkungen auf meine Wahl.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	38,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	31,42
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	25,63
	Gesamtsumme	62	
Die Privatsphäreskala ist verwirrend.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	31,24
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	29,72
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	33,13
	Gesamtsumme	62	
Die von der Privatsphäreskala bereitgestellten Informationen sind für die Benutzenden nicht ausreichend.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	26,02
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	26,89
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	40,11
	Gesamtsumme	62	
Die Privatsphäreskala erhöht das Gefühl des Schutzes der Privatsphäre.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	32,24
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	31,31
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	30,98
	Gesamtsumme	62	

Fortsetzung Tabelle 111

Aussagen	Gruppe	H	Mittlerer Rang
Ich hätte gerne eine Privatsphäreskala in meinem eigenen App-Markt.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	32,38
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	29,17
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	31,24
	Gesamtsumme	61	
Die Privatsphäreskala ist unnötig komplex.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	31,02
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	34,25
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	29,78
	Gesamtsumme	62	
Wenn es möglich wäre, die Privatsphäreskala zu aktivieren und deaktivieren würde ich die Privatsphäreskala aktivieren.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	34,71
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	29,14
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	30,41
	Gesamtsumme	62	
Die Privatsphäreskala erhöht die Vertrauenswürdigkeit der Applikation.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	34,57
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	32,86
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	27,63
	Gesamtsumme	62	

Fortsetzung Tabelle 111

Teststatistiken[a,b]

Aussage	Chi-Quadrat	df	Asymp. Sig.
Die Privatsphäreskala ist vertrauenswürdig.	3,791	2	0,15
Die Benutzerfreundlichkeit der Privatsphäreskala ist gut.	0,74	2	0,691
Die Privatsphäreskala ist leicht zu verstehen.	2,143	2	0,343
Die Privatsphäreskala ist intuitiv.	0,153	2	0,926
Die Privatsphäreskala ist gültig.	3,171	2	0,205
Die Privatsphäreskala ist zuverlässig.	1,545	2	0,462
Die Privatsphäreskala hatte Auswirkungen auf meine Wahl.	5,46	2	0,065
Die Privatsphäreskala ist verwirrend.	0,404	2	0,817
Die von der Privatsphäreskala bereitgestellten Informationen sind für die Benutzenden nicht ausreichend.	8,583	2	0,014
Die Privatsphäreskala erhöht das Gefühl des Schutzes der Privatsphäre.	0,064	2	0,969
Ich hätte gerne eine Privatsphäreskala in meinem eigenen App-Markt.	0,348	2	0,84
Die Privatsphäreskala ist unnötig komplex.	0,72	2	0,698
Wenn es möglich wäre, die Privatsphäreskala zu aktivieren und deaktivieren würde ich die Privatsphäreskala aktivieren.	1,235	2	0,539
Die Privatsphäreskala erhöht die Vertrauenswürdigkeit der Applikation.	2,091	2	0,352

a. Kruskal-Wallis-Test

b. Gruppierungsvariable: Gruppe

Tabelle 112 *Mann-Whitney-U-Test Vergleich der Bewertung der Datenschutzskala zwischen den Gruppen A und B*

Ränge				
Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Die Privatsphäreskala ist vertrauenswürdig.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	20,98	440,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	18,86	339,50
	Gesamtsumme	39		
Die Benutzerfreundlichkeit der Privatsphäreskala ist gut.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	20,33	427,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	18,47	314,00
	Gesamtsumme	38		
Die Privatsphäreskala ist leicht zu verstehen.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	22,26	467,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	17,36	312,50
	Gesamtsumme	39		
Die Privatsphäreskala ist intuitiv.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,38	407,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	20,72	373,00
	Gesamtsumme	39		
Die Privatsphäreskala ist gültig.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	20,00	420,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	17,69	283,00
	Gesamtsumme	37		

Fortsetzung Tabelle 112

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Die Privatsphäreskala ist zuverlässig.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	20,55	431,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	18,21	309,50
	Gesamtsumme	38		
Die Privatsphäreskala hatte Auswirkungen auf meine Wahl.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	22,17	465,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	17,47	314,50
	Gesamtsumme	39		
Die Privatsphäreskala ist verwirrend.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	20,31	426,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,64	353,50
	Gesamtsumme	39		
Die von der Privatsphäreskala bereitgestellten Informationen sind für die Benutzenden nicht ausreichend.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,67	413,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	20,39	367,00
	Gesamtsumme	39		
Die Privatsphäreskala erhöht das Gefühl des Schutzes der Privatsphäre.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	20,29	426,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,67	354,00
	Gesamtsumme	39		

Fortsetzung Tabelle 112

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Ich hätte gerne eine Privatsphäreskala in meinem eigenen App-Markt.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	20,45	409,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	18,44	332,00
	Gesamtsumme	38		
Die Privatsphäreskala ist unnötig komplex.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,00	399,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	21,17	381,00
	Gesamtsumme	39		
Wenn es möglich wäre, die Privatsphäreskala zu aktivieren und deaktivieren würde ich die Privatsphäreskala aktivieren.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	21,64	454,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	18,08	325,50
	Gesamtsumme	39		
Die Privatsphäreskala erhöht die Vertrauenswürdigkeit der Applikation.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	20,55	431,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,36	348,50
	Gesamtsumme	39		

Fortsetzung Tabelle 112

Teststatistiken[a,b]

Aussage	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)	Exakte Sig. [2*(1-seitige Sig.)]
Die Privatsphäreskala ist vertrauenswürdig.	168,5	339,5	-0,608	0,543	,568b
Die Benutzerfreundlichkeit der Privatsphäreskala ist gut.	161	314	-0,547	0,584	,622b
Die Privatsphäreskala ist leicht zu verstehen.	141,5	312,5	-1,437	0,151	,183b
Die Privatsphäreskala ist intuitiv.	176	407	-0,385	0,7	,728b
Die Privatsphäreskala ist gültig.	147	283	-0,664	0,506	,534b
Die Privatsphäreskala ist zuverlässig.	156,5	309,5	-0,669	0,504	,523b
Die Privatsphäreskala hatte Auswirkungen auf meine Wahl.	143,5	314,5	-1,332	0,183	,202b
Die Privatsphäreskala ist verwirrend.	182,5	353,5	-0,194	0,846	,856b
Die von der Privatsphäreskala bereitgestellten Informationen sind für die Benutzenden nicht ausreichend.	182	413	-0,201	0,841	,856b
Die Privatsphäreskala erhöht das Gefühl des Schutzes der Privatsphäre.	183	354	-0,181	0,856	,878b
Ich hätte gerne eine Privatsphäreskala in meinem eigenen App-Markt.	161	332	-0,582	0,561	,593b
Die Privatsphäreskala ist unnötig komplex.	168	399	-0,623	0,533	,568b
Wenn es möglich wäre, die Privatsphäreskala zu aktivieren und deaktivieren würde ich die Privatsphäreskala aktivieren.	154,5	325,5	-1,056	0,291	,335b
Die Privatsphäreskala erhöht die Vertrauenswürdigkeit der Applikation.	177,5	348,5	-0,355	0,723	,749b

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 113 *Mann-Whitney-U-Test Vergleich der Bewertung der Datenschutzskala zwischen den Gruppen A und C*

Ränge

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Die Privatsphäreskala ist vertrauenswürdig.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	25,24	530,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	18,91	416,00
	Gesamtsumme	43		
Die Benutzerfreundlichkeit der Privatsphäreskala ist gut.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	23,60	495,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	20,48	450,50
	Gesamtsumme	43		
Die Privatsphäreskala ist leicht zu verstehen.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	24,29	510,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,87	480,00
	Gesamtsumme	44		
Die Privatsphäreskala ist intuitiv.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	22,29	468,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,70	522,00
	Gesamtsumme	44		
Die Privatsphäreskala ist gültig.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	25,93	544,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,37	445,50
	Gesamtsumme	44		
Die Privatsphäreskala ist zuverlässig.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	24,93	523,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,28	466,50
	Gesamtsumme	44		
Die Privatsphäreskala hatte Auswirkungen auf meine Wahl.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	26,83	563,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,54	426,50
	Gesamtsumme	44		

Fortsetzung Tabelle 113

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Die Privatsphäreskala ist verwirrend.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	21,93	460,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	23,02	529,50
	Gesamtsumme	44		
Die von der Privatsphäreskala bereitgestellten Informationen sind für die Benutzenden nicht ausreichend.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	17,36	364,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	27,20	625,50
	Gesamtsumme	44		
Die Privatsphäreskala erhöht das Gefühl des Schutzes der Privatsphäre.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	22,95	482,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,09	508,00
	Gesamtsumme	44		
Ich hätte gerne eine Privatsphäreskala in meinem eigenen App-Markt.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	22,43	448,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,63	497,50
	Gesamtsumme	43		
Die Privatsphäreskala ist unnötig komplex.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	23,02	483,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,02	506,50
	Gesamtsumme	44		
Wenn es möglich wäre, die Privatsphäreskala zu aktivieren und deaktivieren würde ich die Privatsphäreskala aktivieren.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	24,07	505,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,07	484,50
	Gesamtsumme	44		
Die Privatsphäreskala erhöht die Vertrauenswürdigkeit der Applikation.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	25,02	525,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,20	464,50
	Gesamtsumme	44		

Fortsetzung Tabelle 113

Teststatistiken[a,b]				
Aussage	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)
Die Privatsphäreskala ist vertrauenswürdig.	163	416	-1,712	0,087
Die Benutzerfreundlichkeit der Privatsphäreskala ist gut.	197,5	450,5	-0,874	0,382
Die Privatsphäreskala ist leicht zu verstehen.	204	480	-0,953	0,341
Die Privatsphäreskala ist intuitiv.	237	468	-0,112	0,911
Die Privatsphäreskala ist gültig.	169,5	445,5	-1,747	0,081
Die Privatsphäreskala ist zuverlässig.	190,5	466,5	-1,238	0,216
Die Privatsphäreskala hatte Auswirkungen auf meine Wahl.	150,5	426,5	-2,202	0,028
Die Privatsphäreskala ist verwirrend.	229,5	460,5	-0,295	0,768
Die von der Privatsphäreskala bereitgestellten Informationen sind für die Benutzenden nicht ausreichend.	133,5	364,5	-2,57	0,01
Die Privatsphäreskala erhöht das Gefühl des Schutzes der Privatsphäre.	232	508	-0,237	0,812
Ich hätte gerne eine Privatsphäreskala in meinem eigenen App-Markt.	221,5	497,5	-0,219	0,827
Die Privatsphäreskala ist unnötig komplex.	230,5	506,5	-0,276	0,782
Wenn es möglich wäre, die Privatsphäreskala zu aktivieren und deaktivieren würde ich die Privatsphäreskala aktivieren.	208,5	484,5	-0,848	0,397
Die Privatsphäreskala erhöht die Vertrauenswürdigkeit der Applikation.	188,5	464,5	-1,345	0,179

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 114 *Mann-Whitney-U-Test Vergleich der Bewertung der Datenschutzskala zwischen den Gruppen B und C*

Ränge				
Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Die Privatsphäreskala ist vertrauenswürdig.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	23,42	421,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	18,11	398,50
	Gesamtsumme	40		
Die Benutzerfreundlichkeit der Privatsphäreskala ist gut.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	20,29	345,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	19,77	435,00
	Gesamtsumme	39		
Die Privatsphäreskala ist leicht zu verstehen.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,92	358,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,85	502,50
	Gesamtsumme	41		
Die Privatsphäreskala ist intuitiv.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	21,56	388,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,57	473,00
	Gesamtsumme	41		
Die Privatsphäreskala ist gültig.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	16	22,09	353,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,54	426,50
	Gesamtsumme	39		
Die Privatsphäreskala ist zuverlässig.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	21,50	365,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,76	454,50
	Gesamtsumme	40		
Die Privatsphäreskala hatte Auswirkungen auf meine Wahl.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	23,44	422,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,09	439,00
	Gesamtsumme	41		

Fortsetzung Tabelle 114

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Die Privatsphäreskala ist verwirrend.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,58	352,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,11	508,50
	Gesamtsumme	41		
Die von der Privatsphäreskala bereitgestellten Informationen sind für die Benutzenden nicht ausreichend.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	16,00	288,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	24,91	573,00
	Gesamtsumme	41		
Die Privatsphäreskala erhöht das Gefühl des Schutzes der Privatsphäre.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	21,14	380,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,89	480,50
	Gesamtsumme	41		
Ich hätte gerne eine Privatsphäreskala in meinem eigenen App-Markt.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	20,22	364,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,61	497,00
	Gesamtsumme	41		
Die Privatsphäreskala ist unnötig komplex.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	22,58	406,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,76	454,50
	Gesamtsumme	41		
Wenn es möglich wäre, die Privatsphäreskala zu aktivieren und deaktivieren würde ich die Privatsphäreskala aktivieren.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	20,56	370,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,35	491,00
	Gesamtsumme	41		
Die Privatsphäreskala erhöht die Vertrauenswürdigkeit der Applikation.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	23,00	414,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,43	447,00
	Gesamtsumme	41		

Fortsetzung Tabelle 114

Teststatistiken[a,b]					
Aussage	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)	Exakte Sig. [2*(1-seitige Sig.)]
Die Privatsphäreskala ist vertrauenswürdig.	145,5	398,5	-1,537	0,124	,155b
Die Benutzerfreundlichkeit der Privatsphäreskala ist gut.	182	435	-0,149	0,882	,900b
Die Privatsphäreskala ist leicht zu verstehen.	187,5	358,5	-0,549	0,583	
Die Privatsphäreskala ist intuitiv.	197	473	-0,274	0,784	
Die Privatsphäreskala ist gültig.	150,5	426,5	-0,995	0,32	,343b
Die Privatsphäreskala ist zuverlässig.	178,5	454,5	-0,481	0,63	,645b
Die Privatsphäreskala hatte Auswirkungen auf meine Wahl.	163	439	-1,199	0,23	
Die Privatsphäreskala ist verwirrend.	181,5	352,5	-0,702	0,483	
Die von der Privatsphäreskala bereitgestellten Informationen sind für die Benutzenden nicht ausreichend.	117	288	-2,409	0,016	
Die Privatsphäreskala erhöht das Gefühl des Schutzes der Privatsphäre.	204,5	480,5	-0,069	0,945	
Ich hätte gerne eine Privatsphäreskala in meinem eigenen App-Markt.	193	364	-0,384	0,701	
Die Privatsphäreskala ist unnötig komplex.	178,5	454,5	-0,792	0,429	
Wenn es möglich wäre, die Privatsphäreskala zu aktivieren und deaktivieren würde ich die Privatsphäreskala aktivieren.	199	370	-0,224	0,823	
Die Privatsphäreskala erhöht die Vertrauenswürdigkeit der Applikation.	171	447	-1,036	0,3	

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 115 *Einfachheit der Auswahl und Vertrauenswürdigkeit der Applikation geteilt nach Gruppen*

Deskriptive Statistiken									
Applikation		Gruppe A		Gruppe B		Gruppe C		Gruppe D	
		M	SD	M	SD	M	SD	M	SD
Messenger	Einfachheit der Auswahl	6,24	1,044	6,37	0,955	5,91	1,203	6,42	0,769
	Vertrauenswürdigkeit	4,43	1,748	5	1,414	4,65	1,229	3,74	1,851
Videokonferenz	Einfachheit der Auswahl	6,11	1,197	5,89	0,937	6,13	0,869	6,06	1,211
	Vertrauenswürdigkeit	5	2,098	5	1,795	4,96	1,364	4,05	1,715
Wetter	Einfachheit der Auswahl	5,86	1,558	6,16	1,015	5,26	1,176	5,74	1,759
	Vertrauenswürdigkeit	5,48	1,834	5,89	1,197	5,17	0,984	5,11	1,779
E-Mail	Einfachheit der Auswahl	5,75	1,41	5	1,7	4,83	1,337	5,22	1,517
	Vertrauenswürdigkeit	5,65	1,268	5,05	1,471	4,59	1,469	4,44	1,423
Musik	Einfachheit der Auswahl	6,75	0,716	6,05	1,471	6,09	1,203	6,44	1,149
	Vertrauenswürdigkeit	5,55	1,572	5,42	1,071	5,35	1,027	5,44	1,294
Fitness	Einfachheit der Auswahl	5,72	1,32	4,89	1,451	4,22	1,594	4,38	1,088
	Vertrauenswürdigkeit	5,29	1,829	5,39	1,335	4,48	1,275	3,63	1,586
Spiele	Einfachheit der Auswahl	5,55	1,395	5,26	1,661	4,61	1,234	5	1,414
	Vertrauenswürdigkeit	5,65	1,461	5,21	1,475	4,78	0,998	4,69	2,12
Nachrichten	Einfachheit der Auswahl	5,71	1,521	6	0,745	5,26	1,176	5,44	1,58
	Vertrauenswürdigkeit	5,62	1,284	5,84	0,898	5,09	0,996	4,89	1,605

Anmerkung. Einfachheit der Auswahl und Vertrauenswürdigkeit verglichen zwischen den Gruppen: höchster Mittelwert (grün) und niedrigster Mittelwert (rot).

Tabelle 116 *Kruskal-Wallis-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikation zwischen den Gruppen*

Ränge			
Aussage	Gruppe	H	Mittlerer Rang
Messenger [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	42,17
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	45,34
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	34,85
	D: Keine Datenschutzskala	19	44,97
	Gesamtsumme	82	
Messenger [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	40,88
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	49,05
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	44,07
	D: Keine Datenschutzskala	19	31,53
	Gesamtsumme	82	
Videokonferenz [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	19	42,89
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	34,92
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	40,43
	D: Keine Datenschutzskala	18	41,75
	Gesamtsumme	79	
Videokonferenz [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	47,45
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	45,58
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	42,20
	D: Keine Datenschutzskala	19	30,00
	Gesamtsumme	82	

Fortsetzung Tabelle 116

Aussage	Gruppe	H	Mittlerer Rang
Wetter [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	44,90
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	48,24
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	30,72
	D: Keine Datenschutzskala	19	44,05
	Gesamtsumme	82	
Wetter [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	44,62
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	48,32
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	34,11
	D: Keine Datenschutzskala	18	37,86
	Gesamtsumme	81	
E-Mail [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	50,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	38,21
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	33,67
	D: Keine Datenschutzskala	18	41,08
	Gesamtsumme	80	
E-Mail [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	51,18
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	41,76
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	34,80
	D: Keine Datenschutzskala	18	32,08
	Gesamtsumme	79	

Fortsetzung Tabelle 116

Aussage	Gruppe	H	Mittlerer Rang
Musik [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	47,90
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	37,61
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	34,78
	D: Keine Datenschutzskala	18	42,64
	Gesamtsumme	80	
Musik [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	44,45
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	39,29
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	38,07
	D: Keine Datenschutzskala	18	40,50
	Gesamtsumme	80	
Fitness [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	52,11
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	39,17
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	30,57
	D: Keine Datenschutzskala	16	31,50
	Gesamtsumme	75	
Fitness [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	45,44
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	46,28
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	34,15
	D: Keine Datenschutzskala	16	24,00
	Gesamtsumme	74	

Fortsetzung Tabelle 116

Aussage	Gruppe	H	Mittlerer Rang
Spiele [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	48,10
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	43,97
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	31,13
	D: Keine Datenschutzskala	17	38,03
	Gesamtsumme	79	
Spiele [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	48,38
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	40,79
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	33,30
	D: Keine Datenschutzskala	16	35,78
	Gesamtsumme	78	
Nachrichten/Neuigkeiten [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	45,64
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	46,03
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	33,20
	D: Keine Datenschutzskala	18	40,25
	Gesamtsumme	81	
Nachrichten [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	45,21
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	49,61
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	34,96
	D: Keine Datenschutzskala	18	34,72
	Gesamtsumme	81	

Fortsetzung Tabelle 116

Teststatistiken[a,b]			
Aussage	Chi-Quadrat	df	Asymp. Sig.
Messenger [Einfachheit der Auswahl.]	3,227	3	0,358
Messenger [Vertrauenswürdigkeit.]	5,698	3	0,127
Videokonferenz [Einfachheit der Auswahl.]	1,521	3	0,677
Videokonferenz [Vertrauenswürdigkeit.]	6,73	3	0,081
Wetter [Einfachheit der Auswahl.]	7,488	3	0,058
Wetter [Vertrauenswürdigkeit.]	4,919	3	0,178
E-Mail [Einfachheit der Auswahl.]	5,799	3	0,122
E-Mail [Vertrauenswürdigkeit.]	8,488	3	0,037
Musik [Einfachheit der Auswahl.]	5,613	3	0,132
Musik [Vertrauenswürdigkeit.]	0,935	3	0,817
Fitness [Einfachheit der Auswahl.]	12,133	3	0,007
Fitness [Vertrauenswürdigkeit.]	12,563	3	0,006
Spiele [Einfachheit der Auswahl.]	6,973	3	0,073
Spiele [Vertrauenswürdigkeit.]	5,522	3	0,137
Nachrichten/Neuigkeiten [Einfachheit der Auswahl.]	4,627	3	0,201
Nachrichten [Vertrauenswürdigkeit.]	6,36	3	0,095

a. Kruskal-Wallis-Test

b. Gruppierungsvariable: Gruppe

Tabelle 117 *Mann-Whitney-U-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikation zwischen den Gruppen A und B*

Ränge				
Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,74	414,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	21,34	405,50
	Gesamtsumme	40		
Messenger [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	18,69	392,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	22,50	427,50
	Gesamtsumme	40		
Videokonferenz [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	19	21,42	407,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	17,58	334,00
	Gesamtsumme	38		
Videokonferenz [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	21,07	442,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	19,87	377,50
	Gesamtsumme	40		
Wetter [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,67	413,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	21,42	407,00
	Gesamtsumme	40		

Fortsetzung Tabelle 117

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Wetter [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,83	416,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	21,24	403,50
	Gesamtsumme	40		
E-Mail [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	22,48	449,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	17,39	330,50
	Gesamtsumme	39		
E-Mail [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	22,23	444,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	17,66	335,50
	Gesamtsumme	39		
Musik [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	22,30	446,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	17,58	334,00
	Gesamtsumme	39		
Musik [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	21,25	425,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	18,68	355,00
	Gesamtsumme	39		
Fitness [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	21,58	388,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	15,42	277,50
	Gesamtsumme	36		

Fortsetzung Tabelle 117

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Fitness [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	18,21	309,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	17,81	320,50
	Gesamtsumme	35		
Spiele [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	20,83	416,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	19,13	363,50
	Gesamtsumme	39		
Spiele [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	21,80	436,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	18,11	344,00
	Gesamtsumme	39		
Nachrichten/Neuigkeiten [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	20,69	434,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	20,29	385,50
	Gesamtsumme	40		
Nachrichten [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,69	413,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	21,39	406,50
	Gesamtsumme	40		

Fortsetzung Tabelle 117

Teststatistiken[a,b]					
Aussage	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)	Exakte Sig. [2*(1-seitige Sig.)]
Messenger [Einfachheit der Auswahl.]	183,5	414,5	-0,486	0,627	,668b
Messenger [Vertrauenswürdigkeit.]	161,5	392,5	-1,046	0,296	,307b
Videokonferenz [Einfachheit der Auswahl.]	144	334	-1,133	0,257	,297b
Videokonferenz [Vertrauenswürdigkeit.]	187,5	377,5	-0,339	0,735	,748b
Wetter [Einfachheit der Auswahl.]	182	413	-0,506	0,613	,649b
Wetter [Vertrauenswürdigkeit.]	185,5	416,5	-0,399	0,69	,708b
E-Mail [Einfachheit der Auswahl.]	140,5	330,5	-1,429	0,153	,166b
E-Mail [Vertrauenswürdigkeit.]	145,5	335,5	-1,285	0,199	,214b
Musik [Einfachheit der Auswahl.]	144	334	-1,686	0,092	,204b
Musik [Vertrauenswürdigkeit.]	165	355	-0,722	0,47	,496b
Fitness [Einfachheit der Auswahl.]	106,5	277,5	-1,797	0,072	,079b
Fitness [Vertrauenswürdigkeit.]	149,5	320,5	-0,119	0,905	,909b
Spiele [Einfachheit der Auswahl.]	173,5	363,5	-0,478	0,632	,647b
Spiele [Vertrauenswürdigkeit.]	154	344	-1,04	0,299	,322b
Nachrichten/Neuigkeiten [Einfachheit der Auswahl.]	195,5	385,5	-0,114	0,909	,915b
Nachrichten [Vertrauenswürdigkeit.]	182,5	413,5	-0,478	0,633	,649b

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 118 *Mann-Whitney-U-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikation zwischen den Gruppen A und C*

Ränge				
Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	24,57	516,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,61	474,00
	Gesamtsumme	44		
Messenger [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	21,64	454,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	23,28	535,50
	Gesamtsumme	44		
Videokonferenz [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	19	22,24	422,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,89	480,50
	Gesamtsumme	42		
Videokonferenz [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	24,19	508,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,96	482,00
	Gesamtsumme	44		
Wetter [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	26,67	560,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,70	430,00
	Gesamtsumme	44		
Wetter [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	25,43	534,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,83	456,00
	Gesamtsumme	44		
E-Mail [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	27,03	540,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	17,63	405,50
	Gesamtsumme	43		

Fortsetzung Tabelle 118

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
E-Mail [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	26,13	522,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	17,30	380,50
	Gesamtsumme	42		
Musik [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	25,90	518,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,61	428,00
	Gesamtsumme	43		
Musik [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	23,90	478,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,35	468,00
	Gesamtsumme	43		
Fitness [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	27,25	490,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	16,11	370,50
	Gesamtsumme	41		
Fitness [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	24,09	409,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	17,85	410,50
	Gesamtsumme	40		
Spiele [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	27,15	543,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	17,52	403,00
	Gesamtsumme	43		
Spiele [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	27,13	542,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	17,54	403,50
	Gesamtsumme	43		

Fortsetzung Tabelle 118

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Nachrichten/Neuigkeiten [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	25,67	539,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,61	451,00
	Gesamtsumme	44		
Nachrichten [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	25,12	527,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,11	462,50
	Gesamtsumme	44		

Fortsetzung Tabelle 118

Teststatistiken[a,b]

Aussage	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)	Exakte Sig. [2*(1-seitige Sig.)]
Messenger [Einfachheit der Auswahl.]	198	474	-1,092	0,275	
Messenger [Vertrauenswürdigkeit.]	223,5	454,5	-0,431	0,667	
Videokonferenz [Einfachheit der Auswahl.]	204,5	480,5	-0,379	0,705	
Videokonferenz [Vertrauenswürdigkeit.]	206	482	-0,867	0,386	
Wetter [Einfachheit der Auswahl.]	154	430	-2,133	0,033	
Wetter [Vertrauenswürdigkeit.]	180	456	-1,494	0,135	
E-Mail [Einfachheit der Auswahl.]	129,5	405,5	-2,525	0,012	
E-Mail [Vertrauenswürdigkeit.]	127,5	380,5	-2,386	0,017	
Musik [Einfachheit der Auswahl.]	152	428	-2,289	0,022	
Musik [Vertrauenswürdigkeit.]	192	468	-0,954	0,34	
Fitness [Einfachheit der Auswahl.]	94,5	370,5	-3,007	0,003	
Fitness [Vertrauenswürdigkeit.]	134,5	410,5	-1,698	0,09	,095b
Spiele [Einfachheit der Auswahl.]	127	403	-2,582	0,01	
Spiele [Vertrauenswürdigkeit.]	127,5	403,5	-2,574	0,01	
Nachrichten/Neuigkeiten [Einfachheit der Auswahl.]	175	451	-1,614	0,106	
Nachrichten [Vertrauenswürdigkeit.]	186,5	462,5	-1,337	0,181	

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 119 *Mann-Whitney-U-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikation zwischen den Gruppen A und D*

Ränge

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,86	417,00
	D: Keine Datenschutzskala	19	21,21	403,00
	Gesamtsumme	40		
Messenger [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	22,55	473,50
	D: Keine Datenschutzskala	19	18,24	346,50
	Gesamtsumme	40		
Videokonferenz [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	19	19,24	365,50
	D: Keine Datenschutzskala	18	18,75	337,50
	Gesamtsumme	37		
Videokonferenz [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	24,19	508,00
	D: Keine Datenschutzskala	19	16,42	312,00
	Gesamtsumme	40		
Wetter [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	20,57	432,00
	D: Keine Datenschutzskala	19	20,42	388,00
	Gesamtsumme	40		
Wetter [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	21,36	448,50
	D: Keine Datenschutzskala	18	18,42	331,50
	Gesamtsumme	39		
E-Mail [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	21,50	430,00
	D: Keine Datenschutzskala	18	17,28	311,00
	Gesamtsumme	38		

Fortsetzung Tabelle 119

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
E-Mail [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	23,83	476,50
	D: Keine Datenschutzskala	18	14,69	264,50
	Gesamtsumme	38		
Musik [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	20,70	414,00
	D: Keine Datenschutzskala	18	18,17	327,00
	Gesamtsumme	38		
Musik [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	20,30	406,00
	D: Keine Datenschutzskala	18	18,61	335,00
	Gesamtsumme	38		
Fitness [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	18	22,28	401,00
	D: Keine Datenschutzskala	16	12,13	194,00
	Gesamtsumme	34		
Fitness [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	21,15	359,50
	D: Keine Datenschutzskala	16	12,59	201,50
	Gesamtsumme	33		
Spiele [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	21,13	422,50
	D: Keine Datenschutzskala	17	16,50	280,50
	Gesamtsumme	37		
Spiele [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	20,45	409,00
	D: Keine Datenschutzskala	16	16,06	257,00
	Gesamtsumme	36		

Fortsetzung Tabelle 119

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Nachrichten/Neuigkeiten [Einfachheit der Auswahl.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	21,29	447,00
	D: Keine Datenschutzskala	18	18,50	333,00
	Gesamtsumme	39		
Nachrichten [Vertrauenswürdigkeit.]	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	22,40	470,50
	D: Keine Datenschutzskala	18	17,19	309,50
	Gesamtsumme	39		

Teststatistiken[a,b]

Aussage	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)	Exakte Sig. [2*(1-seitige Sig.)]
Messenger [Einfachheit der Auswahl.]	186	417	-0,406	0,685	,728b
Messenger [Vertrauenswürdigkeit.]	156,5	346,5	-1,18	0,238	,247b
Videokonferenz [Einfachheit der Auswahl.]	166,5	337,5	-0,148	0,882	,893b
Videokonferenz [Vertrauenswürdigkeit.]	122	312	-2,145	0,032	,036b
Wetter [Einfachheit der Auswahl.]	198	388	-0,043	0,966	,979b
Wetter [Vertrauenswürdigkeit.]	160,5	331,5	-0,829	0,407	,426b
E-Mail [Einfachheit der Auswahl.]	140	311	-1,208	0,227	,251b
E-Mail [Vertrauenswürdigkeit.]	93,5	264,5	-2,59	0,01	,010b
Musik [Einfachheit der Auswahl.]	156	327	-0,987	0,324	,496b
Musik [Vertrauenswürdigkeit.]	164	335	-0,483	0,629	,654b
Fitness [Einfachheit der Auswahl.]	58	194	-3,034	0,002	,002b
Fitness [Vertrauenswürdigkeit.]	65,5	201,5	-2,574	0,01	,010b
Spiele [Einfachheit der Auswahl.]	127,5	280,5	-1,331	0,183	,198b
Spiele [Vertrauenswürdigkeit.]	121	257	-1,28	0,201	,223b
Nachrichten/Neuigkeiten [Einfachheit der Auswahl.]	162	333	-0,797	0,426	,460b
Nachrichten [Vertrauenswürdigkeit.]	138,5	309,5	-1,457	0,145	,156b

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 120 *Mann-Whitney-U-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikation zwischen den Gruppen B und C*

Ränge				
Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	24,37	463,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,13	440,00
	Gesamtsumme	42		
Messenger [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	23,16	440,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,13	463,00
	Gesamtsumme	42		
Videokonferenz [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	19,87	377,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,85	525,50
	Gesamtsumme	42		
Videokonferenz [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	22,61	429,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,59	473,50
	Gesamtsumme	42		
Wetter [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	26,42	502,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	17,43	401,00
	Gesamtsumme	42		
Wetter [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	25,87	491,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	17,89	411,50
	Gesamtsumme	42		
E-Mail [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	22,42	426,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,74	477,00
	Gesamtsumme	42		

Fortsetzung Tabelle 120

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
E-Mail [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	22,92	435,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	19,34	425,50
	Gesamtsumme	41		
Musik [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	22,11	420,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,00	483,00
	Gesamtsumme	42		
Musik [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	21,84	415,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,22	488,00
	Gesamtsumme	42		
Fitness [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	23,64	425,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,93	435,50
	Gesamtsumme	41		
Fitness [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	25,17	453,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	17,74	408,00
	Gesamtsumme	41		
Spiele [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	25,11	477,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,52	426,00
	Gesamtsumme	42		
Spiele [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	23,63	449,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,74	454,00
	Gesamtsumme	42		

Fortsetzung Tabelle 120

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Nachrichten/Neuigkeiten [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	25,61	486,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,11	416,50
	Gesamtsumme	42		
Nachrichten [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	26,26	499,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	17,57	404,00
	Gesamtsumme	42		

Teststatistiken[a,b]

Aussage	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)
Messenger [Einfachheit der Auswahl.]	164	440	-1,481	0,139
Messenger [Vertrauenswürdigkeit.]	187	463	-0,815	0,415
Videokonferenz [Einfachheit der Auswahl.]	187,5	377,5	-0,846	0,398
Videokonferenz [Vertrauenswürdigkeit.]	197,5	473,5	-0,557	0,578
Wetter [Einfachheit der Auswahl.]	125	401	-2,446	0,014
Wetter [Vertrauenswürdigkeit.]	135,5	411,5	-2,179	0,029
E-Mail [Einfachheit der Auswahl.]	201	477	-0,456	0,649
E-Mail [Vertrauenswürdigkeit.]	172,5	425,5	-0,978	0,328
Musik [Einfachheit der Auswahl.]	207	483	-0,323	0,746
Musik [Vertrauenswürdigkeit.]	212	488	-0,172	0,863
Fitness [Einfachheit der Auswahl.]	159,5	435,5	-1,27	0,204
Fitness [Vertrauenswürdigkeit.]	132	408	-2,013	0,044
Spiele [Einfachheit der Auswahl.]	150	426	-1,784	0,074
Spiele [Vertrauenswürdigkeit.]	178	454	-1,063	0,288
Nachrichten/Neuigkeiten [Einfachheit der Auswahl.]	140,5	416,5	-2,068	0,039
Nachrichten [Vertrauenswürdigkeit.]	128	404	-2,392	0,017

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 121 *Mann-Whitney-U-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikation zwischen den Gruppen B und D*

Ränge				
Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	19,63	373,00
	D: Keine Datenschutzskala	19	19,37	368,00
	Gesamtsumme	38		
Messenger [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	23,39	444,50
	D: Keine Datenschutzskala	19	15,61	296,50
	Gesamtsumme	38		
Videokonferenz [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	17,47	332,00
	D: Keine Datenschutzskala	18	20,61	371,00
	Gesamtsumme	37		
Videokonferenz [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	23,11	439,00
	D: Keine Datenschutzskala	19	15,89	302,00
	Gesamtsumme	38		
Wetter [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	20,39	387,50
	D: Keine Datenschutzskala	19	18,61	353,50
	Gesamtsumme	38		
Wetter [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	21,21	403,00
	D: Keine Datenschutzskala	18	16,67	300,00
	Gesamtsumme	37		
E-Mail [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	18,39	349,50
	D: Keine Datenschutzskala	18	19,64	353,50
	Gesamtsumme	37		

Fortsetzung Tabelle 121

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
E-Mail [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	21,18	402,50
	D: Keine Datenschutzskala	18	16,69	300,50
	Gesamtsumme	37		
Musik [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	17,92	340,50
	D: Keine Datenschutzskala	18	20,14	362,50
	Gesamtsumme	37		
Musik [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	18,76	356,50
	D: Keine Datenschutzskala	18	19,25	346,50
	Gesamtsumme	37		
Fitness [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,11	344,00
	D: Keine Datenschutzskala	16	15,69	251,00
	Gesamtsumme	34		
Fitness [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	22,31	401,50
	D: Keine Datenschutzskala	16	12,09	193,50
	Gesamtsumme	34		
Spiele [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	19,74	375,00
	D: Keine Datenschutzskala	17	17,12	291,00
	Gesamtsumme	36		
Spiele [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	19,05	362,00
	D: Keine Datenschutzskala	16	16,75	268,00
	Gesamtsumme	35		

Fortsetzung Tabelle 121

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Nachrichten/Neuigkeiten [Einfachheit der Auswahl.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	20,13	382,50
	D: Keine Datenschutzskala	18	17,81	320,50
	Gesamtsumme	37		
Nachrichten [Vertrauenswürdigkeit.]	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	19	21,95	417,00
	D: Keine Datenschutzskala	18	15,89	286,00
	Gesamtsumme	37		

Teststatistiken[a,b]

Aussage	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)	Exakte Sig. [2*(1-seitige Sig.)]
Messenger [Einfachheit der Auswahl.]	178	368	-0,083	0,934	,954b
Messenger [Vertrauenswürdigkeit.]	106,5	296,5	-2,193	0,028	,030b
Videokonferenz [Einfachheit der Auswahl.]	142	332	-0,936	0,349	,391b
Videokonferenz [Vertrauenswürdigkeit.]	112	302	-2,059	0,04	,046b
Wetter [Einfachheit der Auswahl.]	163,5	353,5	-0,536	0,592	,624b
Wetter [Vertrauenswürdigkeit.]	129	300	-1,32	0,187	,210b
E-Mail [Einfachheit der Auswahl.]	159,5	349,5	-0,356	0,722	,730b
E-Mail [Vertrauenswürdigkeit.]	129,5	300,5	-1,286	0,198	,210b
Musik [Einfachheit der Auswahl.]	150,5	340,5	-0,75	0,453	,538b
Musik [Vertrauenswürdigkeit.]	166,5	356,5	-0,141	0,888	,893b
Fitness [Einfachheit der Auswahl.]	115	251	-1,026	0,305	,330b
Fitness [Vertrauenswürdigkeit.]	57,5	193,5	-3,029	0,002	,002b
Spiele [Einfachheit der Auswahl.]	138	291	-0,763	0,445	,471b
Spiele [Vertrauenswürdigkeit.]	132	268	-0,68	0,496	,523b
Nachrichten/Neuigkeiten [Einfachheit der Auswahl.]	149,5	320,5	-0,697	0,486	,518b
Nachrichten [Vertrauenswürdigkeit.]	115	286	-1,755	0,079	,092b

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 122 *Mann-Whitney-U-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikation zwischen den Gruppen C und D*

Ränge

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger [Einfachheit der Auswahl.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,11	439,50
	D: Keine Datenschutzskala	19	24,39	463,50
	Gesamtsumme	42		
Messenger [Vertrauenswürdigkeit.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	24,65	567,00
	D: Keine Datenschutzskala	19	17,68	336,00
	Gesamtsumme	42		
Videokonferenz [Einfachheit der Auswahl.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,70	476,00
	D: Keine Datenschutzskala	18	21,39	385,00
	Gesamtsumme	41		
Videokonferenz [Vertrauenswürdigkeit.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	24,65	567,00
	D: Keine Datenschutzskala	19	17,68	336,00
	Gesamtsumme	42		
Wetter [Einfachheit der Auswahl.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,59	427,50
	D: Keine Datenschutzskala	19	25,03	475,50
	Gesamtsumme	42		
Wetter [Vertrauenswürdigkeit.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,39	469,00
	D: Keine Datenschutzskala	18	21,78	392,00
	Gesamtsumme	41		
E-Mail [Einfachheit der Auswahl.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,30	444,00
	D: Keine Datenschutzskala	18	23,17	417,00
	Gesamtsumme	41		
E-Mail [Vertrauenswürdigkeit.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	21,16	465,50
	D: Keine Datenschutzskala	18	19,69	354,50
	Gesamtsumme	40		
Musik [Einfachheit der Auswahl.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,17	441,00
	D: Keine Datenschutzskala	18	23,33	420,00
	Gesamtsumme	41		
Musik [Vertrauenswürdigkeit.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,50	471,50
	D: Keine Datenschutzskala	18	21,64	389,50
	Gesamtsumme	41		

Fortsetzung Tabelle 122

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Fitness [Einfachheit der Auswahl.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,52	449,00
	D: Keine Datenschutzskala	16	20,69	331,00
	Gesamtsumme	39		
Fitness [Vertrauenswürdigkeit.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,57	519,00
	D: Keine Datenschutzskala	16	16,31	261,00
	Gesamtsumme	39		
Spiele [Einfachheit der Auswahl.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,09	439,00
	D: Keine Datenschutzskala	17	22,41	381,00
	Gesamtsumme	40		
Spiele [Vertrauenswürdigkeit.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,02	460,50
	D: Keine Datenschutzskala	16	19,97	319,50
	Gesamtsumme	39		
Nachrichten/Neuigkeiten [Einfachheit der Auswahl.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,48	448,00
	D: Keine Datenschutzskala	18	22,94	413,00
	Gesamtsumme	41		
Nachrichten [Vertrauenswürdigkeit.]	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,28	489,50
	D: Keine Datenschutzskala	18	20,64	371,50
	Gesamtsumme	41		

Fortsetzung Tabelle 122

Teststatistiken[a,b]

Aussage	Mann-Whitney-U-Test	Wilcoxon-W	z	Asymp. Sig. (2-seitig)	Exakte Sig. [2*(1-seitige Sig.)]
Messenger [Einfachheit der Auswahl.]	163,5	439,5	-1,493	0,135	
Messenger [Vertrauenswürdigkeit.]	146	336	-1,862	0,063	
Videokonferenz [Einfachheit der Auswahl.]	200	476	-0,196	0,844	
Videokonferenz [Vertrauenswürdigkeit.]	146	336	-1,89	0,059	
Wetter [Einfachheit der Auswahl.]	151,5	427,5	-1,744	0,081	
Wetter [Vertrauenswürdigkeit.]	193	469	-0,379	0,705	
E-Mail [Einfachheit der Auswahl.]	168	444	-1,059	0,29	
E-Mail [Vertrauenswürdigkeit.]	183,5	354,5	-0,403	0,687	,697b
Musik [Einfachheit der Auswahl.]	165	441	-1,261	0,207	
Musik [Vertrauenswürdigkeit.]	195,5	471,5	-0,313	0,755	
Fitness [Einfachheit der Auswahl.]	173	449	-0,321	0,748	,767b
Fitness [Vertrauenswürdigkeit.]	125	261	-1,72	0,085	,095b
Spiele [Einfachheit der Auswahl.]	163	439	-0,93	0,352	,386b
Spiele [Vertrauenswürdigkeit.]	183,5	319,5	-0,015	0,988	,989b
Nachrichten/Neuigkeiten [Einfachheit der Auswahl.]	172	448	-0,956	0,339	
Nachrichten [Vertrauenswürdigkeit.]	200,5	371,5	-0,176	0,861	

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 123 *T-Test Vergleich der Vertrauenswürdigkeit der Applikation Messenger zwischen den Gruppen*

Test bei unabhängigen Stichproben

Gruppe A und B Messenger [Vertrauenswürdigkeit]	Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
								95 % Konfidenzintervall der Differenz	
	F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Varianzgleichheit angenommen	1,765	,192	-1,129	38	,266	-,571	,506	-1,596	,453
Varianzgleichheit nicht angenommen			-1,141	37,560	,261	-,571	,501	-1,586	,443

Test bei unabhängigen Stichproben

Gruppe A und C Messenger [Vertrauenswürdigkeit]	Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
								95 % Konfidenzintervall der Differenz	
	F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Varianzgleichheit angenommen	4,655	,037	-,494	42	,624	-,224	,452	-1,137	,689
Varianzgleichheit nicht angenommen			-,487	35,535	,630	-,224	,460	-1,156	,709

Test bei unabhängigen Stichproben

Gruppe A und D Messenger [Vertrauenswürdigkeit]	Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
								95 % Konfidenzintervall der Differenz	
	F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Varianzgleichheit angenommen	,003	,957	1,215	38	,232	,692	,569	-,461	1,844
Varianzgleichheit nicht angenommen			1,212	37,056	,233	,692	,571	-,465	1,848

Fortsetzung Tabelle 123

Test bei unabhängigen Stichproben

Gruppe B und C Messenger [Vertrauenswürdigkeit]	Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
								95 % Konfidenzintervall der Differenz	
	F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Varianzgleichheit angenommen	,490	,488	,853	40	,399	,348	,408	-,476	1,172
Varianzgleichheit nicht angenommen			,841	35,997	,406	,348	,413	-,491	1,186

, Z. 390-405

Test bei unabhängigen Stichproben

Gruppe B und D Messenger [Vertrauenswürdigkeit]	Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
								95 % Konfidenzintervall der Differenz	
	F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Varianzgleichheit angenommen	1,496	,229	2,364	36	,024	1,263	,534	,179	2,347
Varianzgleichheit nicht angenommen			2,364	33,672	,024	1,263	,534	,177	2,350

Test bei unabhängigen Stichproben

Gruppe C und D Messenger [Vertrauenswürdigkeit]	Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
								95 % Konfidenzintervall der Differenz	
	F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Varianzgleichheit angenommen	3,827	,057	1,917	40	,062	,915	,478	-,050	1,880
Varianzgleichheit nicht angenommen			1,845	30,213	,075	,915	,496	-,097	1,928

Tabelle 124 *T-Test Vergleich der Einfachheit der Auswahl und der Vertrauenswürdigkeit der Applikationen E-Mail, Fitness und Spiele, zwischen den Gruppen B und D*

Test bei unabhängigen Stichproben										
		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
E-Mail [Einfachheit der Auswahl]	Varianzgleichheit angenommen	,241	,626	-,419	35	,678	-,222	,531	-1,300	,855
	Varianzgleichheit nicht angenommen			-,420	34,882	,677	-,222	,529	-1,296	,852
Fitness [Einfachheit der Auswahl]	Varianzgleichheit angenommen	2,121	,155	1,156	32	,256	,514	,444	-,391	1,419
	Varianzgleichheit nicht angenommen			1,176	31,173	,248	,514	,437	-,377	1,405
Spiele [Vertrauenswürdigkeit]	Varianzgleichheit angenommen	3,315	,078	,858	33	,397	,523	,610	-,718	1,764
	Varianzgleichheit nicht angenommen			,832	26,103	,413	,523	,629	-,769	1,815

Tabelle 125 *Häufigkeiten der Einschätzung der Vertrauenswürdigkeit durch die erste Methode (gestauchte Reskalierung)*

Häufigkeiten								
Einschätzung der Vertrauenswürdigkeit	Szenarien							
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
als vertrauenswürdiger eingeschätzt	25	18	15	21	19	36	30	32
als weniger vertrauenswürdig eingeschätzt	40	27	45	34	35	9	19	20
Vertrauenswürdigkeit wird adäquat eingeschätzt	17	33	21	24	26	29	29	29

Tabelle 126 *Häufigkeiten der Einschätzung der Vertrauenswürdigkeit durch die zweite Methode (prozentuale Reskalierung)*

Häufigkeiten								
Einschätzung der Vertrauenswürdigkeit	Szenarien							
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
als vertrauenwürdiger eingeschätzt	29	47	25	32	42	47	42	43
als weniger vertrauenswürdig eingeschätzt	41	29	45	34	35	12	20	20
Vertrauenswürdigkeit wird adequat eingeschätzt	12	2	11	13	3	15	16	18

Tabelle 127 *Häufigkeiten der Einschätzung der Vertrauenswürdigkeit durch die dritte Methode (dividierte Reskalierung)*

Häufigkeiten								
Einschätzung der Vertrauenswürdigkeit	Szenarien							
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
als vertrauenwürdiger eingeschätzt	39	50	30	43	44	58	52	45
als weniger vertrauenswürdig eingeschätzt	41	29	45	34	35	12	20	20
Vertrauenswürdigkeit wird adequat eingeschätzt	2	3	7	5	3	12	10	17

Tabelle 128 *Häufigkeit der Differenzen unter Verwendung der ersten Methode (gestauchte Reskalierung)*

Häufigkeiten nach Gruppen										
		Skala								
Szenario	Gruppe	-4	-3	-2	-1	0	1	2	3	4
Vertrauens-würdigkeit	A	0	0	23,8 (5)	14,3(3)	33,3(7)	14,3(3)	14,3(3)	0	0
	B	0	16,7(3)	22,2(4)	16,7(3)	27,8(5)	16,7(3)	0	0	0
Messenger	C	0	13,0(3)	30,4(7)	26,1(6)	8,7(2)	17,4(4)	4,3(1)	0	0
	D	5,3(1)	0	21,1(4)	5,3(1)	15,8(3)	21,1(4)	26,3(5)	5,3(1)	0
Vertrauens-würdigkeit	A	0	0	0	33,3(7)	42,9(9)	4,8(1)	4,8(1)	4,8(1)	0
	B	0	0	5,6(1)	50,0(9)	27,8(5)		11,1(2)		0
	C	0	0	4,3(1)	26,1(6)	47,8(11)	4,3(1)	8,7(2)	8,7(2)	0
Videokonferenz	D	0	5,3(1)	0	10,5(2)	36,8(7)	10,5(2)	10,5(2)	21,1(4)	0
Vertrauens-würdigkeit	A	0	0	0	38,1(8)	33,3(7)	28,6(6)	0	0	0
	B	0	11,1(2)	16,7(3)	38,9(7)	27,8(5)	5,6(1)	0	0	0
	C	0	17,4(4)	17,4(4)	13,0(3)	34,8(8)	8,7(2)	4,3(1)	4,3(1)	0
Wetter	D	5,3(1)	21,1(4)	15,8(3)	31,6(6)	5,3(1)	5,3(1)	10,5(2)	0	0
Vertrauens-würdigkeit	A	0	0	19,0(4)	19,0(4)	33,3(7)	19,0(4)	0	4,8(1)	0
	B	5,6(1)	0	22,2(4)	16,7(3)	44,4(8)	5,6(1)	5,6(1)	0	0
	C	4,3(1)	0	17,4(4)	17,4(4)	21,7(5)	21,7(5)	8,7(2)	4,3(1)	0
E-Mail	D	0	0	15,8(3)	31,6(6)	21,1(4)	15,8(3)	10,5(2)	0	0
Vertrauens-würdigkeit	A	0	0	0	47,6(10)	28,6(6)	4,8(1)	9,5(2)	4,8(1)	0
	B	0	0	0	16,7(3)	44,4(8)	22,2(4)	16,7(3)	0	0
	C	0	0	0	52,2(12)	34,8(8)	0	13,0(3)	0	0
Musik	D	0	0	0	47,4(9)	21,1(4)	21,1(4)	0	5,3(1)	0
Vertrauens-würdigkeit	A	0	0	0	4,8(1)	42,9(9)	9,5(2)	9,5(2)	4,8(1)	9,5(2)
	B	0	0	0	5,6(1)	44,4(8)	16,7(3)	22,2(4)	5,6(1)	0
	C	0	0	0	8,7(2)	34,8(8)	26,1(6)	21,7(5)	8,7(2)	0
Fitness	D	0	15,8(3)	5,3(1)	5,3(1)	15,8(3)	21,1(4)	10,5(2)	5,3(1)	5,3(1)
Vertrauens-würdigkeit	A	4,8(1)	0	4,8(1)	4,8(1)	61,9(13)	9,5(2)	4,8(1)	0	4,8(1)
	B	0	0	5,6(1)	5,6(1)	38,9(7)	27,8(5)	22,2(4)	0	0
	C	0	4,3(1)	0	21,7(5)	21,7(5)	26,1(6)	17,4(4)	4,3(1)	4,3(1)
Spiele	D	0	10,5(2)	26,3(5)	5,3(1)	15,8(3)	0	26,3(5)	0	0
Vertrauens-würdigkeit	A	0	0	4,8(1)	0	52,4(11)	14,3(3)	28,6(6)	0	0
	B	5,6(1)	0	11,1(2)	0	44,4(8)	33,3(6)	5,6(1)	0	0
	C	4,3(1)	0	8,7(2)	17,4(4)	30,4(7)	30,4(7)	8,7(2)	0	0
Nachrichten	D	5,3(1)	21,1(4)	10,5(2)	10,5(2)	10,5(2)	26,3(5)	5,3(1)	5,3(1)	0

Anmerkung. Häufigkeiten der Differenzen unter Verwendung der ersten Methode zur Reskalierung verglichen zwischen den Gruppen farblich in aufsteigend sortierter Rangfolge: rot, orange, gelb, grün. Angaben in Prozent mit absoluten Häufigkeiten in Klammern.

Fortsetzung Tabelle 128

Häufigkeiten Gesamt									
	Skala								
Szenario	-4	-3	-2	-1	0	1	2	3	4
Vertrauens-würdigkeit Messenger	1,2(1)	7,4(6)	24,7(20)	16(13)	21(17)	17,3(14)	11,1(9)	1,2(1)	0
Vertrauens-würdigkeit Videokonferenz	0	1,2(1)	2,5(2)	29,6(24)	39,5(32)	4,9(4)	8,6(7)	8,6(7)	0
Vertrauens-Würdigkeit Wetter	1,2(1)	12,3(10)	12,3(10)	29,6(24)	25,9(21)	12,3(10)	3,7(3)	1,2(1)	0
Vertrauens-Würdigkeit E-Mail	2,5(2)	0	18,5(15)	21,0(17)	29,6(24)	16,0(13)	6,2(5)	1,2(1)	1,2(1)
Vertrauens-Würdigkeit Musik	0	0	0	42,0(34)	32,1(26)	11,1(9)	9,9(8)	2,5(2)	0
Vertrauens-Würdigkeit Fitness	0	3,7(3)	1,2(1)	6,2(5)	34,6(28)	18,5(15)	16,0(13)	6,2(5)	3,7(3)
Vertrauens-Würdigkeit Spiele	1,2(1)	3,7(3)	8,6(7)	9,9(8)	34,6(28)	16,0(13)	17,3(14)	1,2(1)	2,5(2)
Vertrauens-würdigkeit Nachrichten	3,7(3)	4,9(4)	8,6(7)	7,4(6)	34,6(28)	25,9(21)	12,3(10)	1,2(1)	0

Anmerkung. Häufigkeiten Gesamt der Differenzen unter Verwendung der ersten Methode zur Reskalierung farblich in aufsteigend sortierter Rangfolge: rot, orange, gelb, grün. Angaben in Prozent mit absoluten Häufigkeiten in Klammern.

Tabelle 129 *Häufigkeit der Differenzen unter Verwendung der zweiten Methode (prozentuale Reskalierung)*

		Häufigkeiten																				
	Gr...	Skala																				
		-83,3	-75	-66,67	-58,3	-50	-41,67	-33,3	-25	-16,67	-8,3	0,0	8,3	16,67	25	33,3	41,67	50	58,3	66,67	75	83,3
Messenger	A	0	0	0	0	4,8 (1)	4,8 (1)	19 (4)	0	9,5 (2)	0	28,6 (6)	4,8(1)	14,3 (3)	0	14,3 (3)	0	0	0	0	0	0
	B	0	11,1 (2)	5,6(1)	0	5,6 (1)	0	16,7 (3)	5,6(1)	11,1 (2)	5,6 (1)	11,1 (2)	0	22,2 (4)	0	5,6 (1)	0	0	0	0	0	0
	C	0	0	8,7(2)	4,3 (1)	13 (3)	4,3 (1)	13 (3)	8,7(2)	17,4 (4)	0	4,3(1)	4,3(1)	17,4 (4)	0	0	0	4,3(1)	0	0	0	0
	D	5,3(1)	0	0	0	10,5 (2)	5,3 (1)	5,3(1)	0	5,3 (1)	0	15,8 (3)	0	21,1 (4)	0	15,8 (3)	0	10,5 (2)	0	5,3 (1)	0	0
Videokonferenz	A	0	0	0	0	0	0	0	14,3 (3)	4,8 (1)	14,3 (3)	4,8 (1)	14,3 (3)	23,8 (5)	4,8 (1)	0	4,8 (1)	0	4,8(1)	0	0	0
	B	0	0	0	0	0	0	5,6 (1)	11,1 (2)	5,6 (1)	33,3 (6)	0	22,2 (4)	5,6 (1)	0	0	11,1 (2)	0	0	0	0	0
	C	0	0	0	0	4,3 (1)	0	0	0	0	30,4 (7)	4,3 (1)	26,1 (6)	13 (3)	0	4,3(1)	4,3 (1)	4,3(1)	8,7 (2)	0	0	0
	D	0	5,3 (1)	0	0	0	0	0	0	0	10,5 (2)	0	36,8 (7)	5,3 (1)	5,3 (1)	0	10,5 (2)	0	10,5 (2)	10,5 (2)	0	0
Wetter	A	0	0	0	0	0	0	0	23,8 (5)	9,5 (2)	4,8 (1)	19 (4)	9,5 (2)	19 (4)	4,8 (1)	9,5 (2)	0	0	0	0	0	0
	B	0	5,6 (1)	0	5,6 (1)	5,6 (1)	5,6 (1)	5,6 (1)	16,7 (3)	16,7 (3)	5,6 (1)	16,7 (3)	5,6 (1)	5,6 (1)	5,6 (1)	0	0	0	0	0	0	0
	C	0	4,3 (1)	4,3 (1)	8,7 (2)	0	13 (3)	4,3 (1)	4,3 (1)	4,3 (1)	4,3 (1)	13 (3)	13 (3)	8,7 (2)	0	8,7 (2)	0	4,3 (1)	0	4,3 (1)	0	0
	D	5,3(1)	10,5 (2)	5,3 (1)	5,3 (1)	10,5 (2)	5,3 (1)	0	15,8 (3)	5,3 (1)	10,5 (2)	5,3 (1)	5,3 (1)	0	0	10,5 (2)	0	0	0	0	0	0

Fortsetzung Tabelle 129

	Gruppe	Skala																			
		-83,3	-75	-66,67	-58,3	-50	-41,67	-33,3	-25	-16,67	-8,3	0,0	8,3	16,67	25	33,3	41,67	50	58,3	66,67	75	83,3
E-Mail	A	0	0	0	0	9,5 (2)	4,8 (1)	4,8 (1)	9,5 (2)	4,8 (1)	4,8 (1)	9,5 (2)	4,8 (1)	23,8 (5)	4,8 (1)	9,5 (2)	4,8 (1)	0	0	0	0	0
	B	5,6 (1)	0	0	0	11,1 (2)	0	16,7 (3)	0	5,6 (1)	5,6 (1)	27,8 (5)	5,6 (1)	11,1 (2)	0	11,1 (2)	0	0	0	0	0	0
	C	4,3 (1)	0	0	0	8,7 (2)	0	8,7 (2)	0	17,4 (4)	0	8,7 (2)	0	21,7 (5)	8,7 (2)	4,3 (1)	0	8,7 (2)	0	0	4,3 (1)	0
	D	0	0	0	0	0	0	15,8 (3)	0	31,6 (6)	0	21,1 (4)	0	15,8 (3)	0	10,5 (2)	0	0	0	0	0	0
Musik	A	0	0	0	0	0	0	0	33,3 (7)	0	14,3 (3)	4,8 (1)	23,8 (5)	0	4,8 (1)	0	9,5 (2)	0	4,8 (1)	0	0	0
	B	0	0	0	0	0	0	0	5,6 (1)	0	11,1 (2)	11,1 (2)	11,1 (2)	22,2 (4)	11,1 (2)	11,1 (2)	0	16,7 (3)	0	0	0	0
	C	0	0	0	0	0	0	4,3 (1)	13 (3)	0	34,8 (8)	0	26,1 (6)	8,7 (2)	0	0	0	13 (3)	0	0	0	0
	D	0	0	0	0	0	0	0	26,3 (5)	0	21,1 (4)	0	21,1 (4)	0	21,1 (4)	0	0	0	0	5,3 (1)	0	0
Fitness	A	0	0	0	0	0	0	0	4,8 (1)	0	0	33,3 (7)	0	9,5 (2)	0	9,5 (2)	0	9,5 (2)	0	4,8 (1)	9,5 (2)	0
	B	0	0	0	0	0	0	0	5,6 (1)	0	0	22,2 (4)	0	22,2 (4)	0	16,7 (3)	0	22,2 (4)	0	5,6 (1)	0	0
	C	0	0	0	0	0	0	4,3 (1)	0	4,3 (1)	4,3 (1)	8,7 (2)	4,3 (1)	21,7 (5)	0	26,1 (6)	0	17,4 (4)	0	8,7 (2)	0	0
	D	0	0	5,3 (1)	10,5 (2)	5,3 (1)	0	0	0	0	15,8 (3)	5,3 (1)	5,3 (1)	10,5 (2)	0	0	10,5 (2)	5,3 (1)	0	5,3 (1)	0	5,3 (1)
Spiele	A	4,8 (1)	0	0	0	0	0	4,8 (1)	4,8 (1)	0	0	38,1 (8)	4,8 (1)	19 (4)	0	9,5 (2)	4,8 (1)	0	0	0	4,8 (1)	0
	B	0	0	0	0	5,6 (1)	0	0	0	5,6 (1)	0	22,2 (4)	0	16,7 (3)	5,6 (1)	22,2 (4)	5,6 (1)	16,7 (3)	0	0	0	0
	C	0	0	4,3 (1)	0	0	0	0	0	17,4 (4)	4,3(1)	4,3 (1)	0	17,4 (4)	0	26,1 (6)	0	17,4 (4)	0	4,3 (1)	4,3 (1)	0
	D	0	5,3 (1)	0	5,3 (1)	21,1 (4)	0	5,3 (1)	5,3 (1)	0	0	15,8 (3)	0	0	0	5,3 (1)	0	21,1 (4)	0	0	0	0

Fortsetzung Tabelle 129

	Gruppe	Skala																			
		-83,3	-75	-66,67	-58,3	-50	-41,67	-33,3	-25	-16,67	-8,3	0,0	8,3	16,67	25	33,3	41,67	50	58,3	66,67	75	83,3
Nachrichten	A	0	0	0	0	0	4,8 (1)	0	0	0	0	38,1 (8)	0	14,3 (3)	0	14,3 (3)	0	28,6 (6)	0	0	0	0
	B	5,6 (1)	0	0	0	0	0	11,1 (2)	0	0	0	22,2 (4)	0	22,2 (4)	0	33,3 (6)	0	5,6 (1)	0	0	0	0
	C	4,3 (1)	0	0	0	0	8,7 (2)	4,30 (1)	8,7 (1)	4,3 (1)	0	13,0 (3)	0	17,4 (4)	0	30,4 (7)	0	8,7 (2)	0	0	0	0
	D	5,3 (1)	5,3 (1)	0	15,8 (3)	0	5,3 (1)	10,5 (2)	5,3 (1)	0	0	10,5 (2)	5,3 (1)	10,5 (2)	0	10,5 (2)	0	5,3 (1)	0	5,3 (1)	0	0

Anmerkung. Häufigkeiten der Differenzen unter Verwendung der zweiten Methode zur Reskalierung verglichen zwischen den Gruppen farblich in aufsteigend sortierter Rangfolge: rot, orange, gelb, grün. Angaben in Prozent mit absoluten Häufigkeiten in Klammern.

Fortsetzung Tabelle 129

Szenario	Häufigkeiten Gesamt Skala -78,6	-75	-63,3	-53,6	-50	-38,3	-28,6	-25	-13,3	-3,6	0,0	11,7	21,4	25	36,7	46,4	50	61,7	71,4	86,7
Messenger	1,23 (1)	2,47 (2)	3,7 (3)	1,23 (1)	8,64 (7)	3,7 (3)	13,58 (11)	3,70 (3)	11,11 (9)	1,23 (1)	14,81 (12)	2,47 (2)	18,52 (15)	0	8,64 (7)	0	3,7 (3)	0	1,23 (1)	0
Videokonferenz	0	1,2 (1)	0	0	1,2 (1)	0	1,2 (1)	6,2 (5)	2,5 (2)	22,2 (18)	2,5 (2)	24,7 (20)	12,3 (10)	2,5 (2)	1,2 (1)	7,4 (6)	1,2 (1)	6,2 (5)	2,5 (2)	0
Wetter	1,2 (1)	4,9 (4)	2,5 (2)	4,9 (4)	3,7 (4)	6,2 (5)	2,5 (2)	14,8 (12)	8,6 (7)	6,2 (5)	13,6 (11)	8,6 (7)	8,6 (7)	2,5 (2)	7,4 (6)	0	1,2 (1)	0	1,2 (1)	0
E-Mail	2,5 (2)	0	0	0	7,4 (6)	1,2 (1)	11,1 (9)	2,5 (2)	14,8 (12)	2,5 (2)	16 (13)	2,5 (2)	18,5 (15)	3,7 (3)	8,6 (7)	0	2,5 (2)	0	1,2 (1)	1,2 (1)
Musik	0	0	0	0	0	0	1,2 (1)	19,8 (1)	0	21 (1)	3,7 (3)	21 (17)	7,4 (6)	8,6 (7)	2,5 (2)	2,5 (2)	7,4 (6)	1,2 (1)	1,2 (1)	0
Fitness	0	0	1,2 (1)	2,5 (2)	1,2 (1)	0	1,2 (1)	2,5 (2)	1,2 (1)	4,9 (4)	17,3 (14)	2,5 (2)	16,0 (13)	0	16,0 (13)	0	13,6 (11)	0	6,2 (5)	3,7 (3)
Spiele	1,2 (1)	1,2 (1)	1,2 (1)	1,2 (1)	6,2 (5)	0	2,5 (2)	2,5 (2)	6,2 (5)	1,2 (1)	19,8 (16)	1,2 (1)	13,6 (11)	1,2 (1)	16 (13)	2,5 (2)	13,6 (11)	0	1,2 (1)	2,5 (2)
Nachrichten	3,7 (3)	1,2 (1)	0	3,7 (3)	0	4,9 (4)	6,2 (5)	3,7 (3)	1,2 (1)	0	21 (17)	1,20 (1)	16 (13)	0	22,2 (18)	0	12,3 (10)	0	1,2 (1)	0

Anmerkung. Häufigkeiten Gesamt der Differenzen unter Verwendung der zweiten Methode zur Reskalierung farblich in aufsteigend sortierter Rangfolge: rot, orange, gelb, grün. Angaben in Prozent mit absoluten Häufigkeiten in Klammern.

Tabelle 130 *Häufigkeit der Differenzen unter Verwendung der dritten Methode (dividierte Reskalierung)*

Teil 1

Häufigkeiten

	Gruppe	Skala														
		-3,29	-3,00	-2,57	-2,29	-2,00	-1,86	-1,57	-1,29	-1,14	-1.00	-,86	-,57	-0.29	-,14	,00
Messenger	A	0	0	0	0	4.8 (1)	0	4.8 (1)	14.3 (3)	4.8 (1)	0	0	9.5 (2)	0	0	9.5 (2)
	B	0	11.1 (2)	5.6 (1)	0	5.6 (1)	0	0	16.7 (3)	0	0	5.6 (1)	11.1 (2)	0	5.6 (1)	0
	C	0	0	8.7 (2)	4.3 (1)	4.3 (1)	8.7 (2)	4.3 (1)	13 (3)	0	0	8.7 (2)	17.4 (4)	0	0	0
	D	5.3 (1)	0	0	0	10.5 (2)	0	5.3 (1)	5.3 (1)	0	0	0	5.3 (1)	0	0	0
Videokonferenz	A	0	0	0	0	0	0	0	0	0	14.3 (3)	0	4.8 (1)	14.3 (3)	0	9.5 (2)
	B	0	0	0	0	0	0	0	5.6 (1)	0	11.1 (2)	0	5.6 (1)	33.3 (6)	0	0
	C	0	0	0	0	0	4.3 (1)	0	0	0	0	0	0	26.1 (6)	4.3 (1)	4.3 (1)
	D	0	5.3 (1)	0	0	0	0	0	0	0	0	0	0	10.5 (2)	0	0
Wetter	A	0	0	0	0	0	0	0	0	0	23.8 (5)	0	9.5 (2)	4.8 (1)	0	19 (4)
	B	0	5.6 (1)	0	5.6 (1)	5.6 (1)	0	5.6 (1)	5.6 (1)	0	16.7 (3)	0	16.7 (3)	5.6 (1)	0	16.7 (3)
	C	0	4.3 (1)	4.3 (1)	8.7 (2)	0	0	13 (3)	4.3 (1)	0	4.3 (1)	0	4.3 (1)	4.3 (1)	13 (3)	0
	D	5.3 (1)	10.5 (2)	5.3 (1)	5.3 (1)	10.5 (2)	0	5.3 (1)	0	0	5.3 (1)	10.5 (2)	5.3 (1)	10.5 (2)	0	0
E-Mail	A	0	0	0	0	9.5 (2)	0	4.8 (1)	4.8 (1)	0	9.5 (2)	0	4.8 (1)	4.8 (1)	0	9.5 (2)
	B	5.6 (1)	0	0	0	5.6 (1)	5.6 (1)	0	11.1 (2)	5.6 (1)	0	0	5.6 (1)	5.6 (1)	0	11.1 (2)
	C	4.3 (1)	0	0	0	4.3 (1)	4.3 (1)	0	8.7 (2)	0	0	0	17.4 (4)	0	0	0
	D	0	0	0	0	0	0	0	15.8 (3)	0	0	0	31.6 (6)	0	0	5.3 (1)
Musik	A	0	0	0	0	0	0	0	0	0	33.3 (7)	0	0	14.3 (3)	0	4.8 (1)
	B	0	0	0	0	0	0	0	0	0	5.6 (1)	0	0	11.1 (2)	0	11.1 (2)
	C	0	0	0	0	0	0	0	0	4.3 (1)	8.7 (2)	4.3 (1)	0	34.8 (8)	0	0
	D	0	0	0	0	0	0	0	0	0	26.3 (5)	0	0	21.1 (4)	0	0

Fortsetzung Tabelle 130

Teil 1

	Gruppe	Skala														
		- 3,29	- 3,00	- 2,57	- 2,29	- 2,00	- 1,86	- 1,57	- 1,29	- 1,14	- 1.00	- ,86	-,57	- 0.29	-,14	,00
Fitness	A	0	0	0	0	0	0	0	0	0	4.8 (1)	0	0	0	0	28.6 (6)
	B	0	0	0	0	0	0	0	0	0	0	5.6 (1)	0	0	0	22.2 (4)
	C	0	0	0	0	0	0	0	0	4.3 (1)	0	0	4.3 (1)	0	4.3 (1)	4.3 (1)
	D	0	0	5.3 (1)	10.5 (2)	0	5.3 (1)	0	0	0	0	0	0	5.3 (1)	10.5 (2)	0
Spiele	A	4.8 (1)	0	0	0	0	0	0	4.8 (1)	0	4.8 (1)	0	0	0	0	28.6 (6)
	B	0	0	0	0	5.6 (1)	0	0	0	0	0	0	5.6 (1)	0	0	22.2 (4)
	C	0	0	4.3 (1)	0	0	0	0	0	0	0	0	17.4 (4)	4.3 (1)	0	0
	D	0	5.3 (1)	0	5.3 (1)	21.1 (4)	0	0	5.3 (1)	0	0	5.3 (1)	0	0	0	0
Nachrichten	A	0	0	0	0	0	0	4.8 (1)	0	0	0	0	0	0	0	38.1 (8)
	B	5.6 (1)	0	0	0	0	0	0	11.1 (2)	0	0	0	0	0	0	22.2 (4)
	C	4.3 (1)	0	0	0	0	0	8.7 (2)	0	4.3 (1)	0	8.7 (2)	4.3 (1)	0	0	8.7 (2)
	D	5.3 (1)	5.3 (1)	0	15.8 (3)	0	0	5.3 (1)	5.3 (1)	5.3 (1)	0	5.3 (1)	0	0	0	10.5 (2)

Anmerkung. Häufigkeit der Differenzen verglichen unter den Gruppen farblich aufsteigend in folgender Reihenfolge markiert: rot, orange, gelb, grün.

Fortsetzung Tabelle 130

Teil 2

		Häufigkeiten																
		Skala																
Gruppe		0.14	0.29	0.43	,57	,71	,86	1.14	1.29	1,43	1,57	1.86	2,14	2,29	2.57	2,86	3.57	4
Messenger	A	19 (4)	0	0	4.8 (1)	4.8 (1)	9.5 (2)	0	0	0	14.3 (3)	0	0	0	0	0	0	0
	B	11.1 (2)	0	0	0	11.1 (2)	11.1 (2)	0	0	5.6 (1)	0	0	0	0	0	0	0	0
	C	4.3 (1)	0	0	4.3 (1)	4.3 (1)	13 (3)	0	0	0	0	0	4.3 (1)	0	0	0	0	0
	D	15.8 (3)	0	0	0	0	21.1 (4)	0	0	0	15.8 (3)	0	0	10.5 (2)	0	5.3 (1)	0	0
Videokonferenz	A	0	0	14.3 (3)	0	19 (4)	0	4.8 (1)	0	0	0	4.8 (1)	0	0	4.8 (1)	0	0	9.5 (2)
	B	0	0	22.2 (4)	0	5.6 (1)	0	0	0	0	0	11.1 (2)	0	0	0	0	0	5.6 (1)
	C	0	0	26.1 (6)	0	13 (3)	0	0	0	4.3 (1)	0	4.3 (1)	4.3 (1)	0	8.7 (2)	0	0	0
	D	0	0	36.8 (7)	0	0	5.3 (1)	5.3 (1)	0	0	0	10.5 (2)	0	0	10.5 (2)	10.5 (2)	0	5.3 (1)
Wetter	A	0	0	4.8 (1)	4.8 (1)	9.5 (2)	9.5 (2)	0	4.8 (1)	9.5 (2)	0	0	0	0	0	0	0	0
	B	0	0	5.6 (1)	0	5.6 (1)	0	5.6 (1)	0	0	0	0	0	0	0	0	0	0
	C	0	0	13 (3)	0	8.7 (2)	0	0	0	8.7 (2)	0	0	4.3 (1)	0	0	4.3 (1)	0	0
	D	5.3 (1)	0	0	5.3 (1)	0	0	0	0	0	10.5 (2)	0	0	0	0	0	0	0

Fortsetzung Tabelle 130

Teil 2

Gruppe		Skala																
		0.14	0.29	0.43	,57	,71	,86	1.14	1.29	1,43	1,57	1.86	2,14	2,29	2.57	2,86	3.57	4
E-Mail	A	0	0	4.8 (1)	0	19 (4)	4.8 (1)	4.8 (1)	0	9.5 (2)	0	0	0	0	0	4.8 (1)	0	0
	B	16.7 (3)	0	5.6 (1)	0	11.1 (2)	0	0	0	5.6 (1)	5.6 (1)	0	0	0	0	0	0	0
	C	4.3 (1)	4.3 (1)	0	0	13 (3)	8.7 (2)	8.7 (2)	0	4.3 (1)	0	0	8.7 (2)	0	0	0	4.3 (1)	0
	D	15.8 (3)	0	0	0	0	15.8 (3)	0	0	0	10.5 (2)	0	0	0	0	0	0	0
Musik	A	0	0	23.8 (5)	0	0	0	4.8 (1)	0	0	0	9.5 (2)	0	0	4.8 (1)	0	0	0
	B	0	0	11.1 (2)	0	22.2 (4)	0	11.1 (2)	0	11.1 (2)	0	0	16.7 (3)	0	0	0	0	0
	C	0	0	26.1 (6)	0	8.7 (2)	0	0	0	0	0	0	13 (3)	0	0	0	0	0
	D	0	0	21.1 (4)	0	0	0	21.1 (4)	0	0	0	0	0	0	0	5.3 (1)	0	0
Fitness	A	4.8 (1)	0	0	0	9.5 (2)	0	0	0	9.5 (2)	0	0	9.5 (2)	0	0	4.8 (1)	9.5 (2)	0
	B	0	0	0	0	22.2 (4)	0	0	0	16.7 (3)	0	0	22.2 (4)	0	0	5.6 (1)	0	0
	C	4.3 (1)	0	4.3 (1)	0	17.4 (4)	4.3 (1)	0	0	21.7 (5)	4.3 (1)	0	17.4 (4)	0	0	8.7 (2)	0	0
	D	0	5.3 (1)	0	5.3 (1)	0	10.5 (2)	0	0	5.3 (1)	5.3 (1)	0	5.3 (1)	0	0	5.3 (1)	5.3 (1)	0
Spiele	A	9.5 (2)	0	4.8 (1)	0	19 (4)	0	0	0	9.5 (2)	0	4.8 (1)	0	0	0	0	4.8 (1)	0
	B	0	0	0	0	16.7 (3)	0	5.6 (1)	0	22.2 (4)	0	5.6 (1)	16.7 (3)	0	0	0	0	0
	C	4.3 (1)	0	0	0	17.4 (4)	0	0	0	26.1 (6)	0	0	17.4 (4)	0	0	4.3 (1)	4.3 (1)	0
	D	15.8 (3)	0	0	0	0	0	0	0	0	5.3 (1)	0	10.5 (2)	10.5 (2)	0	0	0	0

Fortsetzung Tabelle 130

Teil 2

Gruppe		Skala																
		0.14	0.29	0.43	,57	,71	,86	1.14	1.29	1,43	1,57	1.86	2,14	2,29	2.57	2,86	3.57	4
Nachrichten	A	0	0	0	0	14.3 (3)	0	0	0	14.3 (3)	0	0	28.6 (6)	0	0	0	0	0
	B	0	0	0	0	22.2 (4)	0	0	0	33.3 (6)	0	0	5.6 (1)	0	0	0	0	0
	C	4.3 (1)	0	0	0	17.4 (4)	0	0	0	30.4 (7)	0	0	8.7 (2)	0	0	0	0	0
	D	0	0	0	5.3 (1)	0	10.5 (2)	0	0	10.5 (2)	0	0	5.3 (1)	0	0	5.3 (1)	0	0

Fortsetzung Tabelle 130

Teil 1

Szenario	Häufigkeiten Gesamt														
	Skala														
	- 3,29	- 3,00	- 2,57	- 2,29	- 2,00	- 1,86	- 1,57	- 1,29	- 1,14	- 1.00	- ,86	-,57	- 0.29	- ,14	,00
Messenger	1.2 (1)	2.5 (2)	3.7 (3)	1.2 (1)	6.2 (5)	2.5 (2)	3.7 (3)	12.3 (10)	1.2 (1)	0	3.7 (3)	11.1 (9)	0	1.2 (1)	2.5 (2)
Videokonferenz	0	1.2 (1)	0	0	0	1.2 (1)	0	1.2 (1)	0	6.2 (5)	0	2.5 (2)	21 (17)	1.2 (1)	3.7 (3)
Wetter	1.2 (1)	4.9 (4)	2.5 (2)	4.9 (4)	3.7 (3)	0	6.2 (5)	2.5 (2)	0	12.3 (10)	2.5 (2)	8.6 (7)	6.2 (5)	0	8.6 (7)
E-Mail	2.5 (2)	0	0	0	4.9 (4)	2.5 (2)	1.2 (1)	9.9 (8)	1.2 (1)	2.5 (2)	0	14.8 (12)	2.5 (2)	0	6.2 (5)
Musik	0	0	0	0	0	0	0	0	1.2 (1)	18.5 (15)	1.2 (1)	0	21 (17)	0	3.7 (3)
Fitness	0	0	1.2 (1)	2.5 (2)	0	1.2 (1)	0	0	1.2 (1)	1.2 (1)	1.2 (1)	1.2 (1)	1.2 (1)	3.7 (3)	13.6 (11)
Spiele	1.2 (1)	1.2 (1)	1.2 (1)	1.2 (1)	6.2 (5)	0	0	2.5 (2)	0	1.2 (1)	1 (1)	6.2 (5)	1.2 (1)	0	12 (10)
Nachrichten	3.7 (3)	1.2 (1)	0	3.7 (3)	0	0	4.9 (4)	3.7 (3)	2.5 (2)	0	3 (:	1.2 (1)	0	0	20 (16)

Anmerkung. Häufigkeiten Gesamt farblich aufsteigend in folgender Reihenfolge markiert: rot, orange, gelb, grün.

Fortsetzung Tabelle 130

Teil 2

Häufigkeiten Gesamt																	
Szenario	Skala																
	0.14	0.29	0.43	,57	,71	,86	1.14	1.29	1,43	1,57	1.86	2,14	2,29	2.57	2,86	3.57	4
Messenger	12.3 (10)	0	0	2.5 (2)	4.9 (4)	13.6 (11)	0	0	1.2 (1)	7.4 (6)	0	1.2 (1)	2.5 (2)	0	1.2 (1)	0	0
Videokonferenz	0	0	24.7 (20)	0	9.9 (8)	1.2 (1)	2.5 (2)	0	1.2 (1)	0	7.4 (6)	1.2 (1)	0	6.2 (5)	2.5 (2)	0	4.9 (4)
Wetter	4.9 (4)	0	6.2 (5)	2.5 (2)	6.2 (5)	2.5 (2)	1.2 (1)	1.2 (1)	4.9 (4)	2.5 (2)	0	1.2 (1)	0	0	1.2 (1)	0	0
E-Mail	8.6 (7)	1.2 (1)	2.5 (2)	0	11.1 (9)	7.4 (6)	3.7 (3)	0	4.9 (4)	3.7 (3)	0	2.5 (2)	0	0	1.2 (1)	1.2 (1)	0
Musik	0	0	21 (17)	0	7.4 (6)	0	8.6 (7)	0	2.5 (2)	0	2.5 (2)	7.4 (6)	0	1.2 (1)	1.2 (1)	0	0
Fitness	2.5 (2)	1.2 (1)	1.2 (1)	1.2 (1)	12.3 (10)	3.7 (3)	0	0	13.6 (11)	2.5 (2)	0	13.6 (11)	0	0	6.2 (5)	3.7 (3)	0
Spiele	7.4 (6)	0	1.2 (1)	0	13.6 (11)	0	1.2 (1)	0	14.8 (12)	1.2 (1)	2.5 (2)	11.1 (9)	2.5 (2)	0	1.2 (1)	2.5 (2)	0
Nachrichten	1.2 (1)	0	0	1.2 (1)	13.6 (11)	2.5 (2)	0	0	22.2 (18)	0	0	12.3 (10)	0	0	1.2 (1)	0	0

Tabelle 131 *Mittelwerte der Beträge der Differenzen zwischen der angegebenen Vertrauenswürdigkeit und der angegebenen Aggressivität durch die Datenschutzskala unter Verwendung der ersten Methode (gestauchte Reskalierung)*

Deskriptive Statistiken

Applikation Vertrauenswürdigkeit	Gruppe A				Gruppe B				Gruppe C				Gruppe D				Gesamt			
	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV
Messenger	21	1,05	0,86	,002c	18	1,28	1,07	,030c	23	1,52	0,85	,001c	19	1,58	1,02	,005c	81	1,36	0,95	0
Videokonferenz	19	0,68	0,82	,001c	17	0,88	0,70	,002c	23	0,83	0,98	,000c	18	1,28	1,27	,012c	77	0,91	0,98	0
Wetter	21	0,67	0,48	,000c	18	1,11	0,96	,001c	23	1,30	1,18	,008c	18	1,83	1,04	,011c	80	1,21	1,03	0
E-Mail	20	0,95	0,89	,008c	18	1,00	1,14	,003c	22	1,32	1,13	,001c	18	1,06	0,73	,003c	78	1,09	0,98	0
Musik	20	0,90	0,79	,000c	18	0,72	0,75	,001c	23	0,78	0,67	,000c	18	0,89	0,68	,000c	79	0,82	0,71	0
Fitness	17	1,06	1,43	,000c	17	0,88	0,99	,001c	23	1,04	0,98	,008c	16	1,69	1,25	,060c	73	1,15	1,17	0
Spiele	20	0,75	1,29	,000c	18	0,89	0,83	,005c	23	1,26	1,05	,000c	16	1,69	0,95	,000c	77	1,13	1,09	0
Nachrichten	21	0,81	0,93	,000c	18	0,89	1,08	,008c	23	1,00	0,95	,000c	18	1,78	1,17	,005c	80	1,10	1,07	0

Anmerkung. Mittelwerte der Beträge der Differenzen zwischen der angegebenen Vertrauenswürdigkeit und der angegebenen Aggressivität durch die Datenschutzskala verglichen zwischen den Gruppen farblich in absteigend sortierter Rangfolge: rot, orange, gelb, grün.

Tabelle 132 *Mittelwerte der Beträge der Differenzen zwischen der angegebenen Vertrauenswürdigkeit und der angegebenen Aggressivität durch die Datenschutzskala unter Verwendung der zweiten Methode (prozentuale Reskalierung)*

Deskriptive Statistiken

Applikation Vertrauenswürdigkeit	Gruppe A				Gruppe B				Gruppe C				Gruppe D				Gesamt			
	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV
Messenger	21	19,84	16,13	0,006	18	29,63	23,26	0,028	23	31,52	19,13	0,007	19	32,02	22,95	0,156	81	28,19	20,61	0
Videokonferenz	19	18,42	13,49	0,007	17	16,67	12,15	0	23	19,56	18,57	0	18	29,17	25,45	0	77	20,89	18,47	0
Wetter	21	16,27	10,70	0,069	18	24,54	20,70	0,03	23	30,80	23,63	0,132	18	37,96	25,92	0,2	80	27,19	22,02	0
E-Mail	20	25,00	17,31	0,072	18	23,15	22,79	0,197	22	30,30	22,64	0,005	18	17,59	12,09	0,004	78	24,36	19,54	0
Musik	20	20,42	14,68	0,003	18	21,76	16,20	0,133	23	17,75	14,72	0	18	19,91	14,33	0	79	19,83	14,76	0
Fitness	17	26,96	29,98	0,02	17	26,96	21,15	0,2	23	29,71	19,27	0,039	16	35,42	26,61	0,098	73	29,68	23,89	0
Spiele	20	20,42	25,57	0,019	18	25,93	18,50	0,2	23	32,97	21,09	0,007	16	39,06	22,30	0	77	29,33	22,69	0
Nachrichten	21	23,41	21,67	0,002	18	25,93	20,79	0,004	23	28,99	18,61	0,03	18	38,43	24,94	0,2	80	28,96	21,75	0

Anmerkung. Mittelwerte der Beträge der Differenzen zwischen der angegebenen Vertrauenswürdigkeit und der angegebenen Aggressivität durch die Datenschutzskala verglichen zwischen den Gruppen farblich in absteigend sortierter Rangfolge: rot, orange, gelb, grün.

Tabelle 133 *Mittelwerte der Beträge der Differenzen zwischen der angegebenen Vertrauenswürdigkeit und der angegebenen Aggressivität durch die Datenschutzskala unter Verwendung der dritten Methode (dividierte Reskalierung)*

Deskriptive Statistiken

Applikation Vertrauenswürdigkeit	Gruppe A				Gruppe B				Gruppe C				Gruppe D				Gesamt			
	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV
Messenger	21	0,86	0,62	0,166	18	1,19	0,91	0,062	23	1,25	0,72	0,003	19	1,41	0,91	,200[c,d]	81	1,17	0,80	0
Videokonferenz	21	1,05	1,14	0	18	0,88	0,94	0,002	23	0,83	0,80	0	19	1,43	1,21	,001[c]	81	1,04	1,04	0
Wetter	21	0,70	0,46	0,2	18	0,97	0,82	0,2	23	1,26	0,92	0,126	18	1,52	1,02	,200[c,d]	80	1,11	0,87	0
E-Mail	20	1,04	0,71	0,2	18	0,94	0,88	0,2	22	1,27	0,91	0,087	18	0,75	0,49	,068[c]	78	1,01	0,78	0,001
Musik	20	0,87	0,64	0,012	18	0,94	0,70	0,115	23	0,73	0,62	0	18	0,85	0,62	,002[c]	79	0,84	0,63	0
Fitness	17	1,16	1,28	0,072	17	1,14	0,91	0,2	23	1,27	0,83	0,2	16	1,48	1,08	,200[c,d]	73	1,26	1,01	0,002
Spiele	20	0,87	1,05	0,02	18	1,10	0,79	0,2	23	1,38	0,90	0,013	16	1,64	0,88	,001[c]	77	1,24	0,94	0
Nachrichten	21	0,99	0,92	0,003	18	1,08	0,84	0,015	23	1,18	0,75	0,08	18	1,57	0,98	,200[c,d]	80	1,19	0,88	0,007

Anmerkung. Mittelwerte der Beträge der Differenzen zwischen der angegebenen Vertrauenswürdigkeit und der angegebenen Aggressivität durch die Datenschutzskala verglichen zwischen den Gruppen farblich in absteigend sortierter Rangfolge: rot, orange, gelb, grün.

Tabelle 134 *Kruskal-Wallis-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppen (gestauchte Reskalierung)*

Ränge			
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	45,43
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	34,67
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	33,57
	D: Keine Datenschutzskala	19	51,11
	Gesamtsumme	81	
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	19	36,97
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	29,03
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	39,89
	D: Keine Datenschutzskala	18	49,42
	Gesamtsumme	77	
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	51,86
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	36,03
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	40,93
	D: Keine Datenschutzskala	18	31,17
	Gesamtsumme	80	
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	40,33
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	35,03
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	42,23
	D: Keine Datenschutzskala	18	39,72
	Gesamtsumme	78	
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	37,53
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	50,72
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	35,24
	D: Keine Datenschutzskala	18	38,11
	Gesamtsumme	79	

Fortsetzung Tabelle 134

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	37,56
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	37,29
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	39,26
	D: Keine Datenschutzskala	16	32,84
	Gesamtsumme	73	
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	35,60
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	44,33
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	43,20
	D: Keine Datenschutzskala	16	31,22
	Gesamtsumme	77	
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	48,31
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	40,47
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	39,02
	D: Keine Datenschutzskala	18	33,31
	Gesamtsumme	80	

Teststatistiken[a,b]

	Vertrauenswürdigkeit							
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Chi-Quadrat	8,137	8,335	9,055	1,105	5,978	,959	4,503	4,477
df	3	3	3	3	3	3	3	3
Asymp. Sig.	,043	,040	,029	,776	,113	,811	,212	,214

a. Kruskal-Wallis-Test

b. Gruppierungsvariable: Gruppe

Tabelle *135 Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und B (gestauchte Reskalierung)*

Ränge				
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	22,50	472,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	17,08	307,50
	Gesamtsumme	39		
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	19	20,47	389,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	16,29	277,00
	Gesamtsumme	36		
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	24,07	505,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	15,25	274,50
	Gesamtsumme	39		
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	20,80	416,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	18,06	325,00
	Gesamtsumme	38		
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	16,55	331,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	22,78	410,00
	Gesamtsumme	38		
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	17,53	298,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	17,47	297,00
	Gesamtsumme	34		

Fortsetzung Tabelle 135

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	17,03	340,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	22,25	400,50
	Gesamtsumme	38		
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	21,76	457,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	17,94	323,00
	Gesamtsumme	39		

Teststatistiken[a]

	Vertrauenswürdigkeit							
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	136,500	124,000	103,500	154,000	121,000	144,000	130,500	152,000
Wilcoxon-W	307,500	277,000	274,500	325,000	331,000	297,000	340,500	323,000
z	-1,517	-1,286	-2,527	-,792	-1,812	-,019	-1,573	-1,120
Asymp. Sig. (2-seitig)	,129	,198	,011	,428	,070	,985	,116	,263
Exakte Sig. [2*(1-seitige Sig.)]	,140[b]	,244[b]	,015[b]	,460[b]	,087[b]	1,000[b]	,149[b]	,308[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 136 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und C (gestauchte Reskalierung)*

Ränge

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	26,14	549,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,17	441,00
	Gesamtsumme	44		
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	19	20,58	391,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,26	512,00
	Gesamtsumme	42		
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	25,33	532,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,91	458,00
	Gesamtsumme	44		
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	20,88	417,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	22,07	485,50
	Gesamtsumme	42		
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	22,60	452,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,48	494,00
	Gesamtsumme	43		
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	19,94	339,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,91	481,00
	Gesamtsumme	40		

Fortsetzung Tabelle 136

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	19,73	394,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	23,98	551,50
	Gesamtsumme	43		
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	25,38	533,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,87	457,00
	Gesamtsumme	44		

Teststatistiken[a]

	Vertrauenswürdigkeit							
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	165,000	201,000	182,000	207,500	218,000	186,000	184,500	181,000
Wilcoxon-W	441,000	391,000	458,000	417,500	494,000	339,000	394,500	457,000
z	-1,836	-,476	-1,444	-,322	-,321	-,273	-1,157	-1,488
Asymp. Sig. (2-seitig)	,066	,634	,149	,747	,748	,785	,247	,137
Exakte Sig. [2*(1-seitige Sig.)]						,808[b]		

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle *137 Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und D gestauchte (Reskalierung)*

Ränge

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	18,79	394,50
	D: Keine Datenschutzskala	19	22,39	425,50
	Gesamtsumme	40		
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	19	15,92	302,50
	D: Keine Datenschutzskala	18	22,25	400,50
	Gesamtsumme	37		
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	24,45	513,50
	D: Keine Datenschutzskala	18	14,81	266,50
	Gesamtsumme	39		
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	19,65	393,00
	D: Keine Datenschutzskala	18	19,33	348,00
	Gesamtsumme	38		
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	19,38	387,50
	D: Keine Datenschutzskala	18	19,64	353,50
	Gesamtsumme	38		
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	18,09	307,50
	D: Keine Datenschutzskala	16	15,84	253,50
	Gesamtsumme	33		
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	19,85	397,00
	D: Keine Datenschutzskala	16	16,81	269,00
	Gesamtsumme	36		
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	23,17	486,50
	D: Keine Datenschutzskala	18	16,31	293,50
	Gesamtsumme	39		

Fortsetzung Tabelle 137

Teststatistiken[a]								
	Vertrauenswürdigkeit							
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	163,500	112,500	95,500	177,000	177,500	117,500	133,000	122,500
Wilcoxon-W	394,500	302,500	266,500	348,000	387,500	253,500	269,000	293,500
z	-,996	-1,872	-2,719	-,090	-,079	-,686	-,905	-1,925
Asymp. Sig. (2-seitig)	,319	,061	,007	,928	,937	,493	,366	,054
Exakte Sig. [2*(1-seitige Sig.)]	,333[b]	,075[b]	,007[b]	,942[b]	,942[b]	,510[b]	,404[b]	,060[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 138 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe B und C (gestauchte Reskalierung)*

Ränge				
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	21,42	385,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,67	475,50
	Gesamtsumme	41		
Videokonferenz	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	17,18	292,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,96	528,00
	Gesamtsumme	40		

Fortsetzung Tabelle 138

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Wetter	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,69	354,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,02	506,50
	Gesamtsumme	41		
E-Mail	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	18,50	333,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	22,14	487,00
	Gesamtsumme	40		
Musik	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	25,64	461,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	17,37	399,50
	Gesamtsumme	41		
Fitness	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	19,82	337,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,00	483,00
	Gesamtsumme	40		
Spiele	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	21,17	381,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,87	480,00
	Gesamtsumme	41		
Nachrichten	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	21,47	386,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,63	474,50
	Gesamtsumme	41		

Fortsetzung Tabelle 138

Teststatistiken[a]

	Vertrauenswürdigkeit							
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	199,500	139,000	183,500	162,000	123,500	184,000	204,000	198,500
Wilcoxon-W	475,500	292,000	354,500	333,000	399,500	337,000	480,000	474,500
z	-,201	-1,645	-,635	-1,005	-2,328	-,329	-,081	-,233
Asymp. Sig. (2-seitig)	,840	,100	,526	,315	,020	,742	,935	,816
Exakte Sig. [2*(1-seitige Sig.)]		,126[b]		,338[b]		,766[b]		

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 139 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe B und D (gestauchte Reskalierung)*

Ränge

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	15,17	273,00
	D: Keine Datenschutzskala	19	22,63	430,00
	Gesamtsumme	37		
Videokonferenz	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	13,56	230,50
	D: Keine Datenschutzskala	18	22,19	399,50
	Gesamtsumme	35		

Fortsetzung Tabelle 139

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Wetter	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	20,08	361,50
	D: Keine Datenschutzskala	18	16,92	304,50
	Gesamtsumme	36		
E-Mail	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	17,47	314,50
	D: Keine Datenschutzskala	18	19,53	351,50
	Gesamtsumme	36		
Musik	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	21,31	383,50
	D: Keine Datenschutzskala	18	15,69	282,50
	Gesamtsumme	36		
Fitness	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	18,00	306,00
	D: Keine Datenschutzskala	16	15,94	255,00
	Gesamtsumme	33		
Spiele	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,92	358,50
	D: Keine Datenschutzskala	16	14,78	236,50
	Gesamtsumme	34		
Nachrichten	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	20,06	361,00
	D: Keine Datenschutzskala	18	16,94	305,00
	Gesamtsumme	36		

Fortsetzung Tabelle 139

Teststatistiken[a]								
	Vertrauenswürdigkeit							
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	102,000	77,500	133,500	143,500	111,500	119,000	100,500	134,000
Wilcoxon-W	273,000	230,500	304,500	314,500	282,500	255,000	236,500	305,000
z	-2,130	-2,589	-,930	-,604	-1,670	-,629	-1,542	-,910
Asymp. Sig. (2-seitig)	,033	,010	,352	,546	,095	,529	,123	,363
Exakte Sig. [2*(1-seitige Sig.)]	,036[b]	,011[b]	,372[b]	,563[b]	,111[b]	,557[b]	,135[b]	,389[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 140 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe C und D (gestauchte Reskalierung)*

Ränge				
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	17,72	407,50
	D: Keine Datenschutzskala	19	26,08	495,50
	Gesamtsumme	42		
Videokonferenz	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,67	429,50
	D: Keine Datenschutzskala	18	23,97	431,50
	Gesamtsumme	41		
Wetter	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	23,00	529,00
	D: Keine Datenschutzskala	18	18,44	332,00
	Gesamtsumme	41		
E-Mail	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	21,02	462,50
	D: Keine Datenschutzskala	18	19,86	357,50
	Gesamtsumme	40		

Fortsetzung Tabelle 140

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Musik	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,39	469,00
	D: Keine Datenschutzskala	18	21,78	392,00
	Gesamtsumme	41		
Fitness	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,35	491,00
	D: Keine Datenschutzskala	16	18,06	289,00
	Gesamtsumme	39		
Spiele	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,35	514,00
	D: Keine Datenschutzskala	16	16,63	266,00
	Gesamtsumme	39		
Nachrichten	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,52	518,00
	D: Keine Datenschutzskala	18	19,06	343,00
	Gesamtsumme	41		

Teststatistiken[a]

	Vertrauenswürdigkeit							
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	131,500	153,500	161,000	186,500	193,000	153,000	130,000	172,000
Wilcoxon-W	407,500	429,500	332,000	357,500	469,000	289,000	266,000	343,000
z	-2,237	-1,478	-1,229	-,319	-,401	-,906	-1,566	-,939
Asymp. Sig. (2-seitig)	,025	,139	,219	,750	,688	,365	,117	,348
Exakte Sig. [2*(1-seitige Sig.)]				,757[b]		,388[b]	,128[b]	

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 141 *Kruskal-Wallis-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppen (prozentuale Reskalierung)*

Ränge			
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	32,52
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	41,08
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	44,22
	D: Keine Datenschutzskala	19	46,39
	Gesamtsumme	81	
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	19	40,37
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	34,18
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	35,39
	D: Keine Datenschutzskala	18	46,72
	Gesamtsumme	77	
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	30,86
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	37,44
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	44,20
	D: Keine Datenschutzskala	18	50,08
	Gesamtsumme	80	
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	42,73
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	37,06
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	45,16
	D: Keine Datenschutzskala	18	31,44
	Gesamtsumme	78	
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	42,10
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	42,97
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	35,07
	D: Keine Datenschutzskala	18	41,00
	Gesamtsumme	79	

Fortsetzung Tabelle 141

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	32,76
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	35,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	38,04
	D: Keine Datenschutzskala	16	41,59
	Gesamtsumme	73	
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	28,68
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	36,97
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	42,30
	D: Keine Datenschutzskala	16	49,44
	Gesamtsumme	77	
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	36,38
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	36,64
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	40,76
	D: Keine Datenschutzskala	18	48,83
	Gesamtsumme	80	

Teststatistiken[a,b]

	Messenger	Videocongerence	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Chi-Quadrat	4,223	3,731	7,656	4,343	1,642	1,605	8,615	3,573
df	3	3	3	3	3	3	3	3
Asymp. Sig.	,238	,292	,054	,227	,650	,658	,035	,311

a. Kruskal-Wallis-Test

b. Gruppierungsvariable: Gruppe

Tabelle 142 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und B (prozentuale Reskalierung)*

Ränge				
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	18,29	384,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	22,00	396,00
	Gesamtsumme	39		
Videocongerence	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	19	19,79	376,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	17,06	290,00
	Gesamtsumme	36		
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	18,60	390,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	21,64	389,50
	Gesamtsumme	39		
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	20,65	413,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	18,22	328,00
	Gesamtsumme	38		
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	19,25	385,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,78	356,00
	Gesamtsumme	38		
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	16,88	287,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	18,12	308,00
	Gesamtsumme	34		

Fortsetzung Tabelle 142

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	17,25	345,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	22,00	396,00
	Gesamtsumme	38		
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,95	419,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	20,06	361,00
	Gesamtsumme	39		

Teststatistiken[a]

	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	153,000	137,000	159,500	157,000	175,000	134,000	135,000	188,000
Wilcoxon-W	384,000	290,000	390,500	328,000	385,000	287,000	345,000	419,000
z	-1,026	-,789	-,843	-,678	-,149	-,371	-1,345	-,029
Asymp. Sig. (2-seitig)	,305	,430	,399	,498	,882	,711	,179	,977
Exakte Sig. [2*(1-seitige Sig.)]	,321[b]	,452[b]	,410[b]	,515[b]	,897[b]	,734[b]	,196[b]	,989[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 143 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und C (prozentuale Reskalierung)*

Ränge				
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,05	400,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	25,65	590,00
	Gesamtsumme	44		
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	19	23,00	437,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,26	466,00
	Gesamtsumme	42		
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	18,64	391,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	26,02	598,50
	Gesamtsumme	44		
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	20,78	415,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	22,16	487,50
	Gesamtsumme	42		
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	24,00	480,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,26	466,00
	Gesamtsumme	43		
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	18,76	319,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,78	501,00
	Gesamtsumme	40		
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	17,73	354,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	25,72	591,50
	Gesamtsumme	43		
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	21,40	449,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	23,50	540,50
	Gesamtsumme	44		

Fortsetzung Tabelle 143

Teststatistiken[a]								
	Messenger	Videocongerence	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	169,000	190,000	160,500	205,500	190,000	166,000	144,500	218,500
Wilcoxon-W	400,000	466,000	391,500	415,500	466,000	319,000	354,500	449,500
z	-1,718	-,732	-1,916	-,369	-,999	-,819	-2,107	-,551
Asymp. Sig. (2-seitig)	,086	,464	,055	,712	,318	,413	,035	,582
Exakte Sig. [2*(1-seitige Sig.)]						,432[b]		

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 144 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und D (prozentuale Reskalierung)*

Ränge				
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	17,19	361,00
	D: Keine Datenschutzskala	19	24,16	459,00
	Gesamtsumme	40		
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	19	17,58	334,00
	D: Keine Datenschutzskala	18	20,50	369,00
	Gesamtsumme	37		
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	15,62	328,00
	D: Keine Datenschutzskala	18	25,11	452,00
	Gesamtsumme	39		
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	22,30	446,00
	D: Keine Datenschutzskala	18	16,39	295,00
	Gesamtsumme	38		

Fortsetzung Tabelle 144

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	19,85	397,00
	D: Keine Datenschutzskala	18	19,11	344,00
	Gesamtsumme	38		
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	15,12	257,00
	D: Keine Datenschutzskala	16	19,00	304,00
	Gesamtsumme	33		
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	14,70	294,00
	D: Keine Datenschutzskala	16	23,25	372,00
	Gesamtsumme	36		
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	17,02	357,50
	D: Keine Datenschutzskala	18	23,47	422,50
	Gesamtsumme	39		

Teststatistiken[a]

	Messenger	Videocongerence	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	130,000	144,000	97,000	124,000	173,000	104,000	84,000	126,500
Wilcoxon-W	361,000	334,000	328,000	295,000	344,000	257,000	294,000	357,500
z	-1,905	-,833	-2,615	-1,655	-,217	-1,165	-2,471	-1,785
Asymp. Sig. (2-seitig)	,057	,405	,009	,098	,828	,244	,013	,074
Exakte Sig. [2*(1-seitige Sig.)]	,061[b]	,425[b]	,009[b]	,105[b]	,851[b]	,260[b]	,015[b]	,078[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 145 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe B und C (prozentuale Reskalierung)*

Ränge				
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	20,31	365,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,54	495,50
	Gesamtsumme	41		
Videokonferenz	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	20,09	341,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,80	478,50
	Gesamtsumme	40		
Wetter	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,11	344,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,48	517,00
	Gesamtsumme	41		
E-Mail	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	18,36	330,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	22,25	489,50
	Gesamtsumme	40		
Musik	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	23,22	418,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,26	443,00
	Gesamtsumme	41		
Fitness	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	19,82	337,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,00	483,00
	Gesamtsumme	40		
Spiele	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,50	351,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,17	510,00
	Gesamtsumme	41		
Nachrichten	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,58	352,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,11	508,50
	Gesamtsumme	41		

Fortsetzung Tabelle 145

Teststatistiken[a]								
	Messenger	Videocongerence	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	194,500	188,500	173,000	159,500	167,000	184,000	180,000	181,500
Wilcoxon-W	365,500	341,500	344,000	330,500	443,000	337,000	351,000	352,500
z	-,331	-,197	-,897	-1,056	-1,067	-,320	-,720	-,685
Asymp. Sig. (2-seitig)	,741	,844	,370	,291	,286	,749	,471	,493
Exakte Sig. [2*(1-seitige Sig.)]		,850[b]		,299[b]		,766[b]		

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 146 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe C und D (prozentuale Reskalierung)*

Ränge				
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,02	483,50
	D: Keine Datenschutzskala	19	22,08	419,50
	Gesamtsumme	42		
Videokonferenz	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,33	421,50
	D: Keine Datenschutzskala	18	24,42	439,50
	Gesamtsumme	41		
Wetter	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,70	453,00
	D: Keine Datenschutzskala	18	22,67	408,00
	Gesamtsumme	41		
E-Mail	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	23,75	522,50
	D: Keine Datenschutzskala	18	16,53	297,50
	Gesamtsumme	40		
Musik	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,54	449,50
	D: Keine Datenschutzskala	18	22,86	411,50
	Gesamtsumme	41		
Fitness	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,26	443,00
	D: Keine Datenschutzskala	16	21,06	337,00
	Gesamtsumme	39		

Fortsetzung Tabelle 146

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Spiele	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,41	423,50
	D: Keine Datenschutzskala	16	22,28	356,50
	Gesamtsumme	39		
Nachrichten	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,15	440,50
	D: Keine Datenschutzskala	18	23,36	420,50
	Gesamtsumme	41		

Teststatistiken[a]

	Messenger	Videocongerence	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	207,500	145,500	177,000	126,500	173,500	167,000	147,500	164,500
Wilcoxon-W	483,500	421,500	453,000	297,500	449,500	443,000	423,500	440,500
z	-,280	-1,653	-,790	-1,974	-,910	-,490	-1,062	-1,126
Asymp. Sig. (2-seitig)	,779	,098	,429	,048	,363	,624	,288	,260
Exakte Sig. [2*(1-seitige Sig.)]				,051[b]		,641[b]	,301[b]	

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 147 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe B und D (prozentuale Reskalierung)*

Ränge				
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	17,78	320,00
	D: Keine Datenschutzskala	19	20,16	383,00
	Gesamtsumme	37		
Videokonferenz	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	15,03	255,50
	D: Keine Datenschutzskala	18	20,81	374,50
	Gesamtsumme	35		
Wetter	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	15,69	282,50
	D: Keine Datenschutzskala	18	21,31	383,50
	Gesamtsumme	36		
E-Mail	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,47	350,50
	D: Keine Datenschutzskala	18	17,53	315,50
	Gesamtsumme	36		
Musik	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	18,97	341,50
	D: Keine Datenschutzskala	18	18,03	324,50
	Gesamtsumme	36		
Fitness	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	15,56	264,50
	D: Keine Datenschutzskala	16	18,53	296,50
	Gesamtsumme	33		
Spiele	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	14,47	260,50
	D: Keine Datenschutzskala	16	20,91	334,50
	Gesamtsumme	34		
Nachrichten	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	16,00	288,00
	D: Keine Datenschutzskala	18	21,00	378,00
	Gesamtsumme	36		

Fortsetzung Tabelle 147

Teststatistiken[a]								
	Messenger	Videocongerence	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	149,000	102,500	111,500	144,500	153,500	111,500	89,500	117,000
Wilcoxon-W	320,000	255,500	282,500	315,500	324,500	264,500	260,500	288,000
z	-,674	-1,706	-1,607	-,563	-,276	-,891	-1,935	-1,440
Asymp. Sig. (2-seitig)	,500	,088	,108	,574	,783	,373	,053	,150
Exakte Sig. [2*(1-seitige Sig.)]	,518[b]	,096[b]	,111[b]	,584[b]	,791[b]	,382[b]	,059[b]	,161[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 148 *T-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und B, den Gruppen A und C, den Gruppen A und D (prozentuale Reskalierung)*

Test bei unabhängigen Stichproben										
Vertrauenswürdigkeit Gruppe A und B		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
								Standardfehlerdifferenz	95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz		Unterer	Oberer
E-Mail	Varianzgleichheit angenommen	1,715	,199	,284	36	,778	1,85328	6,52512	-11,38027	15,08683
	Varianzgleichheit nicht angenommen			,280	31,617	,781	1,85328	6,62045	-11,63855	15,34511

Fortsetzung Tabelle 148

Test bei unabhängigen Stichproben

Vertrauenswürdigkeit Gruppe A und C		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwert differenz	Standard fehlerdifferenz	Unterer	Oberer
Wetter	Varianzgleichheit angenommen	16,113	,000	-2,584	42	,013	-14,52696	5,62186	-25,87234	-3,18157
	Varianzgleichheit nicht angenommen			-2,665	31,252	,012	-14,52696	5,45192	-25,64259	-3,41132

Test bei unabhängigen Stichproben

Vertrauenswürdigkeit Gruppe A und D		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standard fehlerdifferenz	Unterer	Oberer
E-Mail	Varianzgleichheit angenommen	2,213	,146	1,513	36	,139	7,40717	4,89697	-2,52435	17,33868
	Varianzgleichheit nicht angenommen			1,541	34,007	,133	7,40717	4,80659	-2,36092	17,17525

Tabelle 149 *Kruskal-Wallis-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppen (dividierte Reskalierung)*

Ränge			
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	32,48
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	40,22
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	43,67
	D: Keine Datenschutzskala	19	47,92
	Gesamtsumme	81	
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	42,36
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	37,42
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	35,63
	D: Keine Datenschutzskala	19	49,39
	Gesamtsumme	81	
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	31,12
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	37,03
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	44,22
	D: Keine Datenschutzskala	18	50,17
	Gesamtsumme	80	
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	41,65
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	36,22
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	45,82
	D: Keine Datenschutzskala	18	32,67
	Gesamtsumme	78	
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	41,48
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	43,75
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	34,17
	D: Keine Datenschutzskala	18	42,06
	Gesamtsumme	79	

Fortsetzung Tabelle 149

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	32,41
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	34,62
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	38,20
	D: Keine Datenschutzskala	16	42,69
	Gesamtsumme	73	
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	28,23
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	36,19
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	42,65
	D: Keine Datenschutzskala	16	50,38
	Gesamtsumme	77	
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	36,05
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	36,42
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	40,72
	D: Keine Datenschutzskala	18	49,50
	Gesamtsumme	80	

Teststatistiken[a,b]

	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Chi-Quadrat	4,784	4,216	7,573	3,936	2,255	2,263	9,784	4,129
df	3	3	3	3	3	3	3	3
Asymp. Sig.	,188	,239	,056	,268	,521	,520	,020	,248

a. Kruskal-Wallis-Test

b. Gruppierungsvariable: Gruppe

Tabelle 150 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und B (dividierte Reskalierung)*

Ränge				
Vertrauens-würdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	18,43	387,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	21,83	393,00
	Gesamtsumme	39		
Video-konferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	21,02	441,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	18,81	338,50
	Gesamtsumme	39		
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	18,74	393,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	21,47	386,50
	Gesamtsumme	39		
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	20,58	411,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	18,31	329,50
	Gesamtsumme	38		
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	18,93	378,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	20,14	362,50
	Gesamtsumme	38		
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	17,03	289,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	17,97	305,50
	Gesamtsumme	34		
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	17,43	348,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	21,81	392,50
	Gesamtsumme	38		
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,95	419,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	20,06	361,00
	Gesamtsumme	39		

Fortsetzung Tabelle 150

Teststatistiken[a]								
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	156,000	167,500	162,500	158,500	168,500	136,500	138,500	188,000
Wilcoxon-W	387,000	338,500	393,500	329,500	378,500	289,500	348,500	419,000
z	-,937	-,613	-,754	-,631	-,340	-,281	-1,231	-,029
Asymp. Sig. (2-seitig)	,349	,540	,451	,528	,734	,779	,218	,977
Exakte Sig. [2*(1-seitige Sig.)]	,364[b]	,549[b]	,460[b]	,534[b]	,740[b]	,786[b]	,228[b]	,989[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 151 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und C (dividierte Reskalierung)*

Ränge				
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,14	402,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	25,57	588,00
	Gesamtsumme	44		
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	24,33	511,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,83	479,00
	Gesamtsumme	44		
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	18,60	390,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	26,07	599,50
	Gesamtsumme	44		
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	20,38	407,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	22,52	495,50
	Gesamtsumme	42		

Fortsetzung Tabelle 151

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	24,28	485,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,02	460,50
	Gesamtsumme	43		
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	18,53	315,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,96	505,00
	Gesamtsumme	40		
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	17,58	351,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	25,85	594,50
	Gesamtsumme	43		
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	21,21	445,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	23,67	544,50
	Gesamtsumme	44		

Teststatistiken[a]

	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	171,000	203,000	159,500	197,500	184,500	162,000	141,500	214,500
Wilcoxon-W	402,000	479,000	390,500	407,500	460,500	315,000	351,500	445,500
z	-1,670	-,915	-1,933	-,569	-1,132	-,925	-2,174	-,645
Asymp. Sig. (2-seitig)	,095	,360	,053	,569	,257	,355	,030	,519
Exakte Sig. [2*(1-seitige Sig.)]						,371[b]		

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 152 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe A und D (dividierte Reskalierung)*

Ränge				
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	16,90	355,00
	D: Keine Datenschutzskala	19	24,47	465,00
	Gesamtsumme	40		
Videokonferenz	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,00	399,00
	D: Keine Datenschutzskala	19	22,16	421,00
	Gesamtsumme	40		
Wetter	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	15,79	331,50
	D: Keine Datenschutzskala	18	24,92	448,50
	Gesamtsumme	39		
E-Mail	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	21,70	434,00
	D: Keine Datenschutzskala	18	17,06	307,00
	Gesamtsumme	38		
Musik	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	19,28	385,50
	D: Keine Datenschutzskala	18	19,75	355,50
	Gesamtsumme	38		
Fitness	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	17	14,85	252,50
	D: Keine Datenschutzskala	16	19,28	308,50
	Gesamtsumme	33		
Spiele	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	20	14,23	284,50
	D: Keine Datenschutzskala	16	23,84	381,50
	Gesamtsumme	36		
Nachrichten	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	16,88	354,50
	D: Keine Datenschutzskala	18	23,64	425,50
	Gesamtsumme	39		

Fortsetzung Tabelle 152

Teststatistiken[a]								
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	124,000	168,000	100,500	136,000	175,500	99,500	74,500	123,500
Wilcoxon-W	355,000	399,000	331,500	307,000	385,500	252,500	284,500	354,500
z	-2,064	-,862	-2,504	-1,294	-,135	-1,321	-2,736	-1,869
Asymp. Sig. (2-seitig)	,039	,389	,012	,196	,892	,187	,006	,062
Exakte Sig. [2*(1-seitige Sig.)]	,041[b]	,405[b]	,011[b]	,206[b]	,897[b]	,191[b]	,005[b]	,065[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 153 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe B und C (dividierte Reskalierung)*

Ränge				
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,46	470,50
	D: Keine Datenschutzskala	19	22,76	432,50
	Gesamtsumme	42		
Videokonferenz	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,17	418,00
	D: Keine Datenschutzskala	19	25,53	485,00
	Gesamtsumme	42		
Wetter	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,48	448,00
	D: Keine Datenschutzskala	18	22,94	413,00
	Gesamtsumme	41		
E-Mail	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	23,61	519,50
	D: Keine Datenschutzskala	18	16,69	300,50
	Gesamtsumme	40		
Musik	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,09	439,00
	D: Keine Datenschutzskala	18	23,44	422,00
	Gesamtsumme	41		
Fitness	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,98	436,50
	D: Keine Datenschutzskala	16	21,47	343,50
	Gesamtsumme	39		

Fortsetzung Tabelle 153

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Spiele	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,46	424,50
	D: Keine Datenschutzskala	16	22,22	355,50
	Gesamtsumme	39		
Nachrichten	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,89	434,50
	D: Keine Datenschutzskala	18	23,69	426,50
	Gesamtsumme	41		

Teststatistiken[a]

	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	192,000	198,500	168,500	150,000	162,500	177,500	176,000	180,500
Wilcoxon-W	363,000	474,500	339,500	321,000	438,500	313,500	347,000	351,500
z	-,397	-,228	-1,014	-1,309	-1,186	-,188	-,825	-,712
Asymp. Sig. (2-seitig)	,691	,820	,311	,190	,236	,851	,409	,477
Exakte Sig. [2*(1-seitige Sig.)]				,199[b]		,855[b]		

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 154 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe C und D (dividierte Reskalierung)*

Ränge

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,46	470,50
	D: Keine Datenschutzskala	19	22,76	432,50
	Gesamtsumme	42		
Videokonferenz	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,17	418,00
	D: Keine Datenschutzskala	19	25,53	485,00
	Gesamtsumme	42		
Wetter	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,48	448,00
	D: Keine Datenschutzskala	18	22,94	413,00
	Gesamtsumme	41		
E-Mail	C: Datenschutzskala ohne eine detaillierte Beschreibung	22	23,61	519,50
	D: Keine Datenschutzskala	18	16,69	300,50
	Gesamtsumme	40		

Fortsetzung Tabelle 154

Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Musik	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,09	439,00
	D: Keine Datenschutzskala	18	23,44	422,00
	Gesamtsumme	41		
Fitness	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,98	436,50
	D: Keine Datenschutzskala	16	21,47	343,50
	Gesamtsumme	39		
Spiele	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,46	424,50
	D: Keine Datenschutzskala	16	22,22	355,50
	Gesamtsumme	39		
Nachrichten	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,89	434,50
	D: Keine Datenschutzskala	18	23,69	426,50
	Gesamtsumme	41		

Teststatistiken[a]

	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	194,500	142,000	172,000	129,500	163,000	160,500	148,500	158,500
Wilcoxon-W	470,500	418,000	448,000	300,500	439,000	436,500	424,500	434,500
z	-,612	-1,971	-,922	-1,882	-1,184	-,674	-1,019	-1,284
Asymp. Sig. (2-seitig)	,541	,049	,356	,060	,237	,500	,308	,199
Exakte Sig. [2*(1-seitige Sig.)]				,062[b]		,507[b]	,315[b]	

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 155 *Mann-Whitney-U-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppe B und D (dividierte Reskalierung)*

Ränge				
Vertrauenswürdigkeit	Gruppe	H	Mittlerer Rang	Summe der Ränge
Messenger	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	17,22	310,00
	D: Keine Datenschutzskala	19	20,68	393,00
	Gesamtsumme	37		
Videokonferenz	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	16,14	290,50
	D: Keine Datenschutzskala	19	21,71	412,50
	Gesamtsumme	37		
Wetter	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	15,69	282,50
	D: Keine Datenschutzskala	18	21,31	383,50
	Gesamtsumme	36		
E-Mail	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,08	343,50
	D: Keine Datenschutzskala	18	17,92	322,50
	Gesamtsumme	36		
Musik	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,14	344,50
	D: Keine Datenschutzskala	18	17,86	321,50
	Gesamtsumme	36		
Fitness	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	17	15,18	258,00
	D: Keine Datenschutzskala	16	18,94	303,00
	Gesamtsumme	33		
Spiele	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	14,11	254,00
	D: Keine Datenschutzskala	16	21,31	341,00
	Gesamtsumme	34		
Nachrichten	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	15,83	285,00
	D: Keine Datenschutzskala	18	21,17	381,00
	Gesamtsumme	36		

Fortsetzung Tabelle 155

Teststatistiken[a]								
	Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Mann-Whitney-U-Test	139,000	119,500	111,500	151,500	150,500	105,000	83,000	114,000
Wilcoxon-W	310,000	290,500	282,500	322,500	321,500	258,000	254,000	285,000
z	-,979	-1,595	-1,604	-,335	-,368	-1,122	-2,116	-1,533
Asymp. Sig. (2-seitig)	,327	,111	,109	,738	,713	,262	,034	,125
Exakte Sig. [2*(1-seitige Sig.)]	,343[b]	,118[b]	,111[b]	,743[b]	,719[b]	,276[b]	,036[b]	,134[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 156 *T-Test Vergleich der Adäquatheit der geschätzten Vertrauenswürdigkeit der ausgewählten Applikation zwischen den Gruppen (dividierte Reskalierung)*

		Test bei unabhängigen Stichproben								
	Vertrauenswürdigkeit Gruppe A und B	Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Messenger	Varianzgleichheit angenommen	1,545	,222	-1,353	37	,184	-,33389	,24678	-,83392	,16614
	Varianzgleichheit nicht angenommen			-1,315	29,400	,199	-,33389	,25392	-,85291	,18513
Wetter	Varianzgleichheit angenommen	3,777	,060	-1,278	37	,209	-,26738	,20930	-,69146	,15670
	Varianzgleichheit nicht angenommen			-1,225	25,613	,232	-,26738	,21827	-,71637	,18161
E-Mail	Varianzgleichheit angenommen	1,083	,305	,353	36	,726	,09106	,25759	-,43136	,61347
	Varianzgleichheit nicht angenommen			,350	32,824	,729	,09106	,26046	-,43897	,62108
Fitness	Varianzgleichheit angenommen	2,266	,142	,045	32	,965	,01706	,38033	-,75764	,79176
	Varianzgleichheit nicht angenommen			,045	28,898	,965	,01706	,38033	-,76092	,79503

Fortsetzung Tabelle 156

		Test bei unabhängigen Stichproben								
	Vertrauenswürdigkeit Gruppe A und C	Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit					95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Wetter	Varianzgleichheit angenommen	12,350	,001	-2,527	42	,015	-,55992	,22157	-1,00706	-,11278
	Varianzgleichheit nicht angenommen			-2,599	32,912	,014	-,55992	,21544	-,99829	-,12155
E-Mail	Varianzgleichheit angenommen	,889	,351	-,909	40	,369	-,23041	,25337	-,74250	,28168
	Varianzgleichheit nicht angenommen			-,920	39,184	,363	-,23041	,25043	-,73687	,27606
Nachrichten	Varianzgleichheit angenommen	4,567	,038	-,744	42	,461	-,18766	,25207	-,69635	,32103
	Varianzgleichheit nicht angenommen			-,738	38,679	,465	-,18766	,25445	-,70246	,32714
Fitness	Varianzgleichheit angenommen	4,769	,035	-,322	38	,749	-,10726	,33312	-,78164	,56711
	Varianzgleichheit nicht angenommen			-,302	25,688	,765	-,10726	,35478	-,83695	,62243

Fortsetzung Tabelle 156

		Test bei unabhängigen Stichproben								
	Vertrauenswürdigkeit Gruppe A und D	Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit					95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Messenger	Varianzgleichheit angenommen	2,322	,136	-2,257	38	,030	-,55018	,24380	-1,04371	-,05664
	Varianzgleichheit nicht angenommen			-2,216	31,539	,034	-,55018	,24830	-1,05623	-,04412
Wetter	Varianzgleichheit angenommen	13,661	,001	-3,346	37	,002	-,82349	,24611	-1,32215	-,32483
	Varianzgleichheit nicht angenommen			-3,175	22,809	,004	-,82349	,25940	-1,36034	-,28664
E-Mail	Varianzgleichheit angenommen	1,387	,247	1,442	36	,158	,28939	,20065	-,11756	,69633
	Varianzgleichheit nicht angenommen			1,470	33,904	,151	,28939	,19688	-,11077	,68955
Fitness	Varianzgleichheit angenommen	,531	,472	-,786	31	,438	-,32430	,41261	-1,16583	,51722
	Varianzgleichheit nicht angenommen			-,790	30,644	,436	-,32430	,41043	-1,16177	,51317
Nachrichten	Varianzgleichheit angenommen	,064	,802	-1,883	37	,068	-,57310	,30436	-1,18978	,04359
	Varianzgleichheit nicht angenommen			-1,874	35,291	,069	-,57310	,30585	-1,19383	,04764

Fortsetzung Tabelle 156

Test bei unabhängigen Stichproben										
	Vertrauenswürdigkeit Gruppe B und C	Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit					95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Wetter	Varianzgleichheit angenommen	,978	,329	-1,060	39	,296	-,29254	,27605	-,85090	,26582
	Varianzgleichheit nicht angenommen			-1,074	38,187	,290	-,29254	,27242	-,84394	,25887
E-Mail	Varianzgleichheit angenommen	,003	,957	-1,132	38	,265	-,32146	,28392	-,89623	,25330
	Varianzgleichheit nicht angenommen			-1,136	36,929	,263	-,32146	,28287	-,89465	,25172
Fitness	Varianzgleichheit angenommen	,442	,510	-,450	38	,655	-,12432	,27617	-,68340	,43475
	Varianzgleichheit nicht angenommen			-,444	32,708	,660	-,12432	,28014	-,69446	,44582

Fortsetzung Tabelle 156

		Test bei unabhängigen Stichproben								
	Vertrauenswürdigkeit Gruppe C und D	Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit					95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Wetter	Varianzgleichheit angenommen	,229	,635	-,872	39	,389	-,26357	,30244	-,87531	,34816
	Varianzgleichheit nicht angenommen			-,860	34,668	,396	-,26357	,30637	-,88574	,35859
E-Mail	Varianzgleichheit angenommen	3,974	,053	2,178	38	,036	,51980	,23866	,03665	1,00294
	Varianzgleichheit nicht angenommen			2,303	33,490	,028	,51980	,22569	,06088	,97872
Fitness	Varianzgleichheit angenommen	2,176	,149	-,712	37	,481	-,21704	,30504	-,83511	,40104
	Varianzgleichheit nicht angenommen			-,679	26,806	,503	-,21704	,31981	-,87346	,43938
Nachrichten	Varianzgleichheit angenommen	2,172	,149	-1,429	39	,161	-,38543	,26976	-,93107	,16020
	Varianzgleichheit nicht angenommen			-1,383	31,121	,177	-,38543	,27871	-,95377	,18291

Tabelle 157 *Korrelation zwischen der Technikaffinität und der Adäquatheit der angegebenen Vertrauenswürdigkeit*

		Spearman-Rho							
Technikaffinität		Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Erste Methode (Gestauchte Skala)	r	-,152	-,223	,012	,025	,000	-,028	-,082	,059
	Sig. (2-seitig)	,176	,051	,914	,831	,997	,816	,478	,600
	N	81	77	80	78	79	73	77	80
Zweite Methode (prozentuale Skala)	r	-,143	-,233*	-,024	,024	-,060	-,027	-,149	,028
	Sig. (2-seitig)	,202	,041	,834	,834	,602	,818	,195	,808
	N	81	77	80	78	79	73	77	80
Dritte Methode (dividierte Skala)	r	-,152	-,124	-,023	,017	-,057	-,038	-,149	,026
	Sig. (2-seitig)	,177	,271	,839	,880	,616	,751	,195	,820
	N	81	81	80	78	79	73	77	80

Tabelle 158 *Korrelation zwischen dem Alter und der Adäquatheit der angegebenen Vertrauenswürdigkeit*

		Spearman-Rho							
Alter		Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Erste Methode (Gestauchte Skala)	r	-,224*	-,200	-,159	,039	,200	-,210	,112	,001
	Sig. (2-seitig)	,044	,082	,160	,737	,078	,074	,334	,993
	N	81	77	80	78	79	73	77	80
Zweite Methode (prozentuale Skala)	r	-,202	-,177	-,167	,021	,157	-,181	,124	-,015
	Sig. (2-seitig)	,070	,123	,139	,855	,168	,126	,284	,892
	N	81	77	80	78	79	73	77	80
Dritte Methode (dividierte Skala)	r	-,205	-,141	-,158	,022	,163	-,186	,110	-,017
	Sig. (2-seitig)	,066	,210	,162	,851	,151	,115	,339	,878
	N	81	81	80	78	79	73	77	80

Tabelle 159 *Korrelation zwischen dem Geschlecht und der Adäquatheit der angegebenen Vertrauenswürdigkeit*

		Spearman-Rho							
Geschlecht		Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Erste Methode (Gestauchte Skala)	r	-,148	-,040	-,031	-,119	,009	-,070	-,283*	-,104
	Sig. (2-seitig)	,190	,731	,787	,304	,941	,558	,013	,360
	N	80	76	79	77	78	72	76	79
Zweite Methode (prozentuale Skala)	r	-,128	-,062	-,008	-,111	-,031	-,005	-,225	-,060
	Sig. (2-seitig)	,258	,596	,942	,338	,789	,968	,050	,600
	N	80	76	79	77	78	72	76	79
Dritte Methode (dividierte Skala)	r	-,138	-,085	-,011	-,107	-,035	-,017	-,238*	-,063
	Sig. (2-seitig)	,223	,452	,922	,353	,759	,888	,038	,580
	N	80	80	79	77	78	72	76	79

Tabelle 160 *Korrelation zwischen dem höchsten Bildungsabschluss und der Adäquatheit der angegebenen Vertrauenswürdigkeit*

		Spearman-Rho							
Höchster Bildungsabschluss		Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Erste Methode (Gestauchte Skala)	r	-,048	-,010	,005	,166	-,022	,009	,077	,071
	Sig. (2-seitig)	,673	,931	,962	,147	,847	,938	,507	,532
	N	81	77	80	78	79	73	77	80
Zweite Methode (prozentuale Skala)	r	-,015	,027	-,030	,121	-,016	-,012	,078	,077
	Sig. (2-seitig)	,894	,816	,788	,292	,892	,923	,502	,500
	N	81	77	80	78	79	73	77	80
Dritte Methode (dividierte Skala)	r	-,015	-,081	-,030	,130	-,016	-,001	,093	,085
	Sig. (2-seitig)	,895	,471	,793	,257	,886	,994	,421	,454
	N	81	81	80	78	79	73	77	80

Tabelle 161 *Korrelation zwischen dem Stunden der Handynutzung und der Adäquatheit der angegebenen Vertrauenswürdigkeit*

		Spearman-Rho							
Stunden Handynutzung		Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Erste Methode (Gestauchte Skala)	r	-,205	-,171	-,006	-,129	-,152	-,075	-,184	-,138
	Sig. (2-seitig)	,066	,136	,955	,259	,182	,526	,109	,223
	N	81	77	80	78	79	73	77	80
Zweite Methode (prozentuale Skala)	r	-,150	-,162	,018	-,096	-,147	-,010	-,180	-,143
	Sig. (2-seitig)	,180	,158	,873	,406	,197	,935	,118	,206
	N	81	77	80	78	79	73	77	80
Dritte Methode (dividierte Skala)	r	-,158	-,152	,002	-,106	-,155	-,028	-,201	-,137
	Sig. (2-seitig)	,158	,176	,985	,355	,172	,812	,080	,227
	N	81	81	80	78	79	73	77	80

Tabelle 162 *Korrelation zwischen der Privatsphäre und der Adäquatheit der angegebenen Vertrauenswürdigkeit*

		Spearman-Rho							
Privatsphäre		Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Erste Methode (Gestauchte Skala)	r	-,131	,005	,009	,159	,192	,112	,164	,113
	Sig. (2-seitig)	,242	,969	,936	,164	,091	,345	,154	,320
	N	81	77	80	78	79	73	77	80
Zweite Methode (prozentuale Skala)	r	-,095	,059	,004	,162	,182	,084	,167	,055
	Sig. (2-seitig)	,400	,609	,973	,156	,109	,480	,147	,630
	N	81	77	80	78	79	73	77	80
Dritte Methode (dividierte Skala)	r	-,116	,113	,008	,149	,183	,096	,167	,056
	Sig. (2-seitig)	,302	,316	,946	,192	,106	,420	,147	,622
	N	81	81	80	78	79	73	77	80

Tabelle 163 *Ergebnisse zur Messung der Bedenken von Mobilfunknutzern hinsichtlich des Datenschutzes (MUIPC)*

Aussage		trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu	Gesamtsumme
Standort wird überwacht.	Häufigkeit	1	4	1	7	10	30	29	82
	Prozent	1,2	4,9	1,2	8,5	12,2	36,6	35,4	100
Sammlung von zu vielen Daten.	Häufigkeit	1	4	11	6	24	18	18	82
	Prozent	1,2	4,9	13,4	7,3	29,3	22	22	100
Aktivitäten auf dem Endgerät werden überwacht.	Häufigkeit	1	3	17	5	21	18	17	82
	Prozent	1,2	3,7	20,7	6,1	25,6	22	20,7	100
Andere wissen mehr als ich will.	Häufigkeit	1	4	12	8	21	21	14	81
	Prozent	1,2	4,9	14,6	9,8	25,6	25,6	17,1	98,8
Informationen sind wegen der Nutzung von Apps für Dritte verfügbar.	Häufigkeit	1	2	7	12	29	15	16	82
	Prozent	1,2	2,4	8,5	14,6	35,4	18,3	19,5	100
Empfinden als Eindringen in Privatsphäre wenn Informationen über den Nutzenden verwendet werden.	Häufigkeit	0	3	9	9	26	19	15	81
	Prozent	0	3,7	11	11	31,7	23,2	18,3	98,8
Nutzung persönlicher Daten ohne Berechtigung oder Benachrichtigung.	Häufigkeit	1	3	9	11	14	27	16	81
	Prozent	1,2	3,7	11	13,4	17,1	32,9	19,5	98,8
Nutzung persönlicher Daten für andere Zwecke.	Häufigkeit	0	2	11	6	23	21	19	81
	Prozent	0	2,4	13,4	7,3	28	25,6	23,2	98,8
Nutzung persönlicher Daten durch andere Instanzen.	Häufigkeit	0	3	8	11	20	21	18	82
	Prozent	0	3,7	9,8	13,4	24,4	25,6	22	100
Offenlegung von persönlichen Informationen für die Nutzung einer Applikation.	Häufigkeit	3	4	5	8	23	26	12	81
	Prozent	3,7	4,9	6,1	9,8	28	31,7	14,6	98,8

Anmerkung. Ergebnisse zur Messung der Bedenken von Mobilfunknutzern hinsichtlich des Datenschutzes farblich in absteigend sortierter Rangfolge: orange, gelb, grün.

Tabelle 164 Ergebnisse zur Messung der Bedenken von Mobilfunknutzern hinsichtlich des Datenschutzes (MUIPC)

Aussage		**kein Mal**	**1 - 2 -mal**	**3 - 4 -mal**	**mehr als 5-mal**	**Gesamtsumme**
Häufigkeit der Vorfälle bei denen persönliche Daten ohne Genehmigung verwendet wurden (in den letzten 2 Jahren).	Häufigkeit	36	17	8	21	82
	Prozent	43,9	20,7	9,8	25,6	100
Häufigkeit des Hörens oder Lesens über die Verwendung und Missbrauch des Sammelns von Information.	Häufigkeit	4	11	17	50	82
	Prozent	4,9	13,4	20,7	61	100
Häufigkeit des Empfindens eines unangemessenen Eingriffs in die Privatsphäre (in den letzten 2 Jahren).	Häufigkeit	41	27	6	8	82
	Prozent	50	32,9	7,3	9,8	100

Tabelle 165 *Mittelwerte der Relevanz der Bewertungsmethoden einer Applikation für die Applikationsauswahl*

Deskriptive Statistiken																			
Relevanz	Gruppe A				Gruppe B				Gruppe C				Gruppe D				Gesamt		
	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV	N	M	SD	NV
Rezensionen	21	6,10	0,89	0,006	18	5,33	1,14	0,176	23	5,00	1,54	0,000	17	5,76	0,97	0,004	81	5,54	1,23	0
Sterne	21	5,29	1,38	0,006	18	5,50	0,86	0,021	23	5,13	1,42	0,001	17	5,76	1,09	0,015	81	5,37	1,25	0
Anzahl	21	4,29	1,65	0,147	18	4,83	1,62	0,042	23	4,09	1,44	0,200	17	3,71	1,45	0,200	81	4,26	1,56	0
Downloads	21	4,62	1,53	0,200	18	5,17	1,25	0,025	23	4,35	1,72	0,200	17	5,18	1,38	0,084	81	4,78	1,50	0
Datenschutzskala	21	5,86	1,11	0,005	18	5,72	1,02	0,001	23	5,30	1,41	0,000	17	5,94	1,20	0,022	79	5,68	1,20	0

Anmerkung. Mittelwerte der Relevanz der Bewertungsmethoden einer Applikation verglichen innerhalb der Gruppen farblich aufsteigend in folgender Reihenfolge markiert: rot, orange, gelb, grün. Die Datensätze, die eine Normalverteilung aufweisen, wurden rötlich markiert.

Tabelle 166 *Friedman-Test Vergleich der verschiedenen Applikationsbewertungsmethoden untereinander*

Ränge	
Aussage	Mittlerer Rang
Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	3,36
Ich halte die Sterne für sehr relevant.	3,27
Ich halte die Anzahl der Aufrufe für sehr relevant.	2,14
Ich halte die Anzahl der Downloads für sehr relevant.	2,61
Ich halte die Privatsphäreskala für sehr relevant.	3,61

Teststatistiken[a]	
H	79
Chi-Quadrat	60,352
df	4
Asymp. Sig.	,000

a. Friedman-Test

Tabelle 167 *Wilcoxon-Test paarweise Vergleich der verschiedenen Applikationsbewertungsmethoden untereinander*

Ränge					
Aussage		H	Mittlerer Rang	Summe der Ränge	
Ich halte die Sterne für sehr relevant. - Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	Negative Ränge	27[a]	25,72	694,50	a. Ich halte die Sterne für sehr relevant. < Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.
	Positive Ränge	21[b]	22,93	481,50	b. Ich halte die Sterne für sehr relevant. > Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.
	Bindungen	33[c]			c. Ich halte die Sterne für sehr relevant. = Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.
	Gesamtsumme	81			
Ich halte die Anzahl der Aufrufe für sehr relevant. - Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	Negative Ränge	50[d]	32,58	1629,00	d. Ich halte die Anzahl der Aufrufe für sehr relevant. < Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.
	Positive Ränge	9[e]	15,67	141,00	e. Ich halte die Anzahl der Aufrufe für sehr relevant. > Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.
	Bindungen	22[f]			f. Ich halte die Anzahl der Aufrufe für sehr relevant. = Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.
	Gesamtsumme	81			

Fortsetzung Tabelle 167

Aussage		H	Mittlerer Rang	Summe der Ränge	
Ich halte die Anzahl der Downloads für sehr relevant. - Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	Negative Ränge	45[g]	34,12	1535,50	g. Ich halte die Anzahl der Downloads für sehr relevant. < Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.
	Positive Ränge	17[h]	24,56	417,50	h. Ich halte die Anzahl der Downloads für sehr relevant. > Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.
	Bindungen	19[i]			i. Ich halte die Anzahl der Downloads für sehr relevant. = Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.
	Gesamtsumme	81			
Ich halte die Privatsphäreskala für sehr relevant. - Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	Negative Ränge	20[j]	32,05	641,00	j. Ich halte die Privatsphäreskala für sehr relevant. < Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.
	Positive Ränge	34[k]	24,82	844,00	k. Ich halte die Privatsphäreskala für sehr relevant. > Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.
	Bindungen	25[l]			l. Ich halte die Privatsphäreskala für sehr relevant. = Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.
	Gesamtsumme	79			
Ich halte die Anzahl der Aufrufe für sehr relevant. - Ich halte die Sterne für sehr relevant.	Negative Ränge	45[m]	30,10	1354,50	m. Ich halte die Anzahl der Aufrufe für sehr relevant. < Ich halte die Sterne für sehr relevant.
	Positive Ränge	10[n]	18,55	185,50	n. Ich halte die Anzahl der Aufrufe für sehr relevant. > Ich halte die Sterne für sehr relevant.
	Bindungen	26[o]			o. Ich halte die Anzahl der Aufrufe für sehr relevant. = Ich halte die Sterne für sehr relevant.
	Gesamtsumme	81			
Ich halte die Anzahl der Downloads für sehr relevant. - Ich halte die Sterne für sehr relevant.	Negative Ränge	38[p]	28,38	1078,50	p. Ich halte die Anzahl der Downloads für sehr relevant. < Ich halte die Sterne für sehr relevant.
	Positive Ränge	15[q]	23,50	352,50	q. Ich halte die Anzahl der Downloads für sehr relevant. > Ich halte die Sterne für sehr relevant.
	Bindungen	28[r]			r. Ich halte die Anzahl der Downloads für sehr relevant. = Ich halte die Sterne für sehr relevant.
	Gesamtsumme	81			
Ich halte die Privatsphäreskala für sehr relevant. - Ich halte die Sterne für sehr relevant.	Negative Ränge	23[s]	25,50	586,50	s. Ich halte die Privatsphäreskala für sehr relevant. < Ich halte die Sterne für sehr relevant.
	Positive Ränge	34[t]	31,37	1066,50	t. Ich halte die Privatsphäreskala für sehr relevant. > Ich halte die Sterne für sehr relevant.
	Bindungen	22[u]			u. Ich halte die Privatsphäreskala für sehr relevant. = Ich halte die Sterne für sehr relevant.
	Gesamtsumme	79			

Fortsetzung Tabelle 167

Aussage		H	Mittlerer Rang	Summe der Ränge	
Ich halte die Anzahl der Downloads für sehr relevant. - Ich halte die Anzahl der Aufrufe für sehr relevant.	Negative Ränge	11[v]	16,86	185,50	v. Ich halte die Anzahl der Downloads für sehr relevant. < Ich halte die Anzahl der Aufrufe für sehr relevant.
	Positive Ränge	28[w]	21,23	594,50	w. Ich halte die Anzahl der Downloads für sehr relevant. > Ich halte die Anzahl der Aufrufe für sehr relevant.
	Bindungen	42[x]			x. Ich halte die Anzahl der Downloads für sehr relevant. = Ich halte die Anzahl der Aufrufe für sehr relevant.
	Gesamtsumme	81			
Ich halte die Privatsphäreskala für sehr relevant. - Ich halte die Anzahl der Aufrufe für sehr relevant.	Negative Ränge	9[y]	17,17	154,50	y. Ich halte die Privatsphäreskala für sehr relevant. < Ich halte die Anzahl der Aufrufe für sehr relevant.
	Positive Ränge	51[z]	32,85	1675,50	z. Ich halte die Privatsphäreskala für sehr relevant. > Ich halte die Anzahl der Aufrufe für sehr relevant.
	Bindungen	19[aa]			aa. Ich halte die Privatsphäreskala für sehr relevant. = Ich halte die Anzahl der Aufrufe für sehr relevant.
	Gesamtsumme	79			
Ich halte die Privatsphäreskala für sehr relevant. - Ich halte die Anzahl der Downloads für sehr relevant.	Negative Ränge	15[ab]	22,63	339,50	ab. Ich halte die Privatsphäreskala für sehr relevant. < Ich halte die Anzahl der Downloads für sehr relevant.
	Positive Ränge	45[ac]	33,12	1490,50	ac. Ich halte die Privatsphäreskala für sehr relevant. > Ich halte die Anzahl der Downloads für sehr relevant.
	Bindungen	19[ad]			ad. Ich halte die Privatsphäreskala für sehr relevant. = Ich halte die Anzahl der Downloads für sehr relevant.
	Gesamtsumme	79			

Fortsetzung Tabelle 167

Teststatistiken[a]

	Ich halte die Sterne für sehr relevant. - Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	Ich halte die Anzahl der Aufrufe für sehr relevant. - Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	Ich halte die Anzahl der Downloads für sehr relevant. - Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	Ich halte die Privatsphäreskala für sehr relevant. - Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	Ich halte die Anzahl der Aufrufe für sehr relevant. - Ich halte die Sterne für sehr relevant.	Ich halte die Anzahl der Downloads für sehr relevant. - Ich halte die Sterne für sehr relevant.	Ich halte die Privatsphäreskala für sehr relevant. - Ich halte die Sterne für sehr relevant.	Ich halte die Anzahl der Downloads für sehr relevant. - Ich halte die Anzahl der Aufrufe für sehr relevant.	Ich halte die Privatsphäreskala für sehr relevant. - Ich halte die Anzahl der Aufrufe für sehr relevant.	Ich halte die Privatsphäreskala für sehr relevant. - Ich halte die Anzahl der Downloads für sehr relevant.
U	-1,153[b]	-5,681[b]	-4,003[b]	-,904[c]	-4,954[b]	-3,287[b]	-1,996[c]	-2,887[c]	-5,653[c]	-4,303[c]
Asymp. Sig. (2-seitig)	,249	,000	,000	,366	,000	,001	,046	,004	,000	,000

a. Wilcoxon-Test

b. Basierend auf positiven Rängen.

c. Basierend auf negativen Rängen.

Tabelle 168 *Kruskal-Wallis-Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen*

Ränge			
Aussage	Gruppe	H	Mittlerer Rang
Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	51,79
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	35,56
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	32,72
	D: Keine Datenschutzskala	19	44,26
	Gesamtsumme	81	
Ich halte die Sterne für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	40,21
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	40,97
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	37,67
	D: Keine Datenschutzskala	19	45,92
	Gesamtsumme	81	
Ich halte die Anzahl der Aufrufe für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	40,60
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	49,92
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	38,85
	D: Keine Datenschutzskala	19	35,61
	Gesamtsumme	81	
Ich halte die Anzahl der Downloads für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	38,19
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	46,89
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	35,13
	D: Keine Datenschutzskala	19	45,63
	Gesamtsumme	81	
Ich halte die Privatsphäreskala für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	42,76
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	39,67
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	33,72
	D: Keine Datenschutzskala	17	45,44
	Gesamtsumme	79	

Fortsetzung Tabelle 168

Teststatistiken[a,b]

	Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	Ich halte die Sterne für sehr relevant.	Ich halte die Anzahl der Aufrufe für sehr relevant.	Ich halte die Anzahl der Downloads für sehr relevant.	Ich halte die Privatsphäreskala für sehr relevant.
Chi-Quadrat	9,355	1,435	3,922	3,743	3,218
df	3	3	3	3	3
Asymp. Sig.	,025	,697	,270	,291	,359

a. Kruskal-Wallis-Test

b. Gruppierungsvariable: Gruppe

Tabelle 169 *Mann-Whitney-U-Test Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen A und B*

Ränge

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	23,50	493,50
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	15,92	286,50
	Gesamtsumme	39		
Ich halte die Sterne für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,86	417,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	20,17	363,00
	Gesamtsumme	39		
Ich halte die Anzahl der Aufrufe für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	18,05	379,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	22,28	401,00
	Gesamtsumme	39		

Fortsetzung Tabelle 169

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Ich halte die Anzahl der Downloads für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	18,00	378,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	22,33	402,00
	Gesamtsumme	39		
Ich halte die Privatsphäreskala für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	20,76	436,00
	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,11	344,00
	Gesamtsumme	39		

Teststatistiken[a]

	Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	Ich halte die Sterne für sehr relevant.	Ich halte die Anzahl der Aufrufe für sehr relevant.	Ich halte die Anzahl der Downloads für sehr relevant.	Ich halte die Privatsphäreskala für sehr relevant.
Mann-Whitney-U-Test	115,500	186,000	148,000	147,000	173,000
Wilcoxon-W	286,500	417,000	379,000	378,000	344,000
z	-2,155	-,089	-1,176	-1,210	-,469
Asymp. Sig. (2-seitig)	,031	,929	,240	,226	,639
Exakte Sig. [2*(1-seitige Sig.)]	,037[b]	,945[b]	,257[b]	,245[b]	,666[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 170 *Mann-Whitney-U-Test Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen A und C*

Ränge

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	27,93	586,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	17,54	403,50
	Gesamtsumme	44		
Ich halte die Sterne für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	23,19	487,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,87	503,00
	Gesamtsumme	44		
Ich halte die Anzahl der Aufrufe für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	22,98	482,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,07	507,50
	Gesamtsumme	44		
Ich halte die Anzahl der Downloads für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	23,45	492,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	21,63	497,50
	Gesamtsumme	44		
Ich halte die Privatsphäreskala für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	25,02	525,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,20	464,50
	Gesamtsumme	44		

Fortsetzung Tabelle 170

Teststatistiken[a]

	Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	Ich halte die Sterne für sehr relevant.	Ich halte die Anzahl der Aufrufe für sehr relevant.	Ich halte die Anzahl der Downloads für sehr relevant.	Ich halte die Privatsphäreskala für sehr relevant.
Mann-Whitney-U-Test	127,500	227,000	231,500	221,500	188,500
Wilcoxon-W	403,500	503,000	507,500	497,500	464,500
z	-2,798	-,357	-,239	-,478	-1,290
Asymp. Sig. (2-seitig)	,005	,721	,811	,633	,197

a. Gruppierungsvariable: Gruppe

Tabelle 171 *Mann-Whitney-U-Test Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen A und D*

Ränge

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	22,36	469,50
	D: Keine Datenschutzskala	19	18,45	350,50
	Gesamtsumme	40		
Ich halte die Sterne für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	19,17	402,50
	D: Keine Datenschutzskala	19	21,97	417,50
	Gesamtsumme	40		
Ich halte die Anzahl der Aufrufe für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	21,57	453,00
	D: Keine Datenschutzskala	19	19,32	367,00
	Gesamtsumme	40		

Fortsetzung Tabelle 171

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Ich halte die Anzahl der Downloads für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	18,74	393,50
	D: Keine Datenschutzskala	19	22,45	426,50
	Gesamtsumme	40		
Ich halte die Privatsphäreskala für sehr relevant.	A: Datenschutzskala mit einer detaillierten Beschreibung als Einführung	21	18,98	398,50
	D: Keine Datenschutzskala	17	20,15	342,50
	Gesamtsumme	38		

Teststatistiken[a]

	Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	Ich halte die Sterne für sehr relevant.	Ich halte die Anzahl der Aufrufe für sehr relevant.	Ich halte die Anzahl der Downloads für sehr relevant.	Ich halte die Privatsphäreskala für sehr relevant.
Mann-Whitney-U-Test	160,500	171,500	177,000	162,500	167,500
Wilcoxon-W	350,500	402,500	367,000	393,500	398,500
z	-1,112	-,788	-,621	-1,022	-,338
Asymp. Sig. (2-seitig)	,266	,431	,534	,307	,735
Exakte Sig. [2*(1-seitige Sig.)]	,294[b]	,452[b]	,555[b]	,320[b]	,750[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 172 *Mann-Whitney-U-Test Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen B und C*

Ränge				
Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	21,75	391,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,41	469,50
	Gesamtsumme	41		
Ich halte die Sterne für sehr relevant.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	21,97	395,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	20,24	465,50
	Gesamtsumme	41		
Ich halte die Anzahl der Aufrufe für sehr relevant.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	24,25	436,50
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,46	424,50
	Gesamtsumme	41		
Ich halte die Anzahl der Downloads für sehr relevant.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	24,28	437,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,43	424,00
	Gesamtsumme	41		
Ich halte die Privatsphäreskala für sehr relevant.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	22,89	412,00
	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,52	449,00
	Gesamtsumme	41		

Fortsetzung Tabelle 172

Teststatistiken[a]					
	Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	Ich halte die Sterne für sehr relevant.	Ich halte die Anzahl der Aufrufe für sehr relevant.	Ich halte die Anzahl der Downloads für sehr relevant.	Ich halte die Privatsphäreskala für sehr relevant.
Mann-Whitney-U-Test	193,500	189,500	148,500	148,000	173,000
Wilcoxon-W	469,500	465,500	424,500	424,000	449,000
z	-,371	-,484	-1,566	-1,585	-,930
Asymp. Sig. (2-seitig)	,711	,628	,117	,113	,353

a. Gruppierungsvariable: Gruppe

Tabelle 173 *Mann-Whitney-U-Test Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen C und D*

Ränge				
Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,76	431,50
	D: Keine Datenschutzskala	19	24,82	471,50
	Gesamtsumme	42		
Ich halte die Sterne für sehr relevant.	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,57	450,00
	D: Keine Datenschutzskala	19	23,84	453,00
	Gesamtsumme	42		
Ich halte die Anzahl der Aufrufe für sehr relevant.	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	22,33	513,50
	D: Keine Datenschutzskala	19	20,50	389,50
	Gesamtsumme	42		
Ich halte die Anzahl der Downloads für sehr relevant.	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	19,07	438,50
	D: Keine Datenschutzskala	19	24,45	464,50
	Gesamtsumme	42		
Ich halte die Privatsphäreskala für sehr relevant.	C: Datenschutzskala ohne eine detaillierte Beschreibung	23	18,00	414,00
	D: Keine Datenschutzskala	17	23,88	406,00
	Gesamtsumme	40		

Fortsetzung Tabelle 173

Teststatistiken[a]

	Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	Ich halte die Sterne für sehr relevant.	Ich halte die Anzahl der Aufrufe für sehr relevant.	Ich halte die Anzahl der Downloads für sehr relevant.	Ich halte die Privatsphäreskala für sehr relevant.
Mann-Whitney-U-Test	155,500	174,000	199,500	162,500	138,000
Wilcoxon-W	431,500	450,000	389,500	438,500	414,000
z	-1,678	-1,173	-,490	-1,442	-1,630
Asymp. Sig. (2-seitig)	,093	,241	,624	,149	,103
Exakte Sig. [2*(1-seitige Sig.)]					,120[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 174 *Mann-Whitney-U-Test Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen B und D*

Ränge

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	16,89	304,00
	D: Keine Datenschutzskala	19	21,00	399,00
	Gesamtsumme	37		
Ich halte die Sterne für sehr relevant.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	17,83	321,00
	D: Keine Datenschutzskala	19	20,11	382,00
	Gesamtsumme	37		

Fortsetzung Tabelle 174

Aussage	Gruppe	H	Mittlerer Rang	Summe der Ränge
Ich halte die Anzahl der Aufrufe für sehr relevant.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	22,39	403,00
	D: Keine Datenschutzskala	19	15,79	300,00
	Gesamtsumme	37		
Ich halte die Anzahl der Downloads für sehr relevant.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	19,28	347,00
	D: Keine Datenschutzskala	19	18,74	356,00
	Gesamtsumme	37		
Ich halte die Privatsphäreskala für sehr relevant.	B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch Klicken auf die Datenschutzskala	18	16,67	300,00
	D: Keine Datenschutzskala	17	19,41	330,00
	Gesamtsumme	35		

Teststatistiken[a]

	Ich halte die Rezensionen (Einzelbewertungen) für sehr relevant.	Ich halte die Sterne für sehr relevant.	Ich halte die Anzahl der Aufrufe für sehr relevant.	Ich halte die Anzahl der Downloads für sehr relevant.	Ich halte die Privatsphäreskala für sehr relevant.
Mann-Whitney-U-Test	155,500	174,000	199,500	162,500	138,000
Wilcoxon-W	431,500	450,000	389,500	438,500	414,000
z	-1,678	-1,173	-,490	-1,442	-1,630
Asymp. Sig. (2-seitig)	,093	,241	,624	,149	,103
Exakte Sig. [2*(1-seitige Sig.)]					,120[b]

a. Gruppierungsvariable: Gruppe

b. Nicht für Bindungen korrigiert.

Tabelle 175 *T-Test Vergleich verschiedenen Applikationsbewertungsmethoden zwischen den Gruppen*

Test bei unabhängigen Stichproben										
Gruppe A und D		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit					95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Ich halte die Anzahl der Aufrufe für sehr relevant.	Varianzgleichheit angenommen	,775	,384	,427	42	,672	,199	,466	-,742	1,139
	Varianzgleichheit nicht angenommen			,424	39,996	,674	,199	,469	-,749	1,146
Ich halte die Anzahl der Downloads für sehr relevant.	Varianzgleichheit angenommen	,310	,581	,550	42	,585	,271	,493	-,724	1,267
	Varianzgleichheit nicht angenommen			,553	41,977	,583	,271	,491	-,719	1,261

Fortsetzung Tabelle 175

Gruppe A und D		Test bei unabhängigen Stichproben								
		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Ich halte die Anzahl der Aufrufe für sehr relevant.	Varianzgleichheit angenommen	,535	,469	,785	38	,437	,391	,498	-,618	1,399
	Varianzgleichheit nicht angenommen			,789	38,000	,435	,391	,496	-,612	1,394
Ich halte die Anzahl der Downloads für sehr relevant.	Varianzgleichheit angenommen	,555	,461	-1,067	38	,293	-,486	,456	-1,409	,436
	Varianzgleichheit nicht angenommen			-1,075	37,941	,289	-,486	,452	-1,402	,430

Fortsetzung Tabelle 175

Gruppe C und D		Test bei unabhängigen Stichproben								
		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Ich halte die Anzahl der Aufrufe für sehr relevant.	Varianzgleichheit angenommen	,009	,925	,424	40	,674	,192	,454	-,724	1,109
	Varianzgleichheit nicht angenommen			,423	38,061	,675	,192	,455	-,729	1,113
Ich halte die Anzahl der Downloads für sehr relevant.	Varianzgleichheit angenommen	1,588	,215	-1,569	40	,125	-,757	,483	-1,733	,218
	Varianzgleichheit nicht angenommen			-1,608	39,845	,116	-,757	,471	-1,709	,195

Fortsetzung Tabelle 175

Gruppe C und D		Test bei unabhängigen Stichproben								
		Levene-Test der Varianzgleichheit		T-Test für die Mittelwertgleichheit						
									95 % Konfidenzintervall der Differenz	
		F	Sig.	t	df	Sig. (2-seitig)	Mittelwertdifferenz	Standardfehlerdifferenz	Unterer	Oberer
Ich halte die Anzahl der Aufrufe für sehr relevant.	Varianzgleichheit angenommen	,024	,879	1,839	35	,074	,939	,510	-,098	1,975
	Varianzgleichheit nicht angenommen			1,835	34,330	,075	,939	,512	-,101	1,978
Ich halte die Anzahl der Downloads für sehr relevant.	Varianzgleichheit angenommen	,184	,671	,145	35	,886	,061	,424	-,800	,923
	Varianzgleichheit nicht angenommen			,145	34,998	,886	,061	,424	-,799	,922

Tabelle 176 *Angemessenheit der Applikationsauswahl (Datenschutzscore)*

Score	N	M	SD	NV (p)
Messenger	62	3,63	1,24	0,26
Videokonferenz	62	2,89	1,04	0,141
Wetter	62	4,08	0,68	0,003
E-Mail	62	3,66	1,13	0,008
Musik	62	4,19	0,67	0
Fitness	61	4,59	0,92	0
Spiele	62	4,45	0,99	0
Nachrichten	62	4,44	1,21	0
MUIPC				
Standort wird überwacht.	62	7,00	1,531	0
Sammlung von zu vielen Daten.	62	5,08	1,571	0
Aktivitäten auf dem Endgerät werden überwacht.	62	4,87	1,542	0
Andere wissen mehr als ich will.	62	4,87	1,624	0
Informationen sind wegen der Nutzung von Apps für Dritte verfügbar.	62	5,00	1,391	0
Empfinden als Eindringen in Privatsphäre wenn Informationen über die Nutzenden verwendet werden.	62	5,08	1,359	0
Nutzung persönlicher Daten ohne Berechtigung oder Benachrichtigung.	61	5,16	1,393	0
Nutzung persönlicher Daten für andere Zwecke.	62	5,29	1,335	0
Nutzung persönlicher Daten durch andere Instanzen.	61	5,25	1,337	0
Offenlegung von persönlichen Informationen für die Nutzung einer Applikation.	61	5,07	1,459	0
Häufigkeit der Vorfälle bei denen persönliche Daten ohne Genehmigung verwendet wurden (in den letzten 2 Jahren).	62	1,94	1,143	0
Häufigkeit des Hörens oder Lesens über die Verwendung und Missbrauch des Sammelns von Information.	62	3,34	,904	0
Häufigkeit des Empfindens eines unangemessenen Eingriffs in der Privatsphäre (in den letzten 2 Jahren).	62	1,76	,953	0

Tabelle 177 *Spearman-Rho-Test zwischen den Datenschutzscore der Scenarios und des MUIPCs*

		Spearman-Rho							
		Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Standort wird überwacht.	r	,023	,077	,158	,255*	-,302*	,060	,230	,156
	Sig. (2-seitig)	,860	,551	,221	,046	,017	,648	,072	,227
	N	62	62	62	62	62	61	62	62
Sammlung von zu vielen Daten.	r	-,122	,012	,054	,208	,065	-,135	,036	,146
	Sig. (2-seitig)	,347	,928	,675	,105	,618	,300	,781	,257
	N	62	62	62	62	62	61	62	62
Aktivitäten auf dem Endgerät werden überwacht.	r	-,043	,121	,157	,218	,025	-,009	,057	,266*
	Sig. (2-seitig)	,741	,347	,223	,089	,849	,943	,658	,037
	N	62	62	62	62	62	61	62	62
Andere wissen mehr als ich will.	r	-,094	,240	,108	,287*	-,079	-,122	,007	,113
	Sig. (2-seitig)	,468	,061	,403	,024	,544	,348	,959	,383
	N	62	62	62	62	62	61	62	62
Informationen sind wegen der Nutzung von Apps für Dritte verfügbar.	r	-,094	,111	,129	,186	-,101	-,145	,078	,059
	Sig. (2-seitig)	,467	,392	,319	,149	,436	,264	,545	,647
	N	62	62	62	62	62	61	62	62
Empfinden als Eindringen in Privatsphäre wenn Informationen über die Nutzenden verwendet werden.	r	-,067	,164	,146	,323*	-,101	-,153	,103	,143
	Sig. (2-seitig)	,607	,204	,258	,010	,435	,239	,425	,269
	N	62	62	62	62	62	61	62	62
Nutzung persönlicher Daten ohne Berechtigung oder Benachrichtigung.	r	,069	,223	,182	,344**	-,105	,078	-,064	,194
	Sig. (2-seitig)	,597	,085	,161	,007	,420	,554	,625	,134
	N	61	61	61	61	61	60	61	61
Nutzung persönlicher Daten für andere Zwecke.	r	-,081	,267*	,178	,315*	,030	-,105	,061	,134
	Sig. (2-seitig)	,530	,036	,167	,013	,819	,420	,639	,298
	N	62	62	62	62	62	61	62	62
Nutzung persönlicher Daten durch andere Instanzen.	r	-,158	,151	,081	,316*	-,062	-,083	,084	-,024
	Sig. (2-seitig)	,223	,244	,536	,013	,633	,526	,520	,854
	N	61	61	61	61	61	60	61	61
Offenlegung von persönlichen Informationen für die Nutzung einer Applikation.	r	,023	,085	-,144	,077	-,216	,141	,099	,004
	Sig. (2-seitig)	,863	,513	,267	,553	,095	,282	,449	,973
	N	61	61	61	61	61	60	61	61

Fortsetzung Tabelle 177

		Messenger	Videokonferenz	Wetter	E-Mail	Musik	Fitness	Spiele	Nachrichten
Häufigkeit der Vorfälle bei denen persönliche Daten ohne Genehmigung verwendet wurden (in den letzten 2 Jahren).	r	,095	-,088	-,067	,170	-,107	,044	,184	,097
	Sig. (2-seitig)	,462	,498	,605	,187	,408	,737	,152	,451
	N	62	62	62	62	62	61	62	62
Häufigkeit des Hörens oder Lesens über die Verwendung und Missbrauch des Sammelns von Information.	r	-,120	,072	,025	-,076	-,073	,344**	,138	,116
	Sig. (2-seitig)	,352	,579	,850	,555	,573	,007	,286	,371
	N	62	62	62	62	62	61	62	62
Häufigkeit der Vorfälle bei denen persönliche Daten ohne Genehmigung verwendet wurden (in den letzten 2 Jahren).	r	,116	,018	,075	,173	,062	,027	,102	,099
	Sig. (2-seitig)	,370	,891	,562	,180	,630	,839	,431	,444
	N	62	62	62	62	62	61	62	62

**. Korrelation ist bei Niveau 0,01 signifikant (zweiseitig).
*. Korrelation ist bei Niveau 0,05 signifikant (zweiseitig).

(Z.527-549)

Anhang Z. Entscheidungsmotive für die Auswahl der Applikationen

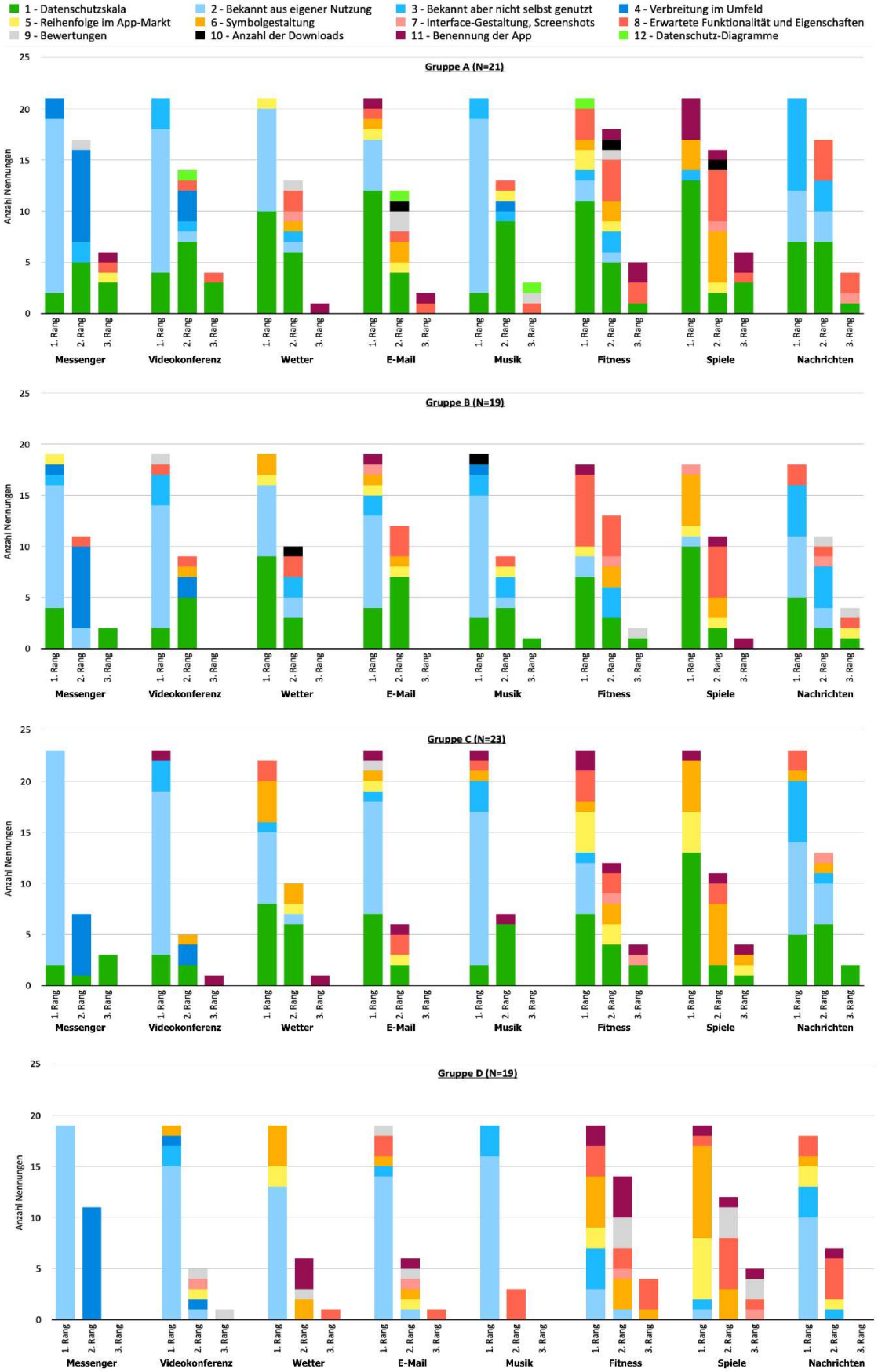


Abbildung 38 Entscheidungsmotive in den ursprünglichen Gruppe A-D des Laborexperimentes

Anhang AA. Variablen zum zweiten Versuch

1. Indicator
2. Gruppe
3. Reihenfolge
4. CH_Messenger
5. CH_Videoconference
6. CH_Weather
7. CH_EMail
8. CH_Music
9. CH_Fittness
10. CH_Games
11. CH_News
12. Versuchspersonennummer
13. CH_VAPP_Messenger_Installiert_Verwendet
14. CH_VAPP_Videoconference_Installiert_Verwendet
15. CH_VAPP_Weather_Installiert_Verwendet
16. CH_VAPP_EMail_Installiert_Verwendet
17. CH_VAPP_Music_Installiert_Verwendet
18. CH_VAPP_Fitness_Installiert_Verwendet
19. CH_VAPP_Games_Installiert_Verwendet
20. CH_VAPP_News_Installiert_Verwendet
21. CH_Messenger_Score
22. CH_Videoconference_Score
23. CH_Weather_Score
24. CH_EMail_Score
25. CH_Music_Score
26. CH_Fittness_Score
27. CH_Games_Score
28. CH_News_Score
29. VAPP_Whatsapp_Installiert_Verwendet
30. VAPP_BiPMessenger_Installiert_Verwendet
31. VAPP_Threema_Installiert_Verwendet
32. VAPP_Signal_Installiert_Verwendet
33. VAPP_FacebookMessenger_Installiert_Verwendet
34. VAPP_Wire_Installiert_Verwendet
35. VAPP_Kik_Installiert_Verwendet
36. VAPP_MessengerForbis_Installiert_Verwendet
37. VAPP_Telegram_Installiert_Verwendet
38. VAPP_Hangouts_Installiert_Verwendet
39. VAPP_Line_Installiert_Verwendet
40. VAPP_Skype_Installiert_Verwendet
41. VAPP_GoogleDuo_Installiert_Verwendet
42. VAPP_TrueConf_Installiert_Verwendet
43. VAPP_JusTalk_Installiert_Verwendet
44. VAPP_Glide_Installiert_Verwendet
45. VAPP_Zoom_Installiert_Verwendet
46. VAPP_VideoCall_Installiert_Verwendet
47. VAPP_Imo_Installiert_Verwendet
48. VAPP_Tango_Installiert_Verwendet
49. VAPP_Viber_Installiert_Verwendet
50. VAPP_AccuWeather_Installiert_Verwendet
51. VAPP_Yr_Installiert_Verwendet
52. VAPP_WetterOnline_Installiert_Verwendet
53. VAPP_BayerAgrarWetter_Installiert_Verwendet
54. VAPP_WeatherLiveInnovativeTeam_Installiert_Verwendet
55. VAPP_YahooWetter_Installiert_Verwendet
56. VAPP_MorecastUBIMET_Installiert_Verwendet
57. VAPP_wetter.com_Installiert_Verwendet
58. VAPP_Windy_Installiert_Verwendet
59. VAPP_Weatherzone_Installiert_Verwendet
60. VAPP_MicrosoftOutlook_Installiert_Verwendet
61. VAPP_K9Mail_Installiert_Verwendet
62. VAPP_myMail_Installiert_Verwendet
63. VAPP_Nine_Installiert_Verwendet
64. VAPP_BlueMail_Installiert_Verwendet
65. VAPP_MailDroid_Installiert_Verwendet
66. VAPP_EMailfürOutlookundandere_Installiert_Verwendet
67. VAPP_OpenMail_Installiert_Verwendet
68. VAPP_PlayMusik_Installiert_Verwendet
69. VAPP_FreeMusicPlayer_Installiert_Verwendet
70. VAPP_SongFlipFreeMusicStreamingampPlayer_Installiert_Verwendet
71. VAPP_Deezer_Installiert_Verwendet
72. VAPP_SoundCloud_Installiert_Verwendet
73. VAPP_Spotify_Installiert_Verwendet
74. VAPP_FreieMusikMHMusik_Installiert_Verwendet
75. VAPP_GratisMusikFreeMusic_Installiert_Verwendet

76. VAPP_AudiomackMusikundMixtapes_Installiert_Verwendet
77. VAPP_Musikspieler_Installiert_Verwendet
78. VAPP_SchrittzählerGratisPedometerampKalorienz._Installiert_Ver
79. VAPP_PacerHealthSchrittzählerampAbnehmtrainer_Installiert_Verw
80. VAPP_GoogleFit_Installiert_Verwendet
81. VAPP_Endomondo_Installiert_Verwendet
82. VAPP_Fitbit_Installiert_Verwendet
83. VAPP_WandernSchrittzählerDiät_Installiert_Verwendet
84. VAPP_StravaTraining_Installiert_Verwendet
85. VAPP_LaufenzurGewichtsabnahme_Installiert_Verwendet
86. VAPP_Sportractiveworkout_Installiert_Verwendet
87. VAPP_Sudoku2MagmaMobile_Installiert_Verwendet
88. VAPP_SudokuclassicQuarzoApps_Installiert_Verwendet
89. VAPP_SudokuVolcanoEntertainment_Installiert_Verwendet
90. VAPP_SudokuCardGames_Installiert_Verwendet
91. VAPP_SudokuFreeTitanIncGeduldsspiele_Installiert_Verwendet
92. VAPP_SudokuFreeJigsawPuzzleFree_Installiert_Verwendet
93. VAPP_SudokuTimeglassWorks_Installiert_Verwendet
94. VAPP_MaterialSudokuOkayCode_Installiert_Verwendet
95. VAPP_SudokuMasterDatVietEntertainment_Installiert_Verwendet
96. VAPP_SudokukostenlosdeutschMarcoMeyer_Installiert_Verwendet
97. VAPP_FlipBoard_Installiert_Verwendet
98. VAPP_bbcNews_Installiert_Verwendet
99. VAPP_CNNBreakingNews_Installiert_Verwendet
100. VAPP_NewsSuite_Installiert_Verwendet
101. VAPP_SQUID_Installiert_Verwendet
102. VAPP_Euronews_Installiert_Verwendet
103. VAPP_RTNews_Installiert_Verwendet
104. VAPP_DieZeit_Installiert_Verwendet
105. VAPP_Googlenews_Installiert_Verwendet
106. VAPP_MicrosoftNews_Installiert_Verwendet
107. APP_EinfachheitDerAuswahl_Messenger
108. APP_Vertrauenswürdigkeit_Messenger
109. APP_EinfachheitDerAuswahl_Videoconference
110. APP_Vertrauenswürdigkeit_Videoconference
111. APP_EinfachheitDerAuswahl_Weather
112. APP_Vertrauenswürdigkeit_Weather
113. APP_EinfachheitDerAuswahl_Email
114. APP_Vertrauenswürdigkeit_Email
115. APP_EinfachheitDerAuswahl_Music
116. APP_Vertrauenswürdigkeit_Music
117. APP_EinfachheitDerAuswahl_Fitness
118. APP_Vertrauenswürdigkeit_Fitness
119. APP_EinfachheitDerAuswahl_Games
120. APP_Vertrauenswürdigkeit_Games
121. APP_EinfachheitDerAuswahl_News
122. APP_Vertrauenswürdigkeit_News
123. APP_5S_Vertrauenswürdigkeit_Messenger
124. APP_5S_Vertrauenswürdigkeit_Videoconference
125. APP_5S_Vertrauenswürdigkeit_Weather
126. APP_5S_Vertrauenswürdigkeit_Email
127. APP_5S_Vertrauenswürdigkeit_Music
128. APP_5S_Vertrauenswürdigkeit_Fitness
129. APP_5S_Vertrauenswürdigkeit_News
130. APP_5S_Vertrauenswürdigkeit_Games
131. DIF_APP_5S_Vertrauenswürdigkeit_Messenger
132. DIF_APP_5S_Vertrauenswürdigkeit_Videoconference
133. DIF_APP_5S_Vertrauenswürdigkeit_Weather
134. DIF_APP_5S_Vertrauenswürdigkeit_Email
135. DIF_APP_5S_Vertrauenswürdigkeit_Music
136. DIF_APP_5S_Vertrauenswürdigkeit_Fitness

137. DIF_APP_5S_Vertrauenswürdigkeit_Games
138. DIF_APP_5S_Vertrauenswürdigkeit_News
139. BET_DIF_APP_5S_Vertrauenswürdigkeit_Messenger
140. BET_DIF_APP_5S_Vertrauenswürdigkeit_Videoconference
141. BET_DIF_APP_5S_Vertrauenswürdigkeit_Weather
142. BET_DIF_APP_5S_Vertrauenswürdigkeit_Email
143. BET_DIF_APP_5S_Vertrauenswürdigkeit_Music
144. BET_DIF_APP_5S_Vertrauenswürdigkeit_Fitness
145. BET_DIF_APP_5S_Vertrauenswürdigkeit_Games
146. BET_DIF_APP_5S_Vertrauenswürdigkeit_News
147. DIF_APP_prozentual_Vertrauenswürdigkeit_Messenger
148. DIF_APP_prozentual_Vertrauenswürdigkeit_Videocongerence
149. DIF_APP_prozentual_Vertrauenswürdigkeit_Weather
150. DIF_APP_prozentual_Vertrauenswürdigkeit_Email
151. DIF_APP_prozentual_Vertrauenswürdigkeit_Music
152. DIF_APP_prozentual_Vertrauenswürdigkeit_Fitness
153. DIF_APP_prozentual_Vertrauenswürdigkeit_Games
154. DIF_APP_prozentual_Vertrauenswürdigkeit_News
155. BET_DIF_APP_prozentual_Vertrauenswürdigkeit_Messenger
156. BET_DIF_APP_prozentual_Vertrauenswürdigkeit_Videocongerence
157. BET_DIF_APP_prozentual_Vertrauenswürdigkeit_Weather
158. BET_DIF_APP_prozentual_Vertrauenswürdigkeit_Email
159. BET_DIF_APP_prozentual_Vertrauenswürdigkeit_Music
160. BET_DIF_APP_prozentual_Vertrauenswürdigkeit_Fitness
161. BET_DIF_APP_prozentual_Vertrauenswürdigkeit_Games
162. BET_DIF_APP_prozentual_Vertrauenswürdigkeit_News
163. DIF_APP_5durch7_Vertrauenswürdigkeit_Messenger
164. DIF_APP_5durch7_Vertrauenswürdigkeit_Videoconference
165. DIF_APP_5durch7_Vertrauenswürdigkeit_Weather
166. DIF_APP_5durch7_Vertrauenswürdigkeit_Email
167. DIF_APP_5durch7_Vertrauenswürdigkeit_Music
168. DIF_APP_5durch7_Vertrauenswürdigkeit_Fitness
169. DIF_APP_5durch7_Vertrauenswürdigkeit_Games
170. DIF_APP_5durch7_Vertrauenswürdigkeit_News
171. BET_DIF_APP_5durch7_Vertrauenswürdigkeit_Messenger
172. BET_DIF_APP_5durch7_Vertrauenswürdigkeit_Videoconference
173. BET_DIF_APP_5durch7_Vertrauenswürdigkeit_Weather
174. BET_DIF_APP_5durch7_Vertrauenswürdigkeit_Email
175. BET_DIF_APP_5durch7_Vertrauenswürdigkeit_Music
176. BET_DIF_APP_5durch7_Vertrauenswürdigkeit_Fitness
177. BET_DIF_APP_5durch7_Vertrauenswürdigkeit_Games
178. BET_DIF_APP_5durch7_Vertrauenswürdigkeit_News
179. SR_vertrauenswürdig
180. SR_gut
181. SR_verständlich
182. SR_intuitiv
183. SR_gültig
184. SR_zuverlässig
185. SR_AuswirkungenApplikationsauswhal
186. SR_verwirrend
187. SR_InformationenNichtGenug
188. SR_erhöhtPrivatsphäregefühl
189. SR_möchteSkalaInAppMarkt
190. SR_komplex
191. SR_aktivieren
192. SR_ErhöhungApplikationsVertrauenswürdigkeit
193. SR_Verbesserungsvorschläge
194. MUIPC_StandortÜberwacht
195. MUIPC_SammlungZuVielerDaten
196. MUIPC_AktivitätenÜberwacht
197. MUIPC_AndereWissenMehrAlsIchWill
198. MUIPC_InformationenFürAndereVerfügbarWegenAppNutzung
199. MUIPC_EindringenInPrivatsphäreWennInfosGenutztWerden
200. MUIPC_DatennutzungOhneBerechtigung
201. MUIPC_DatennutzungFürAndereZwecke
202. MUIPC_DatennutzungDurchAndereInstanzen
203. MUIPC_OffenlegungVonInfosFürAppnutzung

204. MUIPC_HäufigkeitDatennutzungOhneEinwilligung
205. MUIPC_GehörtGelesenVonDatenmissbrauch
206. MUIPC_Opfer2Jahre
207. DEM_Geschlecht
208. DEM_Alter
209. DEM_HöchsterBildungsabschluss
210. DEM_HöchsterBildungsabschluss_Sonstiges
211. DEM_Technikaffinität
212. DEM_StundenHandyNutzung
213. PVC_PrivatsphäreIstWichtig
214. PVC_AktiverDatenschutz_Nein
215. PVC_AktiverDatenschut_Ja
216. PVC_AktiverDatenschut_ApplikationZumDatenschutzInstalliert
217. PVC_AktiverDatenschut_VersucheSoWenigWieMöglichPreiszugeben
218. PVC_AktiverDatenschut_LeseAGBVorInstallation
219. PVC_AktiverDatenschut_Sonstiges
220. RELEVANZ_Rezensionen
221. RELEVANZ_Sterne
222. RELEVANZ_Anzahl
223. RELEVANZ_Downloads
224. RELEVANZ_Privatsphäreskala
225. EV_Videoauswertung
226. EV_1Messenger_AnzahlWechsel_kein_Signal
227. EV_1Messenger_AnzahlWechsel_Eingabe
228. EV_1Messenger_AnzahlWechsel_Symbol
229. EV_1Messenger_AnzahlWechsel_Text
230. EV_1Messenger_AnzahlWechsel_Skala
231. EV_1Messenger_AnzahlWechsel_Leerlauf
232. EV_1Messenger_AnzahlWechsel_Suchzeile
233. EV_1Messenger_AnzahlWechsel_Zurücktaste
234. EV_1Messenger_AnzahlWechsel_Apptaste
235. EV_1Messenger_AnzahlWechsel_Hometaste
236. EV_1Messenger_AnzahlWechsel_Tastatur
237. EV_1Messenger_AnzahlWechsel_Diagramm
238. EV_1Messenger_AnzahlWechsel_AuswahlApp
239. EV_1Messenger_AnzahlWechsel_Bilder
240. EV_1Messenger_AnzahlWechsel_RezensionBerwertung
241. EV_1Messenger_AnzahlWechsel_Rest
242. EV_1Messenger_Frames_kein_Signal
243. EV_1Messenger_Frames_Eingabe
244. EV_1Messenger_Frames_Symbol
245. EV_1Messenger_Frames_Text
246. EV_1Messenger_Frames_Skala
247. EV_1Messenger_Frames_Leerlauf
248. EV_1Messenger_Frames_Suchzeile
249. EV_1Messenger_Frames_Zurücktaste
250. EV_1Messenger_Frames_Apptaste
251. EV_1Messenger_Frames_Hometaste
252. EV_1Messenger_Frames_Tastatur
253. EV_1Messenger_Frames_Diagramm
254. EV_1Messenger_Frames_AuswahlApp
255. EV_1Messenger_Frames_Bilder
256. EV_1Messenger_Frames_RezensionBerwertung
257. EV_1Messenger_Frames_Rest
258. EV_1Messenger_ZeitinS_kein_Signal
259. EV_1Messenger_ZeitinS_Eingabe
260. EV_1Messenger_ZeitinS_Symbol
261. EV_1Messenger_ZeitinS_Text
262. EV_1Messenger_ZeitinS_Skala
263. EV_1Messenger_ZeitinS_Leerlauf
264. EV_1Messenger_ZeitinS_Suchzeile
265. EV_1Messenger_ZeitinS_Zurücktaste
266. EV_1Messenger_ZeitinS_Apptaste
267. EV_1Messenger_ZeitinS_Hometaste
268. EV_1Messenger_ZeitinS_Tastatur
269. EV_1Messenger_ZeitinS_Diagramm
270. EV_1Messenger_ZeitinS_AuswahlApp
271. EV_1Messenger_ZeitinS_Bilder
272. EV_1Messenger_ZeitinS_RezensionBerwertung
273. EV_1Messenger_ZeitinS_Rest
274. EV_1Messenger_zeitAnteilEntscheidung_Symbol
275. EV_1Messenger_zeitAnteilEntscheidung_Text
276. EV_1Messenger_zeitAnteilEntscheidung_Skala
277. EV_1Messenger_zeitAnteilEntscheidung_Leerlauf
278. EV_1Messenger_zeitAnteilEntscheidung_Suchzeile
279. EV_1Messenger_zeitAnteilEntscheidung_Zurücktaste
280. EV_1Messenger_zeitAnteilEntscheidung_Apptaste
281. EV_1Messenger_zeitAnteilEntscheidung_Hometaste

282. EV_1Messenger_zeitAnteilEntscheidung_Tastatur
283. EV_1Messenger_zeitAnteilEntscheidung_Diagramm
284. EV_1Messenger_zeitAnteilEntscheidung_Bilder
285. EV_1Messenger_zeitAnteilEntscheidung_RezensionBerwertung
286. EV_1Messenger_zeitAnteilGesamt_kein_Signal
287. EV_1Messenger_zeitAnteilGesamt_Eingabe
288. EV_1Messenger_zeitAnteilGesamt_Symbol
289. EV_1Messenger_zeitAnteilGesamt_Text
290. EV_1Messenger_zeitAnteilGesamt_Skala
291. EV_1Messenger_zeitAnteilGesamt_Leerlauf
292. EV_1Messenger_zeitAnteilGesamt_Suchzeile
293. EV_1Messenger_zeitAnteilGesamt_Zurücktaste
294. EV_1Messenger_zeitAnteilGesamt_Apptaste
295. EV_1Messenger_zeitAnteilGesamt_Hometaste
296. EV_1Messenger_zeitAnteilGesamt_Tastatur
297. EV_1Messenger_zeitAnteilGesamt_Diagramm
298. EV_1Messenger_zeitAnteilGesamt_AuswahlApp
299. EV_1Messenger_zeitAnteilGesamt_Bilder
300. EV_1Messenger_zeitAnteilGesamt_RezensionBerwertung
301. EV_1Messenger_zeitAnteilGesamt_Rest
302. EV_1Messenger_zeitAnteilEntscheidunginS
303. EV_1Messenger_zeitAnteilGesamtinS
304. EV_1MessengerAnteil_Entscheidung
305. EV_2Videokonferenz_AnzahlWechsel_kein_Signal
306. EV_2Videokonferenz_AnzahlWechsel_Eingabe
307. EV_2Videokonferenz_AnzahlWechsel_Symbol
308. EV_2Videokonferenz_AnzahlWechsel_Text
309. EV_2Videokonferenz_AnzahlWechsel_Skala
310. EV_2Videokonferenz_AnzahlWechsel_Leerlauf
311. EV_2Videokonferenz_AnzahlWechsel_Suchzeile
312. EV_2Videokonferenz_AnzahlWechsel_Zurücktaste
313. EV_2Videokonferenz_AnzahlWechsel_Apptaste
314. EV_2Videokonferenz_AnzahlWechsel_Hometaste
315. EV_2Videokonferenz_AnzahlWechsel_Tastatur
316. EV_2Videokonferenz_AnzahlWechsel_Diagramm
317. EV_2Videokonferenz_AnzahlWechsel_AuswahlApp
318. EV_2Videokonferenz_AnzahlWechsel_Bilder
319. EV_2Videokonferenz_AnzahlWechsel_RezensionBerwertung
320. EV_2Videokonferenz_AnzahlWechsel_Rest
321. EV_2Videokonferenz_Frames_kein_Signal
322. EV_2Videokonferenz_Frames_Eingabe
323. EV_2Videokonferenz_Frames_Symbol
324. EV_2Videokonferenz_Frames_Text
325. EV_2Videokonferenz_Frames_Skala
326. EV_2Videokonferenz_Frames_Leerlauf
327. EV_2Videokonferenz_Frames_Suchzeile
328. EV_2Videokonferenz_Frames_Zurücktaste
329. EV_2Videokonferenz_Frames_Apptaste
330. EV_2Videokonferenz_Frames_Hometaste
331. EV_2Videokonferenz_Frames_Tastatur
332. EV_2Videokonferenz_Frames_Diagramm
333. EV_2Videokonferenz_Frames_AuswahlApp
334. EV_2Videokonferenz_Frames_Bilder
335. EV_2Videokonferenz_Frames_RezensionBerwertung
336. EV_2Videokonferenz_Frames_Rest
337. EV_2Videokonferenz_ZeitinS_kein_Signal
338. EV_2Videokonferenz_ZeitinS_Eingabe
339. EV_2Videokonferenz_ZeitinS_Symbol
340. EV_2Videokonferenz_ZeitinS_Text

341. EV_2Videokonferenz_ZeitinS_Skala
342. EV_2Videokonferenz_ZeitinS_Leerlauf
343. EV_2Videokonferenz_ZeitinS_Suchzeile
344. EV_2Videokonferenz_ZeitinS_Zurücktaste
345. EV_2Videokonferenz_ZeitinS_Apptaste
346. EV_2Videokonferenz_ZeitinS_Hometaste
347. EV_2Videokonferenz_ZeitinS_Tastatur
348. EV_2Videokonferenz_ZeitinS_Diagramm
349. EV_2Videokonferenz_ZeitinS_AuswahlApp
350. EV_2Videokonferenz_ZeitinS_Bilder
351. EV_2Videokonferenz_ZeitinS_RezensionBerwertung
352. EV_2Videokonferenz_ZeitinS_Rest
353. EV_2Videokonferenz_zeitAnteilEntscheidung_Symbol
354. EV_2Videokonferenz_zeitAnteilEntscheidung_Text
355. EV_2Videokonferenz_zeitAnteilEntscheidung_Skala
356. EV_2Videokonferenz_zeitAnteilEntscheidung_Leerlauf
357. EV_2Videokonferenz_zeitAnteilEntscheidung_Suchzeile
358. EV_2Videokonferenz_zeitAnteilEntscheidung_Zurücktaste
359. EV_2Videokonferenz_zeitAnteilEntscheidung_Apptaste
360. EV_2Videokonferenz_zeitAnteilEntscheidung_Hometaste
361. EV_2Videokonferenz_zeitAnteilEntscheidung_Tastatur
362. EV_2Videokonferenz_zeitAnteilEntscheidung_Diagramm
363. EV_2Videokonferenz_zeitAnteilEntscheidung_Bilder
364. EV_2Videokonferenz_zeitAnteilEntscheidung_RezensionBerwertung
365. EV_2Videokonferenz_zeitAnteilGesamt_kein_Signal
366. EV_2Videokonferenz_zeitAnteilGesamt_Eingabe
367. EV_2Videokonferenz_zeitAnteilGesamt_Symbol
368. EV_2Videokonferenz_zeitAnteilGesamt_Text
369. EV_2Videokonferenz_zeitAnteilGesamt_Skala
370. EV_2Videokonferenz_zeitAnteilGesamt_Leerlauf
371. EV_2Videokonferenz_zeitAnteilGesamt_Suchzeile
372. EV_2Videokonferenz_zeitAnteilGesamt_Zurücktaste
373. EV_2Videokonferenz_zeitAnteilGesamt_Apptaste
374. EV_2Videokonferenz_zeitAnteilGesamt_Hometaste
375. EV_2Videokonferenz_zeitAnteilGesamt_Tastatur
376. EV_2Videokonferenz_zeitAnteilGesamt_Diagramm
377. EV_2Videokonferenz_zeitAnteilGesamt_AuswahlApp
378. EV_2Videokonferenz_zeitAnteilGesamt_Bilder
379. EV_2Videokonferenz_zeitAnteilGesamt_RezensionBerwertung
380. EV_2Videokonferenz_zeitAnteilGesamt_Rest
381. EV_2Videokonferenz_zeitAnteilEntscheidunginS
382. EV_2Videokonferenz_zeitAnteilGesamtinS
383. EV_2Videokonferenz_Anteil_Entscheidung
384. EV_3Wetter_AnzahlWechsel_kein_Signal
385. EV_3Wetter_AnzahlWechsel_Eingabe
386. EV_3Wetter_AnzahlWechsel_Symbol
387. EV_3Wetter_AnzahlWechsel_Text
388. EV_3Wetter_AnzahlWechsel_Skala
389. EV_3Wetter_AnzahlWechsel_Leerlauf
390. EV_3Wetter_AnzahlWechsel_Suchzeile
391. EV_3Wetter_AnzahlWechsel_Zurücktaste
392. EV_3Wetter_AnzahlWechsel_Apptaste
393. EV_3Wetter_AnzahlWechsel_Hometaste
394. EV_3Wetter_AnzahlWechsel_Tastatur
395. EV_3Wetter_AnzahlWechsel_Diagramm
396. EV_3Wetter_AnzahlWechsel_AuswahlApp
397. EV_3Wetter_AnzahlWechsel_Bilder
398. EV_3Wetter_AnzahlWechsel_RezensionBerwertung
399. EV_3Wetter_AnzahlWechsel_Rest
400. EV_3Wetter_Frames_kein_Signal

401. EV_3Wetter_Frames_Eingabe
402. EV_3Wetter_Frames_Symbol
403. EV_3Wetter_Frames_Text
404. EV_3Wetter_Frames_Skala
405. EV_3Wetter_Frames_Leerlauf
406. EV_3Wetter_Frames_Suchzeile
407. EV_3Wetter_Frames_Zurücktaste
408. EV_3Wetter_Frames_Apptaste
409. EV_3Wetter_Frames_Hometaste
410. EV_3Wetter_Frames_Tastatur
411. EV_3Wetter_Frames_Diagramm
412. EV_3Wetter_Frames_AuswahlApp
413. EV_3Wetter_Frames_Bilder
414. EV_3Wetter_Frames_RezensionBerwertung
415. EV_3Wetter_Frames_Rest
416. EV_3Wetter_ZeitinS_kein_Signal
417. EV_3Wetter_ZeitinS_Eingabe
418. EV_3Wetter_ZeitinS_Symbol
419. EV_3Wetter_ZeitinS_Text
420. EV_3Wetter_ZeitinS_Skala
421. EV_3Wetter_ZeitinS_Leerlauf
422. EV_3Wetter_ZeitinS_Suchzeile
423. EV_3Wetter_ZeitinS_Zurücktaste
424. EV_3Wetter_ZeitinS_Apptaste
425. EV_3Wetter_ZeitinS_Hometaste
426. EV_3Wetter_ZeitinS_Tastatur
427. EV_3Wetter_ZeitinS_Diagramm
428. EV_3Wetter_ZeitinS_AuswahlApp
429. EV_3Wetter_ZeitinS_Bilder
430. EV_3Wetter_ZeitinS_RezensionBerwertung
431. EV_3Wetter_ZeitinS_Rest
432. EV_3Wetter_zeitAnteilEntscheidung_Symbol
433. EV_3Wetter_zeitAnteilEntscheidung_Text
434. EV_3Wetter_zeitAnteilEntscheidung_Skala
435. EV_3Wetter_zeitAnteilEntscheidung_Leerlauf
436. EV_3Wetter_zeitAnteilEntscheidung_Suchzeile
437. EV_3Wetter_zeitAnteilEntscheidung_Zurücktaste
438. EV_3Wetter_zeitAnteilEntscheidung_Apptaste
439. EV_3Wetter_zeitAnteilEntscheidung_Hometaste
440. EV_3Wetter_zeitAnteilEntscheidung_Tastatur
441. EV_3Wetter_zeitAnteilEntscheidung_Diagramm
442. EV_3Wetter_zeitAnteilEntscheidung_Bilder
443. EV_3Wetter_zeitAnteilEntscheidung_RezensionBerwertung
444. EV_3Wetter_zeitAnteilGesamt_kein_Signal
445. EV_3Wetter_zeitAnteilGesamt_Eingabe
446. EV_3Wetter_zeitAnteilGesamt_Symbol
447. EV_3Wetter_zeitAnteilGesamt_Text
448. EV_3Wetter_zeitAnteilGesamt_Skala
449. EV_3Wetter_zeitAnteilGesamt_Leerlauf
450. EV_3Wetter_zeitAnteilGesamt_Suchzeile
451. EV_3Wetter_zeitAnteilGesamt_Zurücktaste
452. EV_3Wetter_zeitAnteilGesamt_Apptaste
453. EV_3Wetter_zeitAnteilGesamt_Hometaste
454. EV_3Wetter_zeitAnteilGesamt_Tastatur
455. EV_3Wetter_zeitAnteilGesamt_Diagramm
456. EV_3Wetter_zeitAnteilGesamt_AuswahlApp
457. EV_3Wetter_zeitAnteilGesamt_Bilder
458. EV_3Wetter_zeitAnteilGesamt_RezensionBerwertung
459. EV_3Wetter_zeitAnteilGesamt_Rest
460. EV_3Wetter_zeitAnteilEntscheidungingS
461. EV_3Wetter_zeitAnteilGesamtinS
462. EV_3WetterAnteil_Entscheidung
463. EV_4EMail_AnzahlWechsel_kein_Signal
464. EV_4EMail_AnzahlWechsel_Eingabe
465. EV_4EMail_AnzahlWechsel_Symbol
466. EV_4EMail_AnzahlWechsel_Text
467. EV_4EMail_AnzahlWechsel_Skala
468. EV_4EMail_AnzahlWechsel_Leerlauf
469. EV_4EMail_AnzahlWechsel_Suchzeile
470. EV_4EMail_AnzahlWechsel_Zurücktaste
471. EV_4EMail_AnzahlWechsel_Apptaste
472. EV_4EMail_AnzahlWechsel_Hometaste
473. EV_4EMail_AnzahlWechsel_Tastatur
474. EV_4EMail_AnzahlWechsel_Diagramm
475. EV_4EMail_AnzahlWechsel_AuswahlApp
476. EV_4EMail_AnzahlWechsel_Bilder
477. EV_4EMail_AnzahlWechsel_RezensionBerwertung
478. EV_4EMail_AnzahlWechsel_Rest

479. EV_4EMail_Frames_kein_Signal
480. EV_4EMail_Frames_Eingabe
481. EV_4EMail_Frames_Symbol
482. EV_4EMail_Frames_Text
483. EV_4EMail_Frames_Skala
484. EV_4EMail_Frames_Leerlauf
485. EV_4EMail_Frames_Suchzeile
486. EV_4EMail_Frames_Zurücktaste
487. EV_4EMail_Frames_Apptaste
488. EV_4EMail_Frames_Hometaste
489. EV_4EMail_Frames_Tastatur
490. EV_4EMail_Frames_Diagramm
491. EV_4EMail_Frames_AuswahlApp
492. EV_4EMail_Frames_Bilder
493. EV_4EMail_Frames_RezensionBerwertung
494. EV_4EMail_Frames_Rest
495. EV_4EMail_ZeitinS_kein_Signal
496. EV_4EMail_ZeitinS_Eingabe
497. EV_4EMail_ZeitinS_Symbol
498. EV_4EMail_ZeitinS_Text
499. EV_4EMail_ZeitinS_Skala
500. EV_4EMail_ZeitinS_Leerlauf
501. EV_4EMail_ZeitinS_Suchzeile
502. EV_4EMail_ZeitinS_Zurücktaste
503. EV_4EMail_ZeitinS_Apptaste
504. EV_4EMail_ZeitinS_Hometaste
505. EV_4EMail_ZeitinS_Tastatur
506. EV_4EMail_ZeitinS_Diagramm
507. EV_4EMail_ZeitinS_AuswahlApp
508. EV_4EMail_ZeitinS_Bilder
509. EV_4EMail_ZeitinS_RezensionBerwertung
510. EV_4EMail_ZeitinS_Rest
511. EV_4EMail_zeitAnteilEntscheidung_Symbol
512. EV_4EMail_zeitAnteilEntscheidung_Text
513. EV_4EMail_zeitAnteilEntscheidung_Skala
514. EV_4EMail_zeitAnteilEntscheidung_Leerlauf
515. EV_4EMail_zeitAnteilEntscheidung_Suchzeile
516. EV_4EMail_zeitAnteilEntscheidung_Zurücktaste
517. EV_4EMail_zeitAnteilEntscheidung_Apptaste
518. EV_4EMail_zeitAnteilEntscheidung_Hometaste
519. EV_4EMail_zeitAnteilEntscheidung_Tastatur
520. EV_4EMail_zeitAnteilEntscheidung_Diagramm
521. EV_4EMail_zeitAnteilEntscheidung_Bilder
522. EV_4EMail_zeitAnteilEntscheidung_RezensionBerwertung
523. EV_4EMail_zeitAnteilGesamt_kein_Signal
524. EV_4EMail_zeitAnteilGesamt_Eingabe
525. EV_4EMail_zeitAnteilGesamt_Symbol
526. EV_4EMail_zeitAnteilGesamt_Text
527. EV_4EMail_zeitAnteilGesamt_Skala
528. EV_4EMail_zeitAnteilGesamt_Leerlauf
529. EV_4EMail_zeitAnteilGesamt_Suchzeile
530. EV_4EMail_zeitAnteilGesamt_Zurücktaste
531. EV_4EMail_zeitAnteilGesamt_Apptaste
532. EV_4EMail_zeitAnteilGesamt_Hometaste
533. EV_4EMail_zeitAnteilGesamt_Tastatur
534. EV_4EMail_zeitAnteilGesamt_Diagramm
535. EV_4EMail_zeitAnteilGesamt_AuswahlApp
536. EV_4EMail_zeitAnteilGesamt_Bilder
537. EV_4EMail_zeitAnteilGesamt_RezensionBerwertung
538. EV_4EMail_zeitAnteilGesamt_Rest
539. EV_4EMail_zeitAnteilEntscheidungin S
540. EV_4EMail_zeitAnteilGesamtinS
541. EV_4EMailAnteil_Entscheidung
542. EV_5Musik_AnzahlWechsel_kein_Signal
543. EV_5Musik_AnzahlWechsel_Eingabe
544. EV_5Musik_AnzahlWechsel_Symbol
545. EV_5Musik_AnzahlWechsel_Text
546. EV_5Musik_AnzahlWechsel_Skala
547. EV_5Musik_AnzahlWechsel_Leerlauf
548. EV_5Musik_AnzahlWechsel_Suchzeile
549. EV_5Musik_AnzahlWechsel_Zurücktaste
550. EV_5Musik_AnzahlWechsel_Apptaste
551. EV_5Musik_AnzahlWechsel_Hometaste
552. EV_5Musik_AnzahlWechsel_Tastatur
553. EV_5Musik_AnzahlWechsel_Diagramm
554. EV_5Musik_AnzahlWechsel_AuswahlApp
555. EV_5Musik_AnzahlWechsel_Bilder
556. EV_5Musik_AnzahlWechsel_RezensionBerwertung
557. EV_5Musik_AnzahlWechsel_Rest
558. EV_5Musik_Frames_kein_Signal
559. EV_5Musik_Frames_Eingabe
560. EV_5Musik_Frames_Symbol
561. EV_5Musik_Frames_Text
562. EV_5Musik_Frames_Skala
563. EV_5Musik_Frames_Leerlauf

564. EV_5Musik_Frames_Suchzeile
565. EV_5Musik_Frames_Zurücktaste
566. EV_5Musik_Frames_Apptaste
567. EV_5Musik_Frames_Hometaste
568. EV_5Musik_Frames_Tastatur
569. EV_5Musik_Frames_Diagramm
570. EV_5Musik_Frames_AuswahlApp
571. EV_5Musik_Frames_Bilder
572. EV_5Musik_Frames_RezensionBerwertung
573. EV_5Musik_Frames_Rest
574. EV_5Musik_ZeitinS_kein_Signal
575. EV_5Musik_ZeitinS_Eingabe
576. EV_5Musik_ZeitinS_Symbol
577. EV_5Musik_ZeitinS_Text
578. EV_5Musik_ZeitinS_Skala
579. EV_5Musik_ZeitinS_Leerlauf
580. EV_5Musik_ZeitinS_Suchzeile
581. EV_5Musik_ZeitinS_Zurücktaste
582. EV_5Musik_ZeitinS_Apptaste
583. EV_5Musik_ZeitinS_Hometaste
584. EV_5Musik_ZeitinS_Tastatur
585. EV_5Musik_ZeitinS_Diagramm
586. EV_5Musik_ZeitinS_AuswahlApp
587. EV_5Musik_ZeitinS_Bilder
588. EV_5Musik_ZeitinS_RezensionBerwertung
589. EV_5Musik_ZeitinS_Rest
590. EV_5Musik_zeitAnteilEntscheidung_Symbol
591. EV_5Musik_zeitAnteilEntscheidung_Text
592. EV_5Musik_zeitAnteilEntscheidung_Skala
593. EV_5Musik_zeitAnteilEntscheidung_Leerlauf
594. EV_5Musik_zeitAnteilEntscheidung_Suchzeile
595. EV_5Musik_zeitAnteilEntscheidung_Zurücktaste
596. EV_5Musik_zeitAnteilEntscheidung_Apptaste
597. EV_5Musik_zeitAnteilEntscheidung_Hometaste
598. EV_5Musik_zeitAnteilEntscheidung_Tastatur
599. EV_5Musik_zeitAnteilEntscheidung_Diagramm
600. EV_5Musik_zeitAnteilEntscheidung_Bilder
601. EV_5Musik_zeitAnteilEntscheidung_RezensionBerwertung
602. EV_5Musik_zeitAnteilGesamt_kein_Signal
603. EV_5Musik_zeitAnteilGesamt_Eingabe
604. EV_5Musik_zeitAnteilGesamt_Symbol
605. EV_5Musik_zeitAnteilGesamt_Text
606. EV_5Musik_zeitAnteilGesamt_Skala
607. EV_5Musik_zeitAnteilGesamt_Leerlauf
608. EV_5Musik_zeitAnteilGesamt_Suchzeile
609. EV_5Musik_zeitAnteilGesamt_Zurücktaste
610. EV_5Musik_zeitAnteilGesamt_Apptaste
611. EV_5Musik_zeitAnteilGesamt_Hometaste
612. EV_5Musik_zeitAnteilGesamt_Tastatur
613. EV_5Musik_zeitAnteilGesamt_Diagramm
614. EV_5Musik_zeitAnteilGesamt_AuswahlApp
615. EV_5Musik_zeitAnteilGesamt_Bilder
616. EV_5Musik_zeitAnteilGesamt_RezensionBerwertung
617. EV_5Musik_zeitAnteilGesamt_Rest
618. EV_5Musik_zeitAnteilEntscheidungi nS
619. EV_5Musik_zeitAnteilGesamtinS
620. EV_5MusikAnteil_Entscheidung
621. EV_6Fitness_AnzahlWechsel_kein_Signal
622. EV_6Fitness_AnzahlWechsel_Eingabe
623. EV_6Fitness_AnzahlWechsel_Symbol
624. EV_6Fitness_AnzahlWechsel_Text
625. EV_6Fitness_AnzahlWechsel_Skala
626. EV_6Fitness_AnzahlWechsel_Leerlauf
627. EV_6Fitness_AnzahlWechsel_Suchzeile
628. EV_6Fitness_AnzahlWechsel_Zurücktaste
629. EV_6Fitness_AnzahlWechsel_Apptaste
630. EV_6Fitness_AnzahlWechsel_Hometaste
631. EV_6Fitness_AnzahlWechsel_Tastatur
632. EV_6Fitness_AnzahlWechsel_Diagramm
633. EV_6Fitness_AnzahlWechsel_AuswahlApp
634. EV_6Fitness_AnzahlWechsel_Bilder
635. EV_6Fitness_AnzahlWechsel_RezensionBerwertung
636. EV_6Fitness_AnzahlWechsel_Rest
637. EV_6Fitness_Frames_kein_Signal
638. EV_6Fitness_Frames_Eingabe
639. EV_6Fitness_Frames_Symbol
640. EV_6Fitness_Frames_Text
641. EV_6Fitness_Frames_Skala
642. EV_6Fitness_Frames_Leerlauf
643. EV_6Fitness_Frames_Suchzeile

644. EV_6Fitness_Frames_Zurücktaste
645. EV_6Fitness_Frames_Apptaste
646. EV_6Fitness_Frames_Hometaste
647. EV_6Fitness_Frames_Tastatur
648. EV_6Fitness_Frames_Diagramm
649. EV_6Fitness_Frames_AuswahlApp
650. EV_6Fitness_Frames_Bilder
651. EV_6Fitness_Frames_RezensionBerwertung
652. EV_6Fitness_Frames_Rest
653. EV_6Fitness_ZeitinS_kein_Signal
654. EV_6Fitness_ZeitinS_Eingabe
655. EV_6Fitness_ZeitinS_Symbol
656. EV_6Fitness_ZeitinS_Text
657. EV_6Fitness_ZeitinS_Skala
658. EV_6Fitness_ZeitinS_Leerlauf
659. EV_6Fitness_ZeitinS_Suchzeile
660. EV_6Fitness_ZeitinS_Zurücktaste
661. EV_6Fitness_ZeitinS_Apptaste
662. EV_6Fitness_ZeitinS_Hometaste
663. EV_6Fitness_ZeitinS_Tastatur
664. EV_6Fitness_ZeitinS_Diagramm
665. EV_6Fitness_ZeitinS_AuswahlApp
666. EV_6Fitness_ZeitinS_Bilder
667. EV_6Fitness_ZeitinS_RezensionBerwertung
668. EV_6Fitness_ZeitinS_Rest
669. EV_6Fitness_zeitAnteilEntscheidung_Symbol
670. EV_6Fitness_zeitAnteilEntscheidung_Text
671. EV_6Fitness_zeitAnteilEntscheidung_Skala
672. EV_6Fitness_zeitAnteilEntscheidung_Leerlauf
673. EV_6Fitness_zeitAnteilEntscheidung_Suchzeile
674. EV_6Fitness_zeitAnteilEntscheidung_Zurücktaste
675. EV_6Fitness_zeitAnteilEntscheidung_Apptaste
676. EV_6Fitness_zeitAnteilEntscheidung_Hometaste
677. EV_6Fitness_zeitAnteilEntscheidung_Tastatur
678. EV_6Fitness_zeitAnteilEntscheidung_Diagramm
679. EV_6Fitness_zeitAnteilEntscheidung_Bilder
680. EV_6Fitness_zeitAnteilEntscheidung_RezensionBerwertung
681. EV_6Fitness_zeitAnteilGesamt_kein_Signal
682. EV_6Fitness_zeitAnteilGesamt_Eingabe
683. EV_6Fitness_zeitAnteilGesamt_Symbol
684. EV_6Fitness_zeitAnteilGesamt_Text
685. EV_6Fitness_zeitAnteilGesamt_Skala
686. EV_6Fitness_zeitAnteilGesamt_Leerlauf
687. EV_6Fitness_zeitAnteilGesamt_Suchzeile
688. EV_6Fitness_zeitAnteilGesamt_Zurücktaste
689. EV_6Fitness_zeitAnteilGesamt_Apptaste
690. EV_6Fitness_zeitAnteilGesamt_Hometaste
691. EV_6Fitness_zeitAnteilGesamt_Tastatur
692. EV_6Fitness_zeitAnteilGesamt_Diagramm
693. EV_6Fitness_zeitAnteilGesamt_AuswahlApp
694. EV_6Fitness_zeitAnteilGesamt_Bilder
695. EV_6Fitness_zeitAnteilGesamt_RezensionBerwertung
696. EV_6Fitness_zeitAnteilGesamt_Rest
697. EV_6Fitness_zeitAnteilEntscheidungin S
698. EV_6Fitness_zeitAnteilGesamtinS
699. EV_6FitnessAnteil_Entscheidung
700. EV_7Spiele_AnzahlWechsel_kein_Signal
701. EV_7Spiele_AnzahlWechsel_Eingabe
702. EV_7Spiele_AnzahlWechsel_Symbol
703. EV_7Spiele_AnzahlWechsel_Text
704. EV_7Spiele_AnzahlWechsel_Skala
705. EV_7Spiele_AnzahlWechsel_Leerlauf
706. EV_7Spiele_AnzahlWechsel_Suchzeile
707. EV_7Spiele_AnzahlWechsel_Zurücktaste
708. EV_7Spiele_AnzahlWechsel_Apptaste
709. EV_7Spiele_AnzahlWechsel_Hometaste
710. EV_7Spiele_AnzahlWechsel_Tastatur
711. EV_7Spiele_AnzahlWechsel_Diagramm
712. EV_7Spiele_AnzahlWechsel_AuswahlApp
713. EV_7Spiele_AnzahlWechsel_Bilder
714. EV_7Spiele_AnzahlWechsel_RezensionBerwertung
715. EV_7Spiele_AnzahlWechsel_Rest
716. EV_7Spiele_Frames_kein_Signal
717. EV_7Spiele_Frames_Eingabe
718. EV_7Spiele_Frames_Symbol
719. EV_7Spiele_Frames_Text
720. EV_7Spiele_Frames_Skala
721. EV_7Spiele_Frames_Leerlauf
722. EV_7Spiele_Frames_Suchzeile

723. EV_7Spiele_Frames_Zurücktaste
724. EV_7Spiele_Frames_Apptaste
725. EV_7Spiele_Frames_Hometaste
726. EV_7Spiele_Frames_Tastatur
727. EV_7Spiele_Frames_Diagramm
728. EV_7Spiele_Frames_AuswahlApp
729. EV_7Spiele_Frames_Bilder
730. EV_7Spiele_Frames_RezensionBerwertung
731. EV_7Spiele_Frames_Rest
732. EV_7Spiele_ZeitinS_kein_Signal
733. EV_7Spiele_ZeitinS_Eingabe
734. EV_7Spiele_ZeitinS_Symbol
735. EV_7Spiele_ZeitinS_Text
736. EV_7Spiele_ZeitinS_Skala
737. EV_7Spiele_ZeitinS_Leerlauf
738. EV_7Spiele_ZeitinS_Suchzeile
739. EV_7Spiele_ZeitinS_Zurücktaste
740. EV_7Spiele_ZeitinS_Apptaste
741. EV_7Spiele_ZeitinS_Hometaste
742. EV_7Spiele_ZeitinS_Tastatur
743. EV_7Spiele_ZeitinS_Diagramm
744. EV_7Spiele_ZeitinS_AuswahlApp
745. EV_7Spiele_ZeitinS_Bilder
746. EV_7Spiele_ZeitinS_RezensionBerwertung
747. EV_7Spiele_ZeitinS_Rest
748. EV_7Spiele_zeitAnteilEntscheidung_Symbol
749. EV_7Spiele_zeitAnteilEntscheidung_Text
750. EV_7Spiele_zeitAnteilEntscheidung_Skala
751. EV_7Spiele_zeitAnteilEntscheidung_Leerlauf
752. EV_7Spiele_zeitAnteilEntscheidung_Suchzeile
753. EV_7Spiele_zeitAnteilEntscheidung_Zurücktaste
754. EV_7Spiele_zeitAnteilEntscheidung_Apptaste
755. EV_7Spiele_zeitAnteilEntscheidung_Hometaste
756. EV_7Spiele_zeitAnteilEntscheidung_Tastatur
757. EV_7Spiele_zeitAnteilEntscheidung_Diagramm
758. EV_7Spiele_zeitAnteilEntscheidung_Bilder
759. EV_7Spiele_zeitAnteilEntscheidung_RezensionBerwertung
760. EV_7Spiele_zeitAnteilGesamt_kein_Signal
761. EV_7Spiele_zeitAnteilGesamt_Eingabe
762. EV_7Spiele_zeitAnteilGesamt_Symbol
763. EV_7Spiele_zeitAnteilGesamt_Text
764. EV_7Spiele_zeitAnteilGesamt_Skala
765. EV_7Spiele_zeitAnteilGesamt_Leerlauf
766. EV_7Spiele_zeitAnteilGesamt_Suchzeile
767. EV_7Spiele_zeitAnteilGesamt_Zurücktaste
768. EV_7Spiele_zeitAnteilGesamt_Apptaste
769. EV_7Spiele_zeitAnteilGesamt_Hometaste
770. EV_7Spiele_zeitAnteilGesamt_Tastatur
771. EV_7Spiele_zeitAnteilGesamt_Diagramm
772. EV_7Spiele_zeitAnteilGesamt_AuswahlApp
773. EV_7Spiele_zeitAnteilGesamt_Bilder
774. EV_7Spiele_zeitAnteilGesamt_RezensionBerwertung
775. EV_7Spiele_zeitAnteilGesamt_Rest
776. EV_7Spiele_zeitAnteilEntscheidungi nS
777. EV_7Spiele_zeitAnteilGesamtinS
778. EV_7SpieleAnteil_Entscheidung
779. EV_8Nachrichten_AnzahlWechsel_kein_Signal
780. EV_8Nachrichten_AnzahlWechsel_Eingabe
781. EV_8Nachrichten_AnzahlWechsel_Symbol
782. EV_8Nachrichten_AnzahlWechsel_Text
783. EV_8Nachrichten_AnzahlWechsel_Skala
784. EV_8Nachrichten_AnzahlWechsel_Leerlauf
785. EV_8Nachrichten_AnzahlWechsel_Suchzeile
786. EV_8Nachrichten_AnzahlWechsel_Zurücktaste
787. EV_8Nachrichten_AnzahlWechsel_Apptaste
788. EV_8Nachrichten_AnzahlWechsel_Hometaste
789. EV_8Nachrichten_AnzahlWechsel_Tastatur
790. EV_8Nachrichten_AnzahlWechsel_Diagramm
791. EV_8Nachrichten_AnzahlWechsel_AuswahlApp
792. EV_8Nachrichten_AnzahlWechsel_Bilder
793. EV_8Nachrichten_AnzahlWechsel_RezensionBerwertung
794. EV_8Nachrichten_AnzahlWechsel_Rest
795. EV_8Nachrichten_Frames_kein_Signal

796. EV_8Nachrichten_Frames_Eingabe
797. EV_8Nachrichten_Frames_Symbol
798. EV_8Nachrichten_Frames_Text
799. EV_8Nachrichten_Frames_Skala
800. EV_8Nachrichten_Frames_Leerlauf
801. EV_8Nachrichten_Frames_Suchzeile
802. EV_8Nachrichten_Frames_Zurücktaste
803. EV_8Nachrichten_Frames_Apptaste
804. EV_8Nachrichten_Frames_Hometaste
805. EV_8Nachrichten_Frames_Tastatur
806. EV_8Nachrichten_Frames_Diagramm
807. EV_8Nachrichten_Frames_AuswahlApp
808. EV_8Nachrichten_Frames_Bilder
809. EV_8Nachrichten_Frames_RezensionBerwertung
810. EV_8Nachrichten_Frames_Rest
811. EV_8Nachrichten_ZeitinS_kein_Signal
812. EV_8Nachrichten_ZeitinS_Eingabe
813. EV_8Nachrichten_ZeitinS_Symbol
814. EV_8Nachrichten_ZeitinS_Text
815. EV_8Nachrichten_ZeitinS_Skala
816. EV_8Nachrichten_ZeitinS_Leerlauf
817. EV_8Nachrichten_ZeitinS_Suchzeile
818. EV_8Nachrichten_ZeitinS_Zurücktaste
819. EV_8Nachrichten_ZeitinS_Apptaste
820. EV_8Nachrichten_ZeitinS_Hometaste
821. EV_8Nachrichten_ZeitinS_Tastatur
822. EV_8Nachrichten_ZeitinS_Diagramm
823. EV_8Nachrichten_ZeitinS_AuswahlApp
824. EV_8Nachrichten_ZeitinS_Bilder
825. EV_8Nachrichten_ZeitinS_RezensionBerwertung
826. EV_8Nachrichten_ZeitinS_Rest
827. EV_8Nachrichten_zeitAnteilEntscheidung_Symbol
828. EV_8Nachrichten_zeitAnteilEntscheidung_Text
829. EV_8Nachrichten_zeitAnteilEntscheidung_Skala
830. EV_8Nachrichten_zeitAnteilEntscheidung_Leerlauf
831. EV_8Nachrichten_zeitAnteilEntscheidung_Suchzeile
832. EV_8Nachrichten_zeitAnteilEntscheidung_Zurücktaste
833. EV_8Nachrichten_zeitAnteilEntscheidung_Apptaste
834. EV_8Nachrichten_zeitAnteilEntscheidung_Hometaste
835. EV_8Nachrichten_zeitAnteilEntscheidung_Tastatur
836. EV_8Nachrichten_zeitAnteilEntscheidung_Diagramm
837. EV_8Nachrichten_zeitAnteilEntscheidung_Bilder
838. EV_8Nachrichten_zeitAnteilEntscheidung_RezensionBerwertung
839. EV_8Nachrichten_zeitAnteilGesamt_kein_Signal
840. EV_8Nachrichten_zeitAnteilGesamt_Eingabe
841. EV_8Nachrichten_zeitAnteilGesamt_Symbol
842. EV_8Nachrichten_zeitAnteilGesamt_Text
843. EV_8Nachrichten_zeitAnteilGesamt_Skala
844. EV_8Nachrichten_zeitAnteilGesamt_Leerlauf
845. EV_8Nachrichten_zeitAnteilGesamt_Suchzeile
846. EV_8Nachrichten_zeitAnteilGesamt_Zurücktaste
847. EV_8Nachrichten_zeitAnteilGesamt_Apptaste
848. EV_8Nachrichten_zeitAnteilGesamt_Hometaste
849. EV_8Nachrichten_zeitAnteilGesamt_Tastatur
850. EV_8Nachrichten_zeitAnteilGesamt_Diagramm
851. EV_8Nachrichten_zeitAnteilGesamt_AuswahlApp
852. EV_8Nachrichten_zeitAnteilGesamt_Bilder
853. EV_8Nachrichten_zeitAnteilGesamt_RezensionBerwertung
854. EV_8Nachrichten_zeitAnteilGesamt_Rest
855. EV_8Nachrichten_zeitAnteilEntscheidunginS
856. EV_8Nachrichten_zeitAnteilGesamtinS
857. EV_8NachrichtenAnteil_Entscheidung
858. EV_Alle_AnzahlWechsel_kein_Signal
859. EV_Alle_AnzahlWechsel_Eingabe
860. EV_Alle_AnzahlWechsel_Symbol
861. EV_Alle_AnzahlWechsel_Text
862. EV_Alle_AnzahlWechsel_Skala
863. EV_Alle_AnzahlWechsel_Leerlauf
864. EV_Alle_AnzahlWechsel_Suchzeile

865. EV_Alle_AnzahlWechsel_Zurücktaste
866. EV_Alle_AnzahlWechsel_Apptaste
867. EV_Alle_AnzahlWechsel_Hometaste
868. EV_Alle_AnzahlWechsel_Tastatur
869. EV_Alle_AnzahlWechsel_Diagramm
870. EV_Alle_AnzahlWechsel_AuswahlApp
871. EV_Alle_AnzahlWechsel_Bilder
872. EV_Alle_AnzahlWechsel_RezensionBerwertung
873. EV_Alle_AnzahlWechsel_Rest
874. EV_Alle_Frames_kein_Signal
875. EV_Alle_Frames_Eingabe
876. EV_Alle_Frames_Symbol
877. EV_Alle_Frames_Text
878. EV_Alle_Frames_Skala
879. EV_Alle_Frames_Leerlauf
880. EV_Alle_Frames_Suchzeile
881. EV_Alle_Frames_Zurücktaste
882. EV_Alle_Frames_Apptaste
883. EV_Alle_Frames_Hometaste
884. EV_Alle_Frames_Tastatur
885. EV_Alle_Frames_Diagramm
886. EV_Alle_Frames_AuswahlApp
887. EV_Alle_Frames_Bilder
888. EV_Alle_Frames_RezensionBerwertung
889. EV_Alle_Frames_Rest
890. EV_Alle_ZeitinS_kein_Signal
891. EV_Alle_ZeitinS_Eingabe
892. EV_Alle_ZeitinS_Symbol
893. EV_Alle_ZeitinS_Text
894. EV_Alle_ZeitinS_Skala
895. EV_Alle_ZeitinS_Leerlauf
896. EV_Alle_ZeitinS_Suchzeile
897. EV_Alle_ZeitinS_Zurücktaste
898. EV_Alle_ZeitinS_Apptaste
899. EV_Alle_ZeitinS_Hometaste
900. EV_Alle_ZeitinS_Tastatur
901. EV_Alle_ZeitinS_Diagramm
902. EV_Alle_ZeitinS_AuswahlApp
903. EV_Alle_ZeitinS_Bilder
904. EV_Alle_ZeitinS_RezensionBerwertung
905. EV_Alle_ZeitinS_Rest
906. EV_Alle_zeitAnteilEntscheidung_Symbol
907. EV_Alle_zeitAnteilEntscheidung_Text
908. EV_Alle_zeitAnteilEntscheidung_Skala
909. EV_Alle_zeitAnteilEntscheidung_Leerlauf
910. EV_Alle_zeitAnteilEntscheidung_Suchzeile
911. EV_Alle_zeitAnteilEntscheidung_Zurücktaste
912. EV_Alle_zeitAnteilEntscheidung_Apptaste
913. EV_Alle_zeitAnteilEntscheidung_Hometaste
914. EV_Alle_zeitAnteilEntscheidung_Tastatur
915. EV_Alle_zeitAnteilEntscheidung_Diagramm
916. EV_Alle_zeitAnteilEntscheidung_Bilder
917. EV_Alle_zeitAnteilEntscheidung_RezensionBerwertung
918. EV_Alle_zeitAnteilGesamt_kein_Signal
919. EV_Alle_zeitAnteilGesamt_Eingabe
920. EV_Alle_zeitAnteilGesamt_Symbol
921. EV_Alle_zeitAnteilGesamt_Text
922. EV_Alle_zeitAnteilGesamt_Skala
923. EV_Alle_zeitAnteilGesamt_Leerlauf
924. EV_Alle_zeitAnteilGesamt_Suchzeile
925. EV_Alle_zeitAnteilGesamt_Zurücktaste
926. EV_Alle_zeitAnteilGesamt_Apptaste
927. EV_Alle_zeitAnteilGesamt_Hometaste
928. EV_Alle_zeitAnteilGesamt_Tastatur
929. EV_Alle_zeitAnteilGesamt_Diagramm
930. EV_Alle_zeitAnteilGesamt_AuswahlApp
931. EV_Alle_zeitAnteilGesamt_Bilder
932. EV_Alle_zeitAnteilGesamt_RezensionBerwertung
933. EV_Alle_zeitAnteilGesamt_Rest
934. EV_Alle_zeitAnteilEntscheidunginS
935. EV_Alle_zeitAnteilGesamtinS
936. EV_AlleAnteil_Entscheidung
937. EV_Reihenfolge
938. EV_1App_Entscheidungszeit
939. EV_2App_Entscheidungszeit
940. EV_3App_Entscheidungszeit
941. EV_4App_Entscheidungszeit
942. EV_5App_Entscheidungszeit
943. EV_6App_Entscheidungszeit
944. EV_7App_Entscheidungszeit
945. EV_8App_Entscheidungszeit
946. EV_Diff_App_1_2_EntscheidungszeitInS
947. EV_Diff_App_2_3_EntscheidungszeitInS
948. EV_Diff_App_3_4_EntscheidungszeitInS
949. EV_Diff_App_4_5_EntscheidungszeitInS
950. EV_Diff_App_5_6_EntscheidungszeitInS
951. EV_Diff_App_6_7_EntscheidungszeitInS
952. EV_Diff_App_7_8_EntscheidungszeitInS
953. RA_Messenger
954. RA_Videoconference
955. RA_Weather
956. RA_EMail
957. RA_Music
958. RA_Fittness
959. RA_Games
960. RA_News

Anhang BB. Einverständniserklärung zum dritten empirischen Versuch

TU Berlin | Fakultät V | IPA | FG Mensch-Maschine-Systeme |
Sek. MAR 3-1 | Marchstraße 23 | 10587 Berlin

Fakultät V Fakultät Verkehrs- un
Maschinensysteme
Institut für Psychologie und
Arbeitswissenschaft

Fachgebiet
Mensch-Maschine-Systeme

M. Sc. Sven Bock

Sekretariat MAR 3-1
Marchstraße 23
10587 Berlin

Telefon +49 (0)30 314-79523
Sven.Bock@mms.tu-berlin.de

Einverständniserklärung zur Studie
"Benutzerfreundlichkeit einer Nachrichtenapplikation"

Diese Studie zielt darauf ab, die Nutzbarkeit und Handhabung einer bestimmten Applikation zu untersuchen. Laden Sie zunächst die Applikation über den Link herunter der Ihnen per SMS zugesandt wird. Bitte benutzen Sie ggf. Ihren Teilnehmercode, um sich einzuloggen. Danach werden Sie gebeten, einige Aufgaben innerhalb der Applikation zu erledigen, die Ihnen per SMS zugesendet werden. Es werden Ihnen verschiedene Arten von Aufgaben zugeschickt, die Sie angemessen lösen sollen. Das Experiment dauert 10 Tage und schließt mit einem ab. Dabei werden Sie gebeten bestimmte Eigenschaften bezüglich der Benutzererfahrung zu bewerten.
Die Teilnahme am Experiment wird mit zehn Euro oder einer Versuchspersonenstunde vergütet.

Der Zweck der Studie wurde mir erklärt. Mir wurde mitgeteilt, dass ich die Studie jederzeit ohne Angabe von Gründen abbrechen kann und dass mir dadurch keine Nachteile entstehen. Ferner wurde mir mitgeteilt, dass die während der Studie erhobenen Daten zur Auswertung der Studie verwendet werden. Diese werden aus rechtlichen Gründen bis zu zehn Jahre aufbewahrt. Die Aufzeichnungen werden nach der Transkription des Interviews gelöscht. Alle Daten werden für den wissenschaftlichen Gebrauch erhoben und vertraulich sowie anonym behandelt. Die anonymisierten Ergebnisse werden im Rahmen der Doktorarbeit veröffentlicht. Persönliche Daten, wie diese Einverständniserklärung, werden streng vertraulich behandelt und getrennt voneinander aufbewahrt. Ich bin damit einverstanden, dass die erhobenen Daten in anonymisierter Form gespeichert und für wissenschaftliche Zwecke ausgewertet werden. Mir ist bekannt, dass ich bei Bedarf die Möglichkeit habe, innerhalb von zwei Wochen einen Antrag auf Löschung der Versuchsdaten zu stellen, der umgehend bearbeitet wird. Dazu ist die Mitteilung des persönlichen Registrierungscodes erforderlich. Anschließend wird die Zuordnungsliste zwischen persönlichem Code und fortlaufender VP-Nummer gelöscht, so dass die Löschung der Versuchsdaten nicht mehr gewährleistet ist.
Ich bin über Art, Bedeutung und Umfang der geplanten Studie ausreichend informiert worden. Die Fragen zur Überprüfung der Voraussetzungen habe ich wahrheitsgetreu beantwortet.

Meine Teilnahme an der Studie ist freiwillig. Ich bin mir bewusst, dass ich jederzeit die Gelegenheit habe Fragen zu stellen, in dem ich den Versuchsleiter per E-Mail oder Telefon kontaktiere. Ich habe die Teilnehmerinformationen vollständig gelesen und verstanden. Mit der Unterzeichnung der Einverständniserklärung stimme ich dieser zu.

Berlin, _____ _____ _____
Datum Unterschrift Name in Druckbuchstaben

Anhang CC. Aufgabenstellung zum dritten empirischen Versuch

Willkommen bei der Studie zur Evaluation einer Nachrichtenapplikation. Bitte laden Sie sich die zu evaluierende Applikation unter folgendem Link herunter: https://tinyurl.com/TUNewsapp
Zur Installation der Applikation müssen Sie die Option „Unbekannte Quellen“ oder „Unbekannte Herkunft“ oder „Unbekannte Applikation“ aktivieren.
Zunächst würde ich Sie bitten, die gestellten Aufgaben so bald wie möglich zu erfüllen, in jedem Fall jedoch am selben Tag der Aufgabenstellung. Weiterhin möchte ist Sie bitten, mir Ihre „Device ID“ mitzuteilen. Diese finden Sie in der Applikation unter dem Menüpunkt „Setting“ unten rechts in der Applikation. Der einfachste Weg wäre es, einen Screenshot zu erstellen und diesen an sven.bock@mms.tu-berlin.de zu schicken. Die Einstellungen der Applikation dürfen Sie nach Belieben verändern. Die ersten Aufgaben erfolgen am morgigen Tag. Bis dahin würde ich Sie bitten mir die Device-ID geschickt zu haben.
Liebe Grüße Sven Bock

Tag 1

Guten Tag. Es folgen die ersten Aufgaben im Rahmen der Studie zur „Evaluation einer Nachrichtenapplikation“:
1. Bitte öffnen Sie die Nachrichtenapplikation „Local News & Events“ und laden Sie (unter dem Menüpunkt „all news“) die lokalen Nachrichten, indem Sie auf „Read local News“ klicken.
2. Teilen Sie die für Sie wichtigste Nachricht, indem Sie auf „Share news“ klicken.

Tag 2

Guten Tag. Es folgen die nächsten Aufgaben im Rahmen der Studie:
1. Öffnen Sie die Nachrichtenapplikation und rufen Sie die lokalen Nachrichten ab.
2. Speichern Sie eine Nachricht, die sich als interessant erachten auf ihrem Smartphone, indem Sie auf „Save news“ drücken.
3. Suchen Sie unter dem Punkt „Events“ eine Veranstaltung heraus, die Sie interessiert und tragen Sie sich diese mit Hilfe des „Add to calender“-Knopfes in den Kalender ein.

Tag 3

Guten Tag. Es folgen die nächsten Aufgaben im Rahmen der Studie zur „Evaluation einer Nachrichtenapplikation“:
1. Bitte öffnen Sie die Nachrichtenapplikation „Local News & Events“ und rufen Sie die lokalen Nachrichten ab.
2. Bitte suchen Sie unter dem Punkt „Events“ eine Veranstaltung heraus, die Sie interessiert, und aktivieren Sie die „Push notification“.

Tag 4

1. Bitte öffnen Sie die Nachrichtenapplikation „Local News & Events“ und rufen Sie die lokalen Nachrichten ab.
2. Teilen Sie die für Sie unwichtigste Nachricht, indem Sie auf „Share news“ klicken.

Tag 5

Guten Tag. Es folgen die nächsten Aufgaben im Rahmen der Studie zur „Evaluation einer Nachrichtenapplikation“:
1. Bitte öffnen Sie die Nachrichtenapplikation „Local News & Events“ und rufen Sie die lokalen Nachrichten ab.
2. Speichern Sie eine Nachricht, die Sie als nicht interessant erachten auf ihrem Smartphone, indem Sie auf „Save news“ drücken.
3. Bitte suchen Sie unter dem Punkt „Events“ eine Veranstaltung heraus, die Sie nicht interessiert und tragen Sie sich diese mit Hilfe des „Add to calender“-Knopfes in den Kalender ein.

Tag 6

Guten Tag. Es folgen die nächsten Aufgaben im Rahmen der Studie zur „Evaluation einer Nachrichtenapplikation“:

1. Bitte öffnen Sie die Nachrichtenapplikation „Local News & Events“ und rufen Sie die lokalen Nachrichten ab.
2. Bitte suchen Sie unter dem Punkt „Events“ eine Veranstaltung heraus, die Sie nicht interessiert und aktivieren Sie die „Push notification“.

Tag 7

Guten Tag. Es folgen die nächsten Aufgaben im Rahmen der Studie zur „Evaluation einer Nachrichtenapplikation“:

1. Bitte öffnen Sie die Nachrichtenapplikation „Local News & Events“ und rufen Sie die lokalen Nachrichten ab.
2. Speichern Sie eine Nachricht, die Sie als nicht interessant erachten auf ihrem Smartphone, indem Sie auf „Save news“ drücken.
3. Teilen Sie die für Sie unwichtigste Nachricht, indem Sie auf „Share news“ klicken.

Tag 8

Guten Tag. Es folgen die nächsten Aufgaben im Rahmen der Studie zur „Evaluation einer Nachrichtenapplikation“:

1. Bitte öffnen Sie die Nachrichtenapplikation „Local News & Events“ und rufen Sie die lokalen Nachrichten ab.
2. Bitte suchen Sie unter dem Punkt „Events“ eine Veranstaltung heraus, die Sie nicht interessiert und aktivieren Sie die „Push notification“.
3. Teilen Sie die für Sie unwichtigste Nachricht, indem Sie auf „Share news“ klicken.

Tag 9

Guten Tag. Es folgen die nächsten Aufgaben im Rahmen der Studie zur „Evaluation einer Nachrichtenapplikation“:

1. Bitte öffnen Sie die Nachrichtenapplikation „Local News & Events“ und rufen Sie die lokalen Nachrichten ab.
2. Bitte suchen Sie unter dem Punkt „Events“ eine Veranstaltung heraus, die Ihrer/Ihrem besten Freund/-in interessiert und aktivieren Sie die „Push notification“.
3. Bitte suchen Sie unter dem Punkt „all news“ eine Nachricht heraus, die für Ihre/Ihren besten Freund /-in interessant sein könnte, und teilen Sie diese, indem Sie auf „Share news“ klicken.

Tag 10

Guten Tag. Es folgen die nächsten Aufgaben im Rahmen der Studie zur „Evaluation einer Nachrichtenapplikation“:

1. Bitte öffnen Sie die Nachrichtenapplikation „Local News & Events“ und rufen Sie die lokalen Nachrichten ab.
2. Speichern Sie eine Nachricht, die Sie als interessant erachten auf ihrem Smartphone, indem Sie auf „Save news“ drücken.

Anhang DD. Einstellungsmenü mit Device-ID



Anhang EE. Aufklärung zum dritten empirischen Versuch

TU Berlin | Fakultät V | IPA | FG Mensch-Maschine-Systeme |
Sek. MAR 3-1 | Marchstraße 23 | 10587 Berlin

Fakultät V Fakultät Verkehrs- und Maschinensysteme
Institut für Psychologie und Arbeitswissenschaft

Fachgebiet
Mensch-Maschine-Systeme

M. Sc. Sven Bock

Sekretariat MAR 3-1
Marchstraße 23
10587 Berlin

Telefon +49 (0)30 314-79523
Sven.Bock@mms.tu-berlin.de

Aufklärung zur Studie „Evaluation einer Nachrichtenapplikation":

Fokus dieser Studie war der Umgang mit der temporären Zugriffsberechtigung seitens der Nutzer. Gegenwärtig kann der Nutzer die Rechte nur mit einer unbegrenzten Gültigkeit erteilen und hat lediglich eine binäre Option, die angeforderten Zugriffsberechtigung zu akzeptieren oder abzulehnen. Die in diesem Experiment implementierte dritte Option, einer temporären Zugriffsberechtigung soll es dem Nutzer ermöglichen, die gewünschten Berechtigungen mit Einschränkungen, also für eine bestimmte Zeit, zu gewähren. Dies sollte dem Nutzer eine informiertere Entscheidungen ermöglichen, in dem er die Konsequenzen von vorübergehend gewährten Zugriffsberechtigung verstanden hat. Ziel der Studie war es, herauszufinden, ob ein „Ablaufdatum" für die Zugriffsberechtigungen von dem Nutzer gewünscht ist und akzeptiert wird.

Im Rahmen der Studie werden nur drei Arten von Daten erhoben: Name der Berechtigung (Speicher, Mikrophon etc.), gewählte Option („Accept", „Maybe", „Decline") und der Zeitstempel, welcher festhält, wann die Entscheidung getroffen wurde. Während dieser Studie erfolgten keine Zugriffe auf die angeforderten Berechtigungen, wie zum Beispiel auf Standort- oder andere Sensordaten. Mithilfe dieser Studie soll untersucht werden, ob die Implementierung einer temporären Zugriffsberechtigung genutzt und akzeptiert wird. Ferner, soll untersucht werden, ob die Erweiterung der Zugriffsanfrage durch die „Maybe"-Option angemessen ist und wie diese Option weiterhin verbessert werden könnte.

Nach dem Experiment sind Sie berechtigt, die aufgezeichneten Daten einzusehen, indem Sie Ihren persönlichen Code und eine Anfrage innerhalb von zwei Wochen per E-Mail senden.

Mit Ihrer Unterschrift erklären Sie sich damit einverstanden, dass die soeben aufgeführten Daten heruntergeladen und zur wissenschaftlichen Auswertung verwendet werden dürfen.

Berlin, _____ _____ _____
Datum Unterschrift Name in Druckbuchstaben

Anhang FF. Variablen zum dritten Versuch

1. GeräteID
2. Persoenlicher_Code
3. AntwortID
4. DatumAbgeschickt
5. LetzteSeite
6. Zufallsgeneratorstartwert
7. Datumgestartet
8. DatumletzteAktivität
9. MO_Auffallen_Maybe_Oprion
10. MO_Privater_Nutzen_Maybe_Option
11. MO_Veraergerung_durch_wiederkehrende_Anforderung
12. MO_Wichtigkeit_Kontrolle_persoenlicher_Daten
13. MO_Dauer_Zugriffsberechtigung
14. MO_Benutzerfreundlichkeit_wichtiger_als_schutz
15. MO_Gefallen_Maybe_Option
16. MO_Standort_temporaer
17. MO_Handy_Speicher_temporaer
18. MO_SD_Kartenspeicher_temporaer
19. MO_Kontakte_temporaer
20. MO_Nachrichten_Messenger_temporaer
21. MO_Nachrichten_SMS_temporaer
22. MO_Kalender_temporaer
23. MO_Mikrofon_temporaer
24. MO_Verbesserungen_Maybe_Option
25. MO_V_M_O_keine_Angabe
26. MO_V_M_O_Zugriffsberechtigung_kuerzere_Intervalle
27. MO_V_M_O_Zugriffsberechtigung_laengere_Intervalle
28. MO_V_M_O_Verbesserungen_Maybe_Option_Sichtbarkeit
29. MO_V_M_O_Datenabruf
30. MO_V_M_O_Erlaeuterung_Funktion
31. MO_V_M_O_Beliebige_Zeit
32. MO_V_M_O_Timer
33. MO_V_M_O_Berechtigung_nur_aktueller_Nutzung
34. MO_V_M_O_Anzahl_Zugriffe_beschraenken
35. MO_V_M_O_Design
36. MO_V_M_O_Sprache_anpassen
37. MO_V_M_O_Erlaeuterung_Datennutzung
38. MO_Situation_Maybe_Option
39. MO_S_M_O_Neu
40. MO_S_M_O_Immer
41. MO_S_M_O_Arbeit
42. MO_S_M_O_Standortaenderung
43. MO_S_M_O_Persoenliche_Informationen
44. MO_S_M_O_Nie
45. MO_S_M_O_Selten
46. MO_S_M_O_Terminplanung
47. MO_S_M_O_Voruebergehend
48. MO_Erster_Eindruck_Maybe_Option
49. MO_E_E_M_O_Nicht_aufgefallen
50. MO_E_E_M_O_Bedeutung_unklar
51. MO_E_E_M_O_Positiv_aufgefallen
52. MO_E_E_M_O_Nichts
53. MO_E_E_M_O_Negativ_aufgefallen
54. MO_Angeklickt_Maybe_Option
55. MO_Verstaendniss_Maybe_Option
56. MO_U_M_O_Verstanden
57. MO_U_M_O_Verstanden_und_richtig_erklärt
58. MO_U_M_O_Falsch_erklärt
59. MO_Begruendung_Verwendung_Maybe_Option
60. MO_N_B_M_O_Kontrolle
61. MO_N_B_M_O_Nicht_verwendet
62. MO_N_B_M_O_Kein_Grund
63. MO_N_B_M_O_Datenschutz
64. MO_N_B_M_O_Temporaerer_Gebrauch
65. MO_N_B_M_O_Misstrauen_App
66. MO_Ja_Angemessenheit_Dauer_Maybe_Option
67. MO_Ja_Ko_Angemessenheit_Dauer_Maybe_Option
68. MO_Zu_kurz_Angemessenheit_Dauer_Maybe_Option
69. MO_Zu_kurz_Ko_Angemessenheit_Dauer_Maybe_Option
70. MO_Zu_lang_Angemessenheit_Dauer_Maybe_Option
71. MO_Zu_lang_Ko_Angemessenheit_Dauer_Maybe_Option
72. MO_Zu_wenig_Optionen_Angemessenheit_Dauer_Maybe_Option
73. MO_Zu_wenig_Optionen_Ko_Angemessenheit_Dauer_Maybe_Option
74. MO_Andere_Gruende_Angemessenheit_Dauer_Maybe_Option
75. MO_Andere_Gruende_Ko_Angemessenheit_Dauer_Maybe_Option
76. MO_Verbesserung_Maybe_Option_2
77. DEM_Geschlecht
78. DEM_Alter
79. DEM_Bildungsabschluss

80. DEM_Technische_Affinitaet
81. DEM_Handynutzung
82. DEM_Wichtigkeit_Privatsphaere
83. DEM_Nein_Schutz_persoenlicher_Daten
84. DEM_Ja_Schutz_persoenlicher_Daten
85. DEM_Anwendung_Schutz_persoenlicher_Daten
86. DEM_Geringer_Offenlegung_Schutz_persoenlicher_Daten
87. DEM_Lesen_AGB_Schutz_persoenlicher_Daten
88. DEM_Sonstiges_Schutz_persoenlicher_Daten
89. Gesamtzeit
90. GruppenzeitFragebogenabschnittüberdieAkzeptanzdervorübergehend
91. GruppenzeitDemographischeDaten331
92. GruppenzeitAufwandsentschädigung
93. APP_Push_Benachrichtigung_annehmen
94. APP_Push_Benachrichtigung_maybe
95. APP_Push_Benachrichtigung_ablehnen
96. APP_Standort_annehmen
97. APP_Standort_maybe
98. APP_Standort_ablehnen
99. APP_Kontakte_annehmen
100. APP_Kontakte_maybe
101. APP_Kontakte_ablehnen
102. APP_Gerätspeicher_annehmen
103. APP_Gerätespeicher_maybe
104. APP_Gerätspeicher_ablehnen
105. APP_Kalender_annehmen
106. APP_Kalender_maybe
107. APP_Kalender_ablehnen
108. APP_annehmen_insgesamt
109. APP_maybe_insgesamt
110. APP_ablehnen_insgesamt
111. APP_maybe_Dauer_pushBenachrichtigung
112. APP_maybe_Dauer_Standort
113. APP_maybe_Dauer_Kontakte
114. APP_maybe_Dauer_Gerätespeicherung
115. APP_maybe_Dauer_Kalender
116. APP_maybe_1Tage
117. APP_maybe_3Tage
118. APP_maybe_7Tage

Anhang GG. Tabellen zum dritten Versuch

Tabelle 178 *Demographische Daten Alter und Geschlecht*

Alter	M	SD	NV
	29,68	9,18	0,01

	Männlich	**Weiblich**
Geschlecht	11	20

Tabelle 179 *Demographische Daten Bildung*

	Bildung			
	Mittlere Reife	Abitur	Berufsausbildung	Akademische Abschluss
Gesamt	0	14	2	15

Tabelle 180 *Tägliche Handynutzung in Stunden*

	Tägliche Handynutzung				
	<30 Min	30 Min - 1 Std	< 1 Std, aber > 2 Std	2- 4 Std	> 5 Std
Häufigkeit	0	1	7	14	9

Tabelle 181 *Technikaffinität*

	Technikaffinität									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Häufigkeit	0	2	2	0	1	2	12	4	6	2

Tabelle 182 *Wichtigkeit der Privatsphäre*

Wichtigkeit Privatsphäre	M	SD	NV
	5,97	0,912	0

Tabelle 183 *Häufigkeiten des Schutzes der persönlichen Daten*

Häufigkeiten		
17. Sind Sie aktiv tätig, um Ihre persönlichen Daten zu schützen?	Antwort	
	Ja	Nein
Nein.	9	22
Ja.	**22**	**9**
Ich habe eine Anwendung zum Datenschutz installiert.	5	26
Ich versuche, so wenig wie möglich von meinen Daten offenzulegen.	13	18
Ich habe die Bedingungen und Konditionen gelesen, bevor ich eine Anwendung installiere.	6	25
Sonstiges.	1	Teilweise bei sozialen Netzwerken

Tabelle 184 *Mittelwerte zu Bewertung der „Maybe"-Option*

Deskriptive Statistiken				
1.Bitte bewerten Sie die folgenden Aussagen.	N	M	SD	NV
Mir ist die "Maybe"-Option (temporäre Zugriffsberechtigung) aufgefallen.	31	5,10	3,60	0,021
Ich würde die "Maybe"-Option auf meinem privaten Gerät benutzen.	31	5,35	3,03	0,19
Die immer wiederkehrende Anforderung, die Zustimmung zu erteilen, hat mich verärgert.	31	4,32	2,87	0,014
Die Kontrolle der persönlichen Daten ist mir wichtig.	31	8,19	1,94	0,001
Die Benutzerfreundlichkeit ist mir wichtiger als der Schutz meiner persönlichen Daten.	31	4,00	2,70	0,005
Mir gefällt die Idee der "Maybe"-Option.	31	5,87	2,33	0

Anmerkung. Mittelwerte der Beträge der Differenzen zwischen der angegebenen Vertrauenswürdigkeit und der angegebenen Aggressivität durch die Datenschutzskala verglichen zwischen den Gruppen farblich in absteigend sortierter Rangfolge: rot, orange, gelb, grün.

Tabelle 185 *Häufigkeiten der Dauer der Zugriffsberechtigung*

Häufigkeiten										
2. Wie lange sollte einer Anwendung erlaubt werden, auf die Zugriffberechtigung zuzugreifen?										
Maybe-Option	Skala									
	weniger als 30 Minuten	1 Stunde	12 Stunden	1 Tag	2 Tage	1 Woche	2 Wochen	1 Monat	6 Monate	für immer
Dauer der Zugriffsberechtigung	5 (16,1)	3 (9,7)	2 (6,5)	4 (12,9)	1 (3,2)	4 (12,9)	3 (9,7)	4 (12,9)	3 (9,7)	2 (6,5)

Anmerkung. Angaben in absoluten Zahlen, wobei der Prozentsatz in Klammern aufgeführt wird.

Tabelle 186 *Häufigkeiten zu Bewertung der „Maybe"-Option*

Häufigkeiten										
1. Bitte bewerten Sie die folgenden Aussagen.	Skala									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Mir ist die "Maybe"-Option (temporäre Zugriffsberechtigung) **aufgefallen**.	9 (29,03)	1 (3,23)	2 (6,45)	2 (6,45)	6 (19,35)	1 (3,23)		1 (3,23)	1 (3,23)	8 (25,81)
Ich würde die "Maybe"-Option auf meinem privaten Gerät **benutzen**.	6 (19,4)	1 (3,2)	2 (6,5)	1 (3,2)	7 (22,6)	4 (12,9)	1 (3,2)	2 (6,5)	4 (12,9)	3 (9,7)
Die immer wiederkehrende Anforderung, die Zustimmung zu erteilen, hat mich **verärgert**.	7 (22,6)	5 (16,1)	2 (6,5)	2 (6,5)	5 (16,1)	2 (6,5)	2 (6,5)	3 (9,7)	2 (6,5)	1 (3,2)
Die **Kontrolle der persönlichen Daten** ist mir wichtig.			1 (3,2)		3 (9,7)	2 (6,5)	4 (12,9)	4 (12,9)	6 (19,4)	11 (35,5)
Die **Benutzerfreundlichkeit** ist mir **wichtiger** als der **Schutz** meiner persönlichen Daten.	7 (22,6)	3 (9,7)	7 (22,6)	2 (6,5)	3 (9,7)	5 (16,1)		1 (3,2)	1 (3,2)	2 (6,5)
Mir **gefällt** die Idee der "Maybe"-Option.	3 (9,7)		1 (3,2)		12 (38,7)	3 (9,7)	4 (12,9)	3 (9,7)	4 (12,9)	1 (3,2)

Anmerkung. Angaben in absoluten Zahlen, wobei der Prozentsatz in Klammern aufgeführt wird.

Tabelle 187 *Häufigkeiten der Berechtigungen, bei denen die temporäre Zugriffsberechtigung genutzt werden würde*

Häufigkeiten				
3. Für welche Berechtigungen würden Sie die temporäre Zugriffsberechtigung in Betracht ziehen?	Antwort			
	Ja		Nein	
Standort	25	(80,6)	6	(19,4)
Handy-Speicher	11	(35,5)	20	(64,5)
SD-Kartenspeicher	6	(19,4)	25	(80,6)
Kontakte	11	(35,5)	20	(64,5)
Nachrichten (Messenger)	9	(29)	22	(71)
Nachrichten (SMS)	13	(41,9)	18	(58,1)
Kalender	13	(41,9)	18	(58,1)
Mikrofon	9	(29)	22	(71)

Anmerkung. Angaben in absoluten Zahlen, wobei der Prozentsatz in Klammern aufgeführt wird.

Tabelle 188 *Häufigkeiten der Verbesserungsvorschläge für die temporäre Zugriffsberechtigung*

Häufigkeiten	
4. Was würden Sie an der temporären Zugriffsberechtigung verbessern?	Antwort
Keine Angabe	9 (29,03)
Kürzere Intervalle für die Zugriffsberechtigung	3 (9,68)
Längere Intervalle für die Zugriffsberechtigung	1 (3,23)
Verbesserungen der Sichtbarkeit der Maybe-Option	4 (12,90)
Datenabruf	1 (3,23)
Erläuterung der Funktion	1 (3,23)
Beliebige Zeit	5 (16,13)
Timer	1 (3,23)
Nur Berechtigung der aktuellen Nutzung	1 (3,23)
Anzahl der Zugriffe beschränken	1 (3,23)
Design	3 (9,68)
Sprache anpassen	1 (3,23)
Erläuterung der Datennutzung	1 (3,23)

Anmerkung. Angaben in absoluten Zahlen, wobei der Prozentsatz in Klammern aufgeführt wird.

Tabelle 189 *Häufigkeiten der alltäglichen Situationen in denen der temporäre Zugriffsberechtigung genutzt wird*

Häufigkeiten	
5. In welchen alltäglichen Situationen würden Sie die temporäre Zugriffsberechtigung nutzen?	Antwort
Neu	1 (3,23)
Immer	3 (9,68)
Arbeit	1 (3,23)
Standortänderung	9 (29,03)
Persönliche Informationen	3 (9,68)
Nie	2 (6,45)
Selten	1 (3,23)
Terminplanung	1 (3,23)
Vorübergehend	3 (9,68)

Anmerkung. Angaben in absoluten Zahlen, wobei der Prozentsatz in Klammern aufgeführt wird.

Tabelle 190 *Häufigkeiten der ersten Eindrucke über die temporäre Zugriffsberechtigung*

Häufigkeiten	
6. Was dachten Sie über die "Maybe"-Option, als Sie sie zum ersten Mal sahen?	Antwort
Nicht aufgefallen	4 (12,90)
Bedeutung unklar	4 (12,90)
Positiv aufgefallen	5 (16,13)
Nichts	8 (25,81)
Negativ aufgefallen	2 (6,45)

Anmerkung. Angaben in absoluten Zahlen, wobei der Prozentsatz in Klammern aufgeführt wird.

Tabelle 191 *Häufigkeiten der Nutzung der temporären Zugriffsberechtigung*

Häufigkeiten		
7. Haben Sie auf die "Maybe"-Option geklickt?	Antwort	
	Ja	Nein
Anzahl der Personen, welche die Maybe-Option benutzt haben	10 (32,3)	21 (67,7)

Tabelle 192 *Häufigkeiten des Verständnisses über die temporäre Zugriffsberechtigung*

Häufigkeiten	
8. Wenn Sie die "Maybe"-Option (temporäre Zugriffsberechtigung) benutzt haben, haben Sie verstanden, was die Funktion dieser Option ist?	Antwort
Verstanden	1 (10,00)
Verstanden und richtig erklärt	7 (70,00)
Falsch erklärt	1 (10,00)

Anmerkung. Angaben in absoluten Zahlen, wobei der Prozentsatz in Klammern aufgeführt wird.

Tabelle 193 *Häufigkeiten der Gründe für die Verwendung der temporären Zugriffsberechtigung*

Häufigkeiten	
9. Warum haben Sie die temporäre Zugriffsberechtigung verwendet?	Antwort
Kontrolle	3 (9,68)
Nicht verwendet	8 (25,81)
Kein Grund	6 (19,35)
Datenschutz	3 (9,68)
Temporärer Gebrauch	5 (16,13)
Misstrauen App	2 (6,45)

Anmerkung. Angaben in absoluten Zahlen, wobei der Prozentsatz in Klammern aufgeführt wird.

Tabelle 194 *Häufigkeiten der Angemessenheit der Dauer der temporären Zugriffberechtigung*

Häufigkeiten		
10. Sind Sie der Meinung, dass die vorgesehene Dauer der temporären Zugriffsberechtigung angemessen war?	Antwort	
	Ja	Nein
Ja	19 (61,3)	12 (38,7)
Zu kurz	4 (12,9)	27 (87,1)
Zu lang	2 (6,5)	29 (93,5)
Zu wenig Optionen	4 (12,9)	27 (87,1)
Andere Gründe	5 (16,1)	26 (83,9)

Anmerkung. Angaben in absoluten Zahlen, wobei der Prozentsatz in Klammern aufgeführt wird.

Tabelle 195 *Zusammenhang zwischen Auffallen der „Maybe“-Option und Gefallen der „Maybe“-Option sowie der Wichtigkeit der Kontrolle der persönlichen Daten*

Korrelationen				
			Gefallen der Maybe-Option	Wichtigkeit der Kontrolle der persönlichen Daten
Spearman-Rho	Auffallen der Maybe-Option	Korrelationskoeffizient	0,105	-0,361
		Sig. (2-seitig)	0,575	0,0416
		N	31	31

Tabelle 196 *Zusammenhang zwischen der Wichtigkeit der Privatsphäre und den Aussagen der ersten Frage bezüglich der „Maybe“-Option*

Korrelationen								
			Auffallen der Maybe-Option	Privater Nutzen der Maybe-Option	Verärgerung durch wieder-kehrende Anforderung	Wichtigkeit der Kontrolle der persönlichen Daten	Benutzerfreundlichkeit ist wichtiger als Schutz	Gefallen der Maybe-Option
Spearman-Rho	Wichtigkeit Privatsphäre	Korrelationskoeffizient	-0,084	0,172	-0,034	0,721	-0,11	-0,025
		Sig. (2-seitig)	0,655	0,354	0,856	0	0,557	0,896
		N	31	31	31	31	31	31

Tabelle 197 *Zusammenhang zwischen der Dauer der erteilten Zugriffsberechtigung und den zweiten bis vierten Aussagen der ersten Frage bezüglich der „Maybe“-Option*

Korrelationen							
			Privater Nutzen der Maybe-Option	Verärgerung durch die wiederkehrende Anforderung	Wichtigkeit der Kontrolle persönlicher Daten	Benutzerfreundlichkeit ist wichtiger als Schutz	Gefallen der Maybe-Option
Spearman-Rho	Dauer der Zugriffsberechtigung	Korrelationskoeffizient	-0,132	0,170	-0,365	0,156	0,054
		Sig. (2-seitig)	0,479	0,360	0,043	0,403	0,772
		N	31	31	31	31	31

Tabelle 198 *Zusammenhang zwischen der technischen Affinität und den Aussagen der ersten Frage bezüglich der „Maybe“-Option*

Korrelationen								
			Auffallen der Maybe-Option	Privater Nutzen der Maybe-Option	Verärgerung durch wiederkehrende Anforderung	Wichtigkeit der Kontrolle persönlicher Daten	Benutzerfreundlichkeit ist wichtiger als Schutz	Gefallen der Maybe-Option
Spearman-Rho	Technische Affinität	Korrelationskoeffizient	0,269	0,19	0,38	0,225	0,11	0,141
		Sig. (2-seitig)	0,143	0,307	0,035	0,224	0,558	0,45
		N	31	31	31	31	31	31

Tabelle 199 *Zusammenhang zwischen der Handynutzung und den zweiten bis vierten Aussagen der ersten Frage bezüglich der „Maybe“-Option*

Korrelationen							
			Privater Nutzen der Maybe-Option	Verärgerung durch wiederkehrende Anforderung	Wichtigkeit der Kontrolle persönlicher Daten	Benutzerfreundlichkeit ist wichtiger als Schutz	Gefallen der Maybe-Option
Spearman-Rho	Handynutzung	Korrelationskoeffizient	0,011	0,048	-0,225	-0,074	-0,031
		Sig. (2-seitig)	0,953	0,799	0,223	0,691	0,868
		N	31	31	31	31	31

Tabelle 200 *Zusammenhang zwischen dem Alter und den Aussagen der ersten Frage bezüglich der „Maybe“-Option*

Korrelationen								
			Auffallen der Maybe-Option	Privater Nutzen der Maybe-Option	Verärgerung durch wieder-kehrende Anforderung	Wichtigkeit der Kontrolle persönlicher Daten	Benutzerfreundlichkeit ist wichtiger als Schutz	Gefallen der Maybe-Option
Spearman-Rho	Alter	Korrelationskoeffizient	-0,124	-0,033	-0,284	0,059	-0,155	-0,15
		Sig. (2-seitig)	0,506	0,86	0,122	0,751	0,404	0,42
		N	31	31	31	31	31	31

Tabelle 201 *Zusammenhang zwischen der technischen Affinität und der Handynutzung*

Korrelationen			
			Handynutzung
Spearman-Rho	Technische Affinität	Korrelationskoeffizient	-0,053
		Sig. (2-seitig)	0,778
		N	31

Tabelle 202 *Häufigkeiten der gewählten Optionen getrennt nach der Berechtigungsart*

Häufigkeiten										
Berechtigungsart	Option	Häufigkeit der Auswahl							Gesamt	
		0	1	2	3	4	5	6	Häufigkeit der Auswahl	N	Gesamte Auswahl
Push-Benachrichtigung	Allow	5 (16,1)	26 (83,9)						26 (66,7)	26	
	Maybe	26 (83,9)	1 (3,2)	2 (6,5)	2 (6,5)				11 (28,2)	5	39
	Deny	30 (96,8)		1 (3,2)					2 (5,1)	1	
Standort	Allow	2 (6,5)	29 (93,5)						29 (74,4)	29	
	Maybe	29 (93,5)						2 (6,5)	12 (30,8)	2	46
	Deny	27 (87,1)	3 (9,7)	1 (3,2)					5 (12,8)	4	
Kontakte	Allow	6 (19,4)	25 (80,6)						25 (64,1)	25	
	Maybe	26 (83,9)		1 (3,2)	2 (6,5)	2 (6,5)			16 (41,0)	5	45
	Deny	28 (90,3)	2 (6,5)	1 (3,2)					4 (10,3)	3	
Gerätespeicher	Allow	4 (12,9)	27 (87,1)						27 (69,2)	27	
	Maybe	26 (83,9)		1 (3,2)	1 (3,2)	3 (9,7)			17 (43,6)	5	47
	Deny	30 (96,8)			1 (3,2)				3 (7,7)	1	
Kalender	Allow	6 (19,4)	25 (80,6)						25 (64,1)	25	
	Maybe	26 (83,9)	1 (3,2)	4 (12,9)					9 (23,1)	5	36
	Deny	30 (96,8)		1 (3,2)					2 (5,1)	1	

Anmerkung. Angaben in absoluten Zahlen, wobei der Prozentsatz in Klammern aufgeführt wird.

Tabelle 203 *Häufigkeiten der gewählten Optionen insgesamt*

Häufigkeiten							
APP	Häufigkeit der Auswahl					Gesamt	
	0	**1**	**2**	**4**	**5**	Häufigkeit der Auswahl	N
Gesamt “Allow”	2 (6,5)	2 (6,5)	1 (3,2)	2 (6,5)	24 (77,4)	132 (62,0)	29(93,5)

Häufigkeiten							
APP	Häufigkeit der Auswahl					Gesamt	
	0	**2**	**5**	**11**	**13**	**17**	Häufigkeit der Auswahl	N
Gesamt “Maybe”	25 (80,6)	1 (3,2)	1 (3,2)	1 (3,2)	1 (3,2)	2 (6,5)	65 (30,5)	6 (19,4)

Häufigkeiten						
APP	Häufigkeit der Auswahl				Gesamt	
	0	**1**	**3**	**9**	Häufigkeit der Auswahl	N
Gesamt “Deny”	25 (80,6)	4 (12,9)	1 (3,2)	1 (3,2)	16 (7,5)	6 (19,4)

Anmerkung. Angaben in absoluten Zahlen, wobei der Prozentsatz in Klammern aufgeführt wird, farblich in absteigend sortierter Rangfolge: rot, gelb, grün.

Tabelle 204 *Häufigkeiten der ausgewählten Dauer der temporären Zugriffsberechtigung*

Häufigkeiten								
Maybe	Häufigkeit der Auswahl							Gesamt
Dauer	2	3	7	10	12	13	16	
1 Tag	2 (6,5)		1 (3,2)		1 (3,2)	1 (3,2)	1 (3,2)	52 (80)
3 Tage				1 (3,2)				10 (15,38)
7 Tage		1 (3,2)						3 (4,62)

Anmerkung. Angaben in absoluten Zahlen, wobei der Prozentsatz in Klammern aufgeführt wird.

Tabelle 205 *Durchschnittliche Dauer der temporären Zugriffsberechtigung getrennt nach der Berechtigungsart*

Berechtigungsart	Min	Max	M	SD	NV(p)	Gesamt
Push-Benachrichtigung	2	6	3,5	1,732	*	
Standort	1	12	6,33	5,508	*	
Kontakte	3	8	5,2	2,168	0,131	
Gerätespeicherung	2	9	4,2	2,775	0,082	
Kalender	2	8	3,6	2,608	0,079	
						4,566

Anmerkung. * konnte nicht berechnet werden. Farblich in absteigend sortierter Rangfolge: rot, orange, gelb, grün.

Tabelle 206 *Zusammenhang zwischen der Wichtigkeit der Privatsphäre und der gewählten Option*

Korrelationen					
			"Allow" Gesamt	"Maybe" Gesamt	„Deny" Gesamt
Spearman-Rho	Wichtigkeit Privatsphäre	Korrelationskoeffizient	-0,214	0,297	0,136
		Sig. (2-seitig)	0,247	0,104	0,467
		N	31	31	31

Tabelle 207 *Durchschnittliche Auswahl der Optionen auf die angefragte Zugriffsberechtigung*

Gesamt	M	SD	NV(p)
Allow	4,26	1,591	0.000
Maybe	2,1	5,036	0.000
Deny	0,52	1,691	0.000

Tabelle 208 *Durchschnittliche Auswahl der Optionen auf die angefragte Zugriffsberechtigung getrennt nach Nutzen der „Maybe“-Option*

Gesamt	Ja			Nein		
	M	SD	NV(p)	M	SD	NV(p)
Allow	2,90	2,28	0,01	4,90	0,30	0,00
Maybe	6,30	7,42	0,009	0,10	0,44	0,00
Deny	1,20	2,90	0,00	0,19	0,40	0,00

(321-326)

Tabelle 209 *Mann-Whitney-U-Test Vergleich der durchschnittlichen Auswahl der Optionen auf die angefragte Zugriffsberechtigung getrennt nach Nutzen der „Maybe“-Option*

Ränge

Gesamt	Maybe-Option angeklickt	H	Mittlerer Rang	Summe der Ränge
Allow	Ja	10	11,25	112,50
	Nein	21	18,26	383,50
	Gesamtsumme	31		
Maybe	Ja	10	21,00	210,00
	Nein	21	13,62	286,00
	Gesamtsumme	31		
Deny	Ja	10	16,50	165,00
	Nein	21	15,76	331,00
	Gesamtsumme	31		

Teststatistiken[a]

	„Accept“ Gesamt	„Maybe“ Gesamt	„Deny“ Gesamt
Mann-Whitney-U-Test	57,500	55,000	100,000
Wilcoxon-W	112,500	286,000	331,000
z	-2,742	-3,064	-,307
Asymp. Sig. (2-seitig)	,006	,002	,759
Exakte Sig. [2*(1-seitige Sig.)]	,043[b]	,035[b]	,852[b]

a. Gruppierungsvariable: Angeklickt_Maybe_Option

b. Nicht für Bindungen korrigiert.

Teil A: Fragebogenabschnitt über die Akzeptanz der temporären Zugriffsberechtigung

A1. **Bitte tragen Sie ihren persönlichen Code ein, den Sie bereits zu Beginn der Studie übermittelt haben.**

A2. **1. Bitte bewerten Sie die folgenden Aussagen.**

1 = stimmt nicht zu \\ 10 = stimmt voll und ganz zu

	1	2	3	4	5	6	7	8	9	10
Mir ist die "Maybe"-Option (temporären Zugriffsberechtigung) aufgefallen.	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Ich würde die "Maybe"-Option auf meinem privaten Gerät benutzen.	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Die immer wiederkehrende Anforderung, die Zustimmung zu erteilen, hat mich verärgert.	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Die Kontrolle der persönlichen Daten ist mir wichtig.	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Die Benutzerfreundlichkeit ist mir wichtiger als der Schutz meiner persönlichen Daten.	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Mir gefällt die Idee der "Maybe"-Option.	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

A3. **2. Wie lange sollte einer Anwendung erlaubt werden, auf die Zugriffberechtigung zuzugreifen?**

- für immer ☐
- 1 Jahr ☐
- 6 Monate ☐
- 1 Monat ☐
- 2 Wochen ☐
- 1 Woche ☐
- 2 Tage ☐
- 1 Tag ☐
- 12 Stunden ☐
- 6 Stunden ☐
- 1 Stunde ☐
- 30 Minuten ☐
- weniger als 30 Minuten ☐

A4. **3. Für welche Berechtigungen würden Sie die temporäre Zugriffsberechtigung in Betracht ziehen?**

- Standort ☐
- Handy-Speicher ☐
- SD-Kartenspeicher ☐
- Kontakte ☐
- Nachrichten (Messenger) ☐
- Nachrichten (SMS) ☐
- Kalender ☐
- Mikrofon ☐

A5. **4. Was würden Sie an der temporären Zugriffsberechtigung verbessern?**

A6. **5. In welchen alltäglichen Situationen würden Sie die temporäre Zugriffsberechtigung nutzen?**

A7. **6. Was dachten Sie über die "Maybe"-Option, als Sie sie zum ersten Mal sahen?**

A8. **7. Haben Sie auf die "Maybe"-Option geklickt?**

Ja ☐

Nein ☐

A9. **8. Wenn Sie die "Maybe"-Option (temporäre Zugriffsberechtigung) benutzt haben, haben Sie verstanden, was die Funktion dieser Option ist?**

Bitte beschreiben Sie kurz die Funktion der "Maybe"-Option.

A10. **9. Warum haben Sie die temporäre Zugriffsberechtigung verwendet?**

A11. **10. Sind Sie der Meinung, dass die vorgesehene Dauer der temporären Zugriffsberechtigung angemessen war?**

Ja ☐

Kommentar

Nein, die Intervalle waren zu kurz ☐

Kommentar

Nein, die Intervalle waren zu lang ☐

Kommentar

Nein, es gab zu wenige Optionen ☐

Kommentar

Nein, andere Gründe ☐

Kommentar

Teil B: Demographische Daten (331)

Bitte beantworten Sie die folgenden Fragen zu Ihrer Person.

B1. **11. Bitte geben Sie Ihr Geschlecht an.**

Männlich ☐

Weiblich ☐

Diverse ☐

B2. **12. Bitte geben Sie Ihr Alter in Jahren ein.**

B3. **13. Bitte geben Sie Ihren höchsten Bildungsabschluss an.**

- ☐ kein Abschluss
- ☐ Sekundarschule / Oberstufe
- ☐ Abitur / Allgemeine Hochschulreife
- ☐ Berufsausbildung
- ☐ Akademischer Abschluss

B4. **14. Technische Affinität.**

1 = trifft überhaupt nicht zu || 10 = trifft voll und ganz zu

	1	2	3	4	5	6	7	8	9	10
Ich habe eine große Affinität zur Technologie.	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

B5. **15. Bitte geben Sie an, wie viele Stunden pro Tag Sie Ihr Smartphone benutzen.**

- ☐ weniger als eine halbe Stunde
- ☐ mehr als eine halbe Stunde, aber weniger als eine Stunde
- ☐ mehr als eine Stunde, aber weniger als zwei Stunden
- ☐ mehr als zwei Stunden, aber weniger als vier Stunden
- ☐ mehr als vier Stunden

B6. **16. Der Schutz meiner Privatsphäre ist mir wichtig.**

trifft überhaupt nicht zu	trifft nicht zu	trifft eher nicht zu	weder noch	trifft eher zu	trifft zu	trifft völlig zu
☐	☐	☐	☐	☐	☐	☐

B7. **17. Sind Sie aktiv tätig, um Ihre persönlichen Daten zu schützen?**

- ☐ Nein
- ☐ Ja
- ☐ Ich habe eine Anwendung zum Datenschutz installiert.
- ☐ Ich versuche, so wenig wie möglich von meinen Daten offenzulegen.
- ☐ Ich habe die Bedingungen und Konditionen gelesen, bevor ich eine Anwendung installiere.
- ☐ Sonstiges

Sonstiges

Teil C: Aufwandsentschädigung

C1. Bitte wählen Sie die gewünschte Aufwandentschädigung und geben Sie Bankinformation (Name des Kontoinhabers und IBAN) oder PayPal-Adresse an. Falls Sie eine Versuchspersonenstunde gutgeschrieben haben möchte geben Sie Ihre E-Mail an, damit ich Sie kontaktieren kann.

Vielen Dank für die Teilnahme an der Studie!

Der angegebenen Namen und die E-Mail Adresse werden gesondert abgespeichert und nicht in Verbindung mit vorherigen Angaben in Fagebogen gebracht. Nach erfolgreiche Zahlung der Aufwandsentschädigung werden die Angaben umgehend gelöscht.

Nur Teilnehmende die einen persönlichen Code und eine Device ID übermittelt haben, erhalten die Aufwandsentschädigung. Ist dies bis dato nicht geschehen, sollten Sie dies unverzüglich nachholen. Übersenden Sie bitte die fehlenden Unterlagen an: sven.bock@mms.tu-berlin.de.

☐ Banküberweisung (Name des Kontoinhabers / IBAN)

Kommentar

☐ Paypal (E-Mail-Adresse)

Kommentar

☐ Versuchpersonennummer (E-Mail-Adresse)

Kommentar

☐ Ich möchte keine Aufwandentschädigung

Kommentar

Anhang II. Übersicht von den Forschungsfragen und den entsprechenden Hypothesen

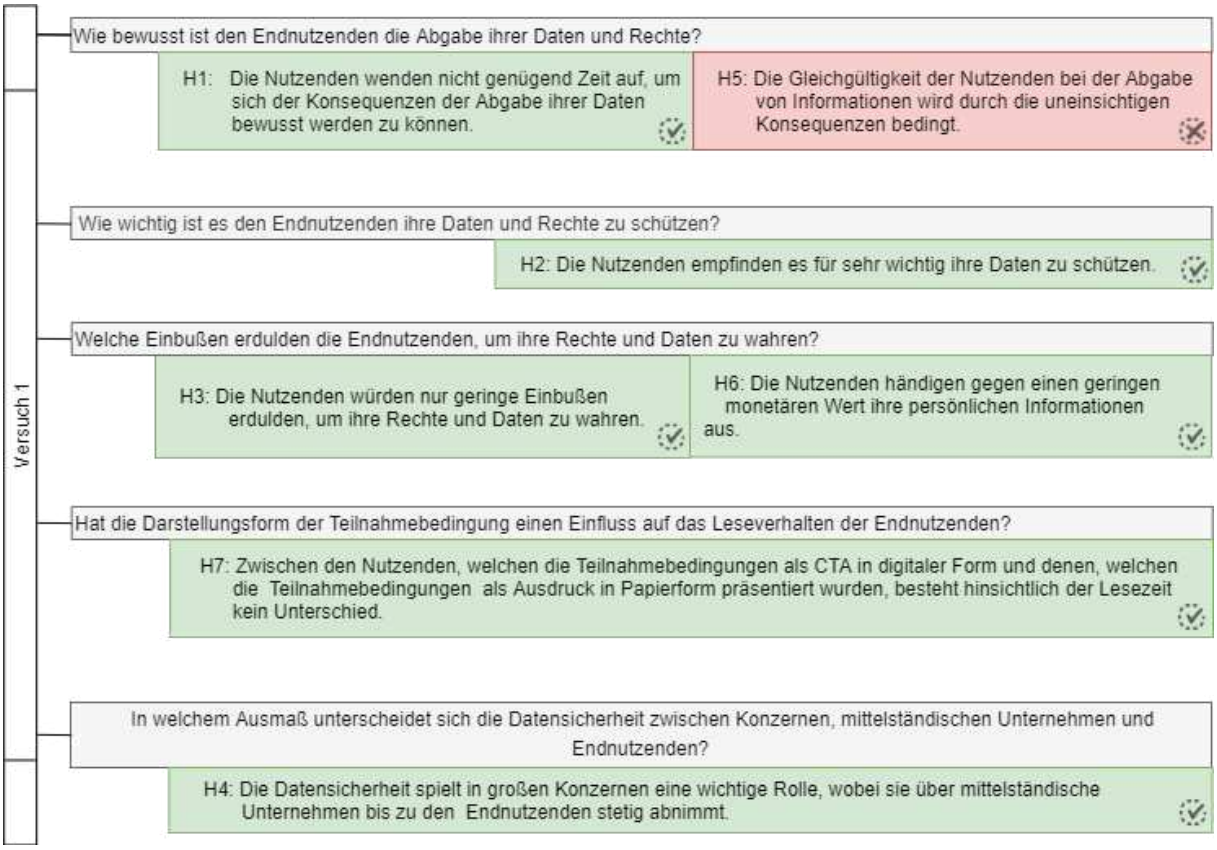


Abbildung 39. Hypothesenübersicht zum ersten Versuch.

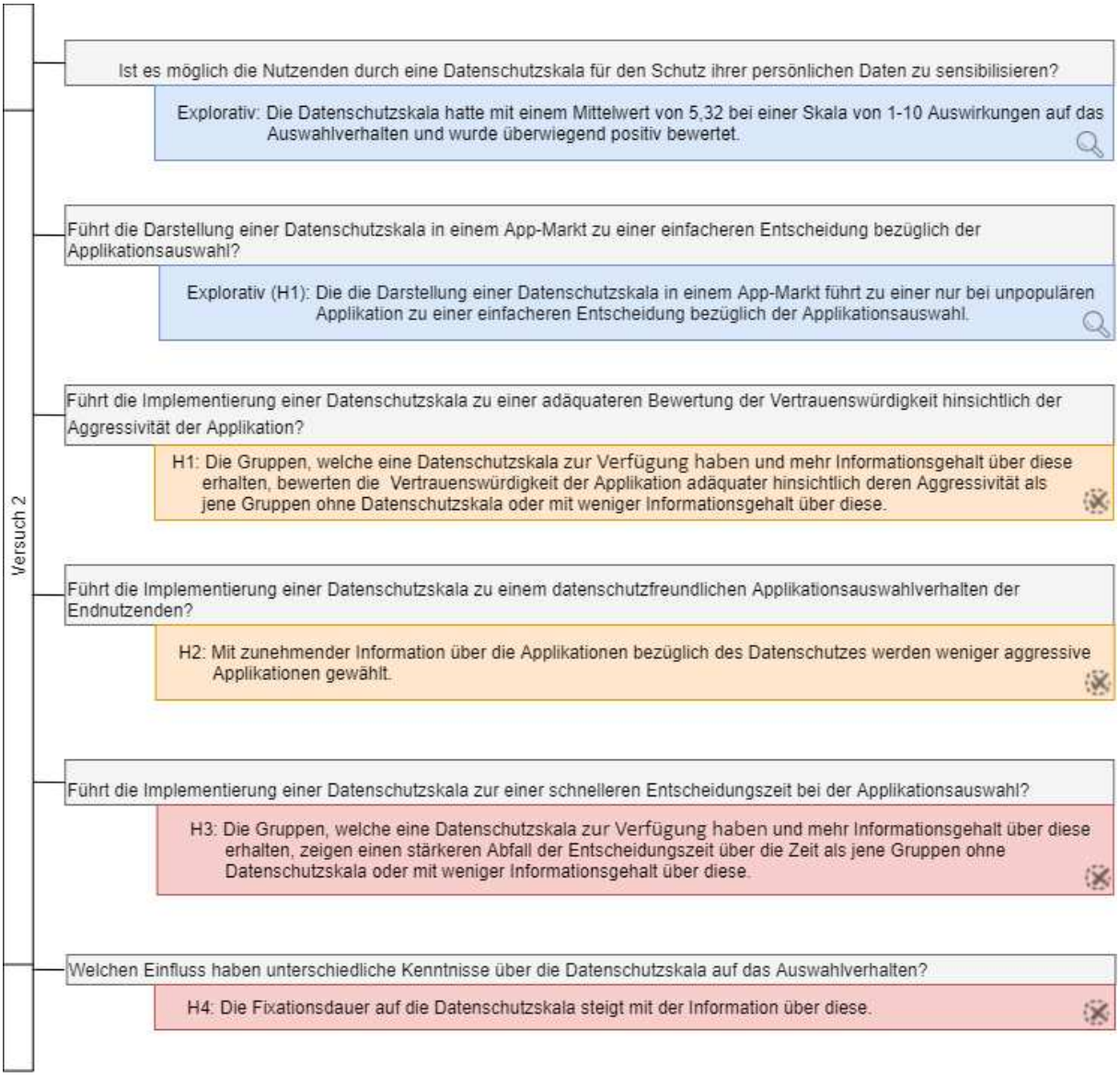


Abbildung 40. Hypothesenübersicht zum zweiten Versuch.

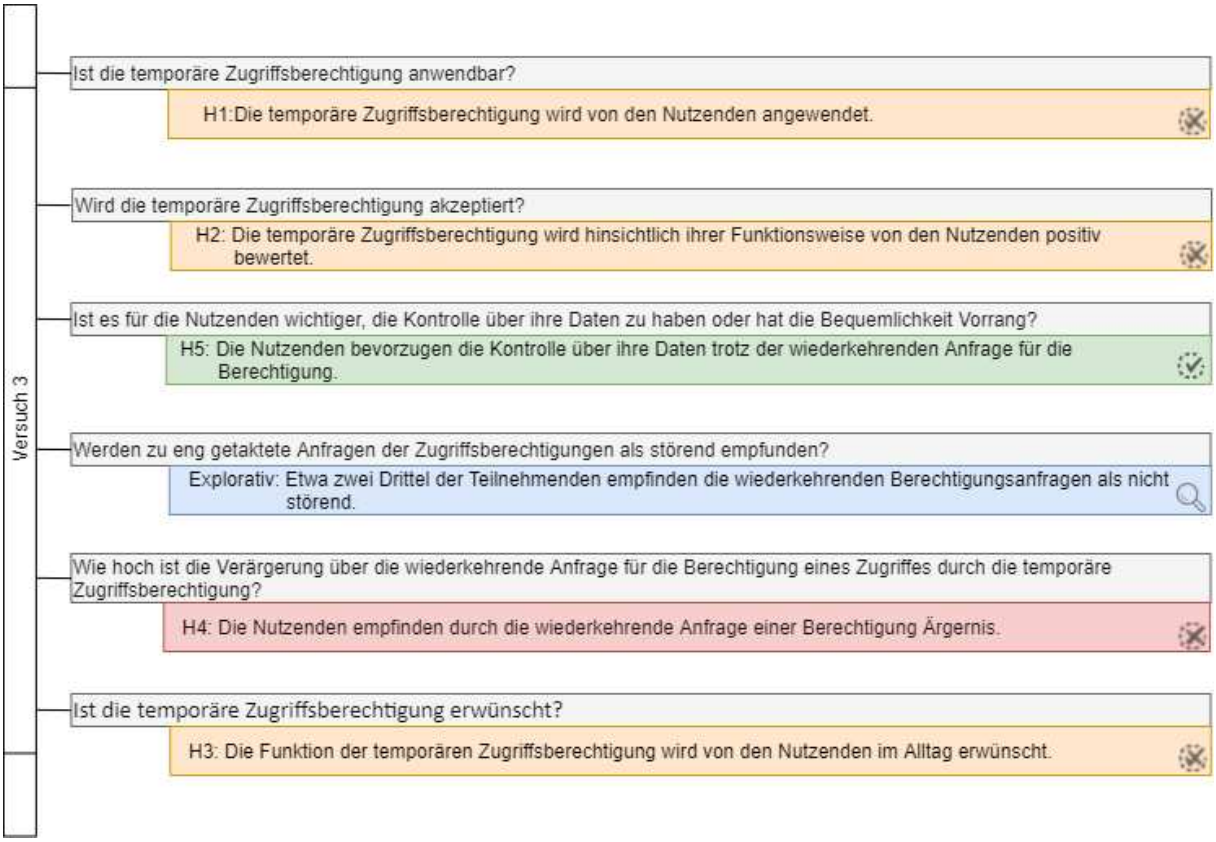


Abbildung 41. Hypothesenübersicht zum dritten Versuch.