infas

Abschlussbericht

Verbraucherinformationen bei Apps – Empirie

Autoren: Robert Follmer, Jana Hölscher, Alexander Markowetz, Ionut Andone

30.11.2017

Auftraggeber:
Projektträger Bundesanstalt für Landwirtschaft und Ernährung (ptble) für
das Bundesministerium der Justiz und für Verbraucherschutz (BMJV)

Projektnummer: 314-06.01-2816EHv002

Projektlaufzeit: 30.05.2017 – 30.11.2017

infas Institut für angewandte
Sozialwissenschaft GmbH

Friedrich-Wilhelm-Straße 18
D-53113 Bonn
Tel. +49 (0)228/38 22-0
Fax +49 (0)228/31 00 71
info@infas.de
www.infas.de

infas

Bericht an

Projektträger Bundesanstalt für Landwirtschaft und Ernährung (ptble)

Referat 314

z. Hd. Herrn Berg

Deichmanns Aue 29

53179 Bonn

Projekt

5826

Bonn, Nov 2017

Fr, Ha

Vorgelegt von

infas Institut für angewandte

Sozialwissenschaft GmbH

Friedrich-Wilhelm-Straße 18

53113 Bonn

Kontakt

Robert Follmer

Bereichsleiter

Tel. +49 (0)228/38 22-0

Fax +49 (0)228/310071

E-Mail r.follmer@infas.de

Autoren

Robert Follmer, Jana Hölscher, Alexander Markowetz, Ionut Andone

infas ist zertifiziert
nach ISO 20252 für die Markt-,
Meinungs- und Sozialforschung

ISO 20252

CERTIFIED BY AUSTRIAN STANDARDS

© infas Institut für angewandte Sozialwissenschaft GmbH
Der Inhalt dieses Berichts darf ganz oder teilweise
nur mit unserer schriftlichen Genehmigung veröffentlicht,
vervielfältigt, gedruckt oder in Informations- und
Dokumentationssystemen (information storage and
retrieval systems) gespeichert, verarbeitet oder ausgegeben
werden.

infas ist Mitglied im
Arbeitskreis Deutscher Markt- und
Sozialforschungsinstitute e.V. (ADM)
und ESOMAR

adm

ESOMAR
member

Inhaltsverzeichnis

1 Ziele und Aufgabenstellung des Projektes 8

2 Planung und Ablauf des Projektes 11

2.1 Projektplanung 12

2.2 Projektablauf 12

3 Wissenschaftlicher und technischer Stand 14

3.1 Überblick zum aktuellen Forschungsstand 14

3.2 Überblick zu relevanten datenschutzrechtlichen Änderungen im Hinblick auf die EU-Datenschutz-Grundverordnung 16

3.3 Technischer Stand 18

4 Material und Methoden 23

4.1 Auswahl der Apps 23

4.2 Vorbereitung und Durchführung der Inhaltsanalyse der Verbraucherinformationen sowie der Datenschutzerklärung 25

4.3 Vorbereitung und Durchführung der technischen Messung 28

4.4 Inhaltliche Analyse der Datenströme 30

4.4.1 Technische Grenzen der Messung 31

4.5 Erstellung eines umfassenden Bewertungsschemas 32

4.5.1 Die Dimension „Im Google Play Store“ 33

4.5.2 Die Dimension „Datenschutzerklärung“ 35

4.5.3 Die Dimension „Installation und Inbetriebnahme“ 37

4.5.4 Die Dimension „Im Betrieb“ 39

4.5.5 Codierung und Gewichtung der Bewertungskriterien 41

4.5.6 Benotung der Dimensionen und Gesamtnote der App 43

5 Darstellung der Ergebnisse 44

5.1 Ergebnisse der Dimension „Im Google Play Store“ 44

5.2 Ergebnisse der Dimension „Datenschutzerklärung“ 47

5.3 Ergebnisse der Dimension „Installation und Inbetriebnahme“ 55

5.4 Ergebnisse der Dimension „Im Betrieb“ 60
5.4.1 Strukturelle Analyse der Datenverbindungen 62
5.4.2 Serviceorientierung in der App 65
5.5 Exkurs: Google versus Apple 68
5.6 Gesamtbewertung der Apps 73

6 Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse 78

7 Zusammenfassung 82

8 Gegenüberstellung der ursprünglich geplanten zu den tatsächlich erreichten Zielen 83

Literaturverzeichnis 84

Anhang 86

Das an diesem Projekt beteiligte Team zeichnet sich durch seine Interdisziplinarität und die daraus entstehenden fachübergreifenden Kompetenzen aus den Bereichen der Soziologie, Informatik, Wirtschaftspsychologie und Politikwissenschaft aus.

An der konzeptionellen Ausarbeitung sowie der inhaltlichen und technischen Durchführung des Projektes beteiligt waren:

Robert Follmer (Dipl. Soziologe)
Alexander Markowetz (PhD Computer Science)
Jana Hölscher (M.A. Soziologie)
Ionut Andone (M.Sc. Computer Science)

Das Projektteam wurde operativ unterstützt durch:
Lara Schneider (B.Sc. Wirtschaftspsychologie)
Simon Werschmöller (B.Sc. Management & Economics)
Lukas Kaechele (M.A. Political Science)

Als externer, juristischer Berater wurde Yoan Hermstrüwer (Dr., Licencié en droit) hinzugezogen.

Im nachfolgenden Bericht wird eine geschlechtsneutrale Sprache verwendet. Sollte aus Gründen der besseren Lesbarkeit nur die männliche Form, zum Beispiel „Nutzer“ oder „Verbraucher“ gewählt sein, sind damit auch immer die weiblichen Personen – die Nutzerinnen und Verbraucherinnen – gemeint.

Der Zugriff auf alle in den Fußnoten angegeben Websites erfolgte zwischen Juni und November 2017.

Abbildungsverzeichnis

Abbildung 1 Projektmodule laut infas-Angebot 11
Abbildung 2 Zeitplan entlang der Meilensteine 12
Abbildung 3 Arbeitsschritte 13
Abbildung 4 Ausgewählte Apps Kategorien 1 bis 5 24
Abbildung 5 Ausgewählte Apps Kategorien 6 bis 10 24
Abbildung 6 Weg des Verbrauchers vom App-Kauf zur Nutzung 33
Abbildung 7 Verständliche Beschreibung der App im Google Play Store 45
Abbildung 8 Bewertung der Dimension „Im Google Play Store“ 46
Abbildung 9 Verfügbarkeit der Datenschutzerklärung in der App 48
Abbildung 10 Bezugnahme auf App in der Datenschutzerklärung 49
Abbildung 11 Bewertung der Dimension „Datenschutzerklärung“ 50
Abbildung 12 „Zugriffsberechtigungen“ in der Datenschutzerklärung 51
Abbildung 13 Bewertung der Dimension „Installation und Inbetriebnahme“ 56
Abbildung 14 Aktive Einwilligung in die Datenschutzbedingungen beim ersten Öffnen der App 57
Abbildung 15 Notwendigkeit eines Nutzerkontos zur App-Nutzung 59
Abbildung 16 Bewertung der Dimension „Im Betrieb“ 60
Abbildung 17 Datensendeverhalten der Apps nach Ländern 63
Abbildung 18 Beispiele für Nutzerfreundlichkeit in der App I 66
Abbildung 19 Beispiele für Nutzerfreundlichkeit in der App II 66
Abbildung 20 Unterschiede: Google Play Store und App Store 69
Abbildung 21 Gesamtbewertung Kategorien 1 bis 5 74
Abbildung 22 Gesamtbewertung Kategorien 6 bis 10 75

Tabellenverzeichnis

Tabelle 1	Bewertungskriterien „Im Google Play Store“	34
Tabelle 2	Bewertungskriterien „Datenschutzerklärung“	36
Tabelle 3	Bewertungskriterien „Installation und Inbetriebnahme“	38
Tabelle 4	Bewertungskriterien „Im Betrieb“	40
Tabelle 5	Beispielbewertung der Kategorie „Vollständigkeit der Datenschutzerklärung“	42
Tabelle 6	Beispielbewertung der Dimension „Datenschutzerklärung“	42
Tabelle 7	Notenschlüssel	43
Tabelle 8	Anteil der Dimensionen an Gesamtnote am Beispiel der App „Focus Online“	43
Tabelle 9	Gesamtbewertung der App-Bereiche	76
Tabelle 10	Bewertungsschritte und Notenskala	86
Tabelle 11	Gesamtübersicht App-Bewertungen (Methodische Erläuterungen siehe Kapitel 4.1 bis 4.5)	87
Tabelle 12	Operationalisierung und Gewichtung der Bewertungskriterien	97

1 Ziele und Aufgabenstellung des Projektes

Applikationen für Smartphones und andere mobile Endgeräte nehmen zunehmend eine wichtige Rolle im Alltag ihrer Nutzer ein und sind für viele Menschen heute der vornehmliche Zugang zum Internet und zu digitalen Dienstleistungen. Viele Unternehmen entwickeln Apps, um den Verbrauchern zum Beispiel Informations-, Shopping- oder Mobilitätsdienste anzubieten. Die zunehmende Relevanz des App-Marktes wird auch durch das starke Wachstum an App-Downloads und der Umsätze der App Stores im dritten Quartal 2017 sichtbar.[1]

Für Apps gelten, wie auch für Websites, umfangreiche Anforderungen an den Daten- und Verbraucherschutz. Verschiedene Studien aus der jüngsten Vergangenheit[2] zeigen, dass bei der Umsetzung dieser Anforderungen häufig erhebliche Mängel bestehen. Hinzu kommt die verbraucherpolitische Herausforderung, dass bei Apps individuelle Nutzer- und Datenschutzeinstellungen oder die Installation von Werbe-Blockern meist nicht möglich sind. Umso wichtiger sind eine umfassende, klare und verständliche Verbraucherinformation bereits vor dem Download der Apps sowie ein sorgsamer und zweckgebundener Umgang mit den Nutzerdaten durch die App-Anbieter.

Die Verbesserung und Stärkung des Verbraucher- und Datenschutzes bei Apps ist ein politischer Schwerpunkt des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV). Die empirische Bestandsaufnahme zu den Verbraucherinformationen und dem Datenschutz bei Apps durch die vorliegende Studie bildet die wissenschaftliche Basis für die verbraucherpolitische Arbeit des BMJV. Ziel der Studie ist daher sowohl Transparenz als auch eine Entscheidungsgrundlage zu schaffen, um daraus verbraucherpolitische Maßnahmen ableiten zu können. Der folgende Bericht soll daher

[1] https://www.appannie.com/de/insights/market-data/global-app-downloads-consumer-spend-hit-q3-2017-recap/
[2] Siehe beispielsweise Stiftung Warentest (2017) oder Moll et al. (2017)

auf Basis von App-Bewertungen einen Überblick über die grundsätzlichen Herausforderungen und Problematiken im Zusammenhang mit der Nutzung von Apps verschaffen. Während bei anderen Studien, wie beispielsweise der Stiftung Warentest, die detaillierte Beurteilung einzelner Apps im Vordergrund steht, zielt die vorliegende Studie darauf ab, mittels der App-Testungen auf übergreifende Problematiken aufmerksam zu machen und erste Empfehlungen daraus abzuleiten. Auf Grundlage der Ergebnisse soll im Rahmen einer Folgestudie eine faire und verbraucherfreundliche Verbraucherinformation im Sinne eines Best-Practice-Beispiels entwickelt werden.

Die konkrete Aufgabenstellung der Studie bestand darin, 200 relevante Apps für den deutschen Markt hinsichtlich der bereitgestellten Verbraucherinformationen und ihrer Datenschutzfreundlichkeit zu überprüfen. Die Auswahl der Apps orientierte sich an 10 unterschiedlichen Angebotskategorien (z. B. „Informationen“, „Spiele“, Musik/Streaming“; gesamte Auswahl siehe Kapitel 4.1), aus welchen jeweils 20 marktrelevante Apps ausgewählt wurden. Nach Rücksprache mit dem Auftraggeber wurden Apps von Autoherstellern, die sich zum Beispiel per Bluetooth mit dem Bordsystem des Autos verbinden, hierbei nicht berücksichtigt.[3]

Im Fokus der Untersuchung der Apps standen:

- die Erläuterung zur Funktionsweise der App im Vorfeld des Downloads,
- die Bereitstellung aller relevanten Informationen im Zusammenhang mit der Nutzung der App, sowohl im Vorfeld als auch während der Nutzung,
- die Vollständigkeit und Datenschutzfreundlichkeit der Datenschutzerklärung,

[3] Für nähere Informationen siehe Stiftung Warentest (2017) „Connected Cars: Die Apps der Autohersteller sind Datenschnüffler“

- die Notwendigkeit der eingeforderten Zugriffsberechtigungen für die Funktionalität der App,
- die Individualisierbarkeit der Datenschutzeinstellungen (z. B. durch Opt-In- bzw. Opt-Out Möglichkeiten) sowie
- das Datensendeverhalten der App.

Bei der Prüfung des Datensendeverhaltens im Rahmen eines experimentellen Versuchsaufbaus sollte ebenfalls beurteilt werden, ob die bereitgestellten Verbraucher- und Datenschutzinformationen mit dem tatsächlichen Verhalten der App übereinstimmen. Daher wurden die Ergebnisse der Datenkommunikation – sofern möglich – auch inhaltlich analysiert und mit den Angaben in der Datenschutzerklärung der App-Anbieter verglichen. Schließlich sollte auch die Darstellung und Informationsaufbereitung im App Store und innerhalb der App bewertet werden.

In den folgenden Kapiteln werden die angewandte Methodik und die Ergebnisse der Studie ausführlich beschrieben.

2 Planung und Ablauf des Projektes

Nach Beauftragung des Projektes fand Ende Juni zunächst eine Projektauftaktsitzung mit dem Auftraggeber statt. Dort wurde das von infas erarbeitete Konzept zur Durchführung der Studie (siehe Abbildung 1) vorgestellt und der Projektansatz anhand einer Präsentation erläutert. Im Rahmen dieser Sitzung wurden auch die Beschränkungen sowie Möglichkeiten der technischen Messung thematisiert und mit dem Auftraggeber abgestimmt (siehe Kapitel 4.4).

Abbildung 1 Projektmodule laut infas-Angebot

Neben der Testung von 200 Android-Apps wurden zusätzlich 20 ausgewählte Apps auf einem iOS-Betriebssystem einbezogen. So wurden neben dem Vergleich der beiden App Stores von Google und Apple hinsichtlich der Verbraucherinformationen auch die Funktionalität und das Datensendeverhalten der 20 Apps im Vergleich zu den Android-Versionen geprüft. Des Weiteren wurde für das Projekt festgelegt, die Anzahl der zu testenden kostenpflichtigen Apps je nach Kategorie auf eine sinnvolle Anzahl (gemessen an der Marktrelevanz) zu begrenzen (siehe Kapitel 4.1).

2.1 Projektplanung

Für die Studie war ein Zeitbedarf von sechs Monaten ab Auftragsvergabe vorgesehen. In Abbildung 2 sind alle Meilensteine und der zeitliche Ablauf grob dargestellt. Die einzelnen Arbeitsschritte lassen sich in weitere Unterarbeitsschritte aufteilen, die in Kapitel 2.2 näher erläutert werden.

Abbildung 2 Zeitplan entlang der Meilensteine

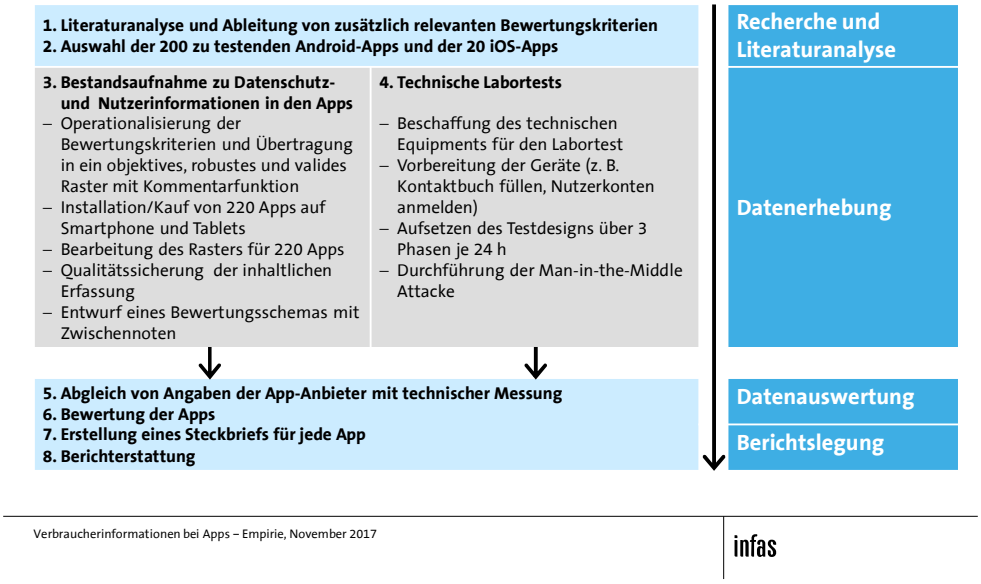
Meilensteine	erl.	Juni	Juli	August	Sept.	Oktober	Nov.
Projektauftakt mit Auftraggeber	√	X					
Literaturrecherche	√	X					
Auswahl der Apps und Kategorien	√	X	X				
Entwicklung des Erfassungs- und Bewertungsrasters	√	X	X	X			
Bestandsaufnahme zu Datenschutz- und Nutzerinformationen in den Apps	√		X	X	X		
Zwischenbericht	√			X			
Technische Labortests	√		X	X	X		
Dokumentation der Labortests und Bewertung der Apps	√				X	X	
Abschlussgespräch	√					X	
Berichterstattung	√						X

Verbraucherinformationen bei Apps – Empirie, November 2017 infas

2.2 Projektablauf

Der Projektablauf orientierte sich an den dargestellten Arbeitsschritten (siehe Abbildung 3). Vor der eigentlichen Phase der Datenerhebung wurden zunächst Recherchen und Literaturanalysen durchgeführt, um an den wissenschaftlichen Forschungsstand anzuknüpfen (siehe Kapitel 3). Im Anschluss erfolgte die Auswahl der 200 Android- sowie der 20 iOS-Apps. Die Bestandsaufnahme zu Datenschutz- und Nutzerinformationen auf der einen Seite sowie die technischen Labortests auf der anderen wurden parallel von jeweils spezialisierten Teams durchgeführt, die jedoch jederzeit miteinander in Austausch zu den einzelnen Arbeitsschritten und Zwischenergebnissen standen.

Abbildung 3 Arbeitsschritte



Nach der Phase der Datenerhebung wurden die Ergebnisse der Inhaltsanalyse und der technischen Messung miteinander verglichen und in ein gemeinsames Bewertungsschema überführt (siehe Kapitel 4.5). Im Rahmen einer umfassenden Qualitätssicherung wurden die Ergebnisse noch einmal von der Projektleitung überprüft. Am Ende der Datenauswertung erfolgte die Benotung der einzelnen Apps anhand der festgelegten Dimensionen des Bewertungsschemas. Die Ergebnisse der Dimensionen wurden schließlich zu einer App-Gesamtnote zusammengefasst.

3 Wissenschaftlicher und technischer Stand

Im Vorfeld der konkreten Ausgestaltung des Studienkonzepts wurde eine Literaturanalyse durchgeführt, um sowohl einen Überblick zum aktuellen Forschungstand als auch über die für Verbraucher und App-Anbieter relevanten rechtlichen Rahmenbedingungen zu erhalten. Die durchgeführte Studie ist hinsichtlich der Anzahl der Apps sowie der Anzahl der überprüften Kriterien nach unserer Kenntnis bisher einmalig. Vorliegende Studien zum Thema App-Testung konzentrieren sich zumeist auf einzelne Schwerpunkte, wie beispielsweise Kinder- oder Fitness-Apps. Im Kapitel 3.1 wird ein Überblick zu verwandten Forschungsvorhaben und deren Ergebnissen gegeben.

Ab Mai 2018 werden die datenschutzrechtlichen Standards durch das Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO) modernisiert und für alle Länder der EU vereinheitlicht. Ziel der DSGVO ist der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, vor allem deren Recht auf Schutz ihrer personenbezogenen Daten, und der freie Verkehr personenbezogener Daten. Die Neuerungen gegenüber dem bisher geltenden nationalen Recht betreffen sowohl die tätigen Unternehmen als auch die Bürger innerhalb der EU. In Bezug auf personenbezogene Daten im Rahmen der App-Nutzung werden einige Änderungen von besonderer Wichtigkeit für App-Entwickler sein. Im Kapitel 3.2 wird erläutert, welche Kriterien im Bewertungsschema sich an diese relevanten Neuerungen anlehnen.

3.1 Überblick zum aktuellen Forschungsstand

Die Anzahl der Studien, die sich mit der Testung von Apps beschäftigen, ist insgesamt noch relativ begrenzt. Allerdings ist auffällig, dass die Thematik insbesondere in den letzten Jahren an Relevanz gewinnt und sowohl im medialen als auch wissenschaftlichen Diskurs zunehmend Raum einnimmt. Die Studien, die wir im Hinblick auf den eigenen Forschungsansatz als be-

sonders interessant eingestuft haben, lassen sich grob in folgende inhaltliche Schwerpunkte einteilen:

- Untersuchung von Apps im Hinblick auf verbraucherschutzrelevante Themen, Datenschutz und/oder Datensicherheit (vgl. u. a. Herrmann und Lindemann 2016, Moll et al. 2017) mit teilweise unterschiedlicher Schwerpunktsetzung wie z. B. Kinder-Apps (vgl. Stiftung Warentest 2017), Fitness-Apps (vgl. Verbraucherzentrale NRW e. V. 2017) oder Social-Apps (vgl. Forbrukerrådet 2016),
- Erarbeitung von Richtlinien zu Datenschutzanforderungen bei Apps und Darstellung von Best-Practice-Fällen (vgl. u. a. Düsseldorfer Kreis 2014, BMJV 2017),
- Verbraucherinformationen und Hinweise zum Umgang bzw. der Verbesserung des Datenschutzes (MOBILSICHER 2017) sowie
- internationale Studien im Hinblick auf Datenschutz und Datensicherheit bei Apps (vgl. Forbrukerrådet 2016, Zang et al. 2015).

Die Methoden, die im Rahmen der Studien eingesetzt wurden, ähneln sich. Die am häufigsten verwendeten Methoden sind:

- Textanalysen, zum Beispiel von allgemeinen Geschäftsbedingungen, Nutzungsbestimmungen oder Datenschutzerklärungen,
- technische Prüfungen oder Messungen, zum Beispiel durch Erfassung des Datenverkehrs, Untersuchung des Datenspeicherverhaltens oder Tracking durch Bluetooth-Verbindung,
- Überprüfung von Apps im Rahmen der aktiven Nutzung und
- repräsentative Befragungen von Nutzern zu ihrem eigenen Verhalten oder ihrem Wissensstand.

In allen Studien wurden bei der überwiegenden Anzahl der geprüften Apps deutliche Mängel und ein dringender Handlungsbedarf beim Umgang mit personenbezogenen Nutzerdaten und/oder in Bezug auf die Datensicherheit festgestellt.

Als problematisch einzustufen sind laut bisheriger Studien vor allem die folgenden Aspekte:

- die unzureichende Verbraucheraufklärung, zum Beispiel über die Weitergabe von (sensiblen) Daten an Dritte,
- die fehlende Einhaltung technischer Standards zum Schutz der Nutzerdaten sowie mangelhafte Schutzmechanismen,
- die fehlende Möglichkeit der Nutzer zur Kontrolle oder Regulierung der eigenen Daten,
- die Diskrepanz zwischen den in den Datenschutz- und Nutzungsbedingungen ausgewiesenen Bestimmungen der Datennutzung und dem tatsächlichen Verhalten der Apps,
- die Mängel beim Kinder- und Jugendschutz, beispielsweise im Hinblick auf Werbeeinblendungen oder besonderes teure In-App-Käufe sowie
- die fehlende Kompatibilität mit den deutschen oder europäischen Verbraucher- und Datenschutzgesetzen, zum Beispiel hinsichtlich einer freiwilligen und informierten Einwilligung der Verbraucher.

Vor dem Hintergrund der Erkenntnisse aus anderen wissenschaftlichen Studien war davon auszugehen, dass sowohl die Ergebnisse der inhaltlichen Testung der Verbraucherinformationen als auch die Messung des Datensendeverhaltens deutliche Mängel bei den 200 geprüften Apps aufdecken würden.

3.2 Überblick zu relevanten datenschutzrechtlichen Änderungen im Hinblick auf die EU-Datenschutz-Grundverordnung

Bei der Entwicklung des im Rahmen dieser Studie angewendeten Bewertungsrasters wurden im Hinblick auf die Datenschutzerklärungen der App-Anbieter einige Prüfkriterien festgelegt, die mit dem Eintreten der Wirksamkeit der EU-Datenschutz-Grundverordnung (DSGVO) im Mai 2018 voraussichtlich an Relevanz gewinnen werden. Diese werden im Folgenden näher erläutert (vgl. hierzu Bitcom e. V. 2016).

Die *Informations- und Auskunftspflichten* (Art. 13, 14 und 15 DSGVO) werden um Angaben über Datennutzung und -verarbeitung erweitert. Dies bedeutet, dass die App-Anbieter unter anderem verpflichtet sein werden, Informationen zur Rechtsgrundlage zu geben, auf die sich die Datenverarbeitung stützt. Des Weiteren müssen sie Angaben zur Dauer der Speicherung personenbezogener Daten oder zumindest zu den Kriterien über die Festlegung der Dauer geben. Sollten sich die Zwecke der Datenverarbeitung ändern, muss der App-Anbieter darüber erneut Informationen bereitstellen. Das Bewertungsraster umfasste daher die Kriterien „Zweck der Verarbeitung der personenbezogenen Daten", „Angaben zur Speicherdauer" und „Begrenzung der Speicherdauer".

An den vorigen Punkt knüpft auch die neue *Regelung zur Zweckbindung* (Art. 5 DSGVO) an. Die DSGVO sieht vor, dass eine Weiterverarbeitung der Daten nur erlaubt ist, wenn sie „mit dem ursprünglichen Zweck vereinbar ist". Wie eng diese Formulierung ausgelegt wird, bleibt abzuwarten. Neben der Angabe von Zwecken bei der Nutzung von personenbezogenen Daten in der Datenschutzerklärung, wurde auch die Angabe von Zwecken bezüglich der eingeholten Zugriffsberechtigungen in das Raster aufgenommen.

In der DSGVO werden zudem die Anforderungen an eine *freiwillige und informierte Einwilligung* erhöht (Art. 4 Nr. 11 und Art. 7 DSGVO). Die Erteilung der Einwilligung erfordert eine eindeutige Handlung des Nutzers, zum Beispiel durch das Anklicken eines Kästchens. Die Untätigkeit des Nutzers dürfte im Gegensatz dazu wohl keine wirksame Einwilligung mehr darstellen (Art. 25 II DSGVO und Erwägungsgrund 32 DSGVO). Bei der Überprüfung der Datenschutzerklärungen wird daher bewertet, ob der App-Anbieter (sofern personenbezogene Daten verarbeitet werden) eine aktive Zustimmung des Nutzers, zum Beispiel beim ersten Öffnen der App oder bei einer Änderung der Datenschutzbestimmungen, einholt.

Darüber hinaus enthält die DSGVO eine neue Verpflichtung zur *Datenübertragbarkeit* (Art. 20 DSGVO). Nutzer haben das Recht, die von ihnen

bereitgestellten personenbezogenen Daten in einem gängigen und maschinenlesbaren Format zu erhalten. Sofern die Annahme nahe liegt, dass die Anforderungen für Datenübertragbarkeit bei dem jeweiligen geprüften App-Anbieter in Zukunft eine Rolle spielen könnten, wird die Datenschutzerklärung hinsichtlich einer Information darüber geprüft.

3.3 Technischer Stand

Zum Messen des Verhaltens von Apps auf Mobiltelefonen stehen prinzipiell zwei Methoden zur Verfügung: der „White-Box-Ansatz“ und der „Black-Box-Ansatz“. Beim White-Box-Ansatz werden die Vorgänge direkt auf dem Smartphone untersucht, beispielsweise welche Funktionen durch welche Apps aufgerufen werden, während beim Black-Box-Ansatz die vom Smartphone versandten Daten inspiziert werden, nicht jedoch die Vorgänge in dem Gerät selber. Beide Ansätze verfügen über spezifische Vor- und Nachteile.

Beim White-Box-Ansatz werden die tatsächlichen Vorgänge auf dem Smartphone gemessen. Diese sind dabei eindeutig einzelnen Apps zuzuweisen. Allerdings müssen die Smartphones hierfür speziell präpariert werden. Dabei ist es insbesondere nötig, sich die Rechte eines „Superusers“ zu verleihen. Dieser Vorgang nennt sich “rooten” (Android) oder “jailbreaking” (iOS). An dieser Stelle zeigt sich der zentrale Nachteil des White-Box-Ansatzes. Manche Apps erkennen, wenn sie auf einem gerooteten Smartphone installiert sind und verweigern in diesem Fall den Dienst. Gängige Beispiele hierfür sind Netflix, Pokémon oder sämtliche Banking-Apps. Würden sie auf einem gerooteten Smartphone laufen, könnten die Apps betrogen werden, oder die Sicherheit des Banking wäre kompromittiert. Allerdings gibt es auch Apps, die gezielt spähen, ob sie in einem Testszenario ausgeführt werden. Es ist also nicht auszuschließen, dass Apps auf einem gerooteten Telefon zwar nicht den Dienst verweigern, jedoch kontroverses Verhalten unterlassen. In diesem Fall wäre eine White-Box-Testmethode leicht irrezuführen.

Beim Black-Box-Ansatz wird hingegen der aus einem Smartphone ausgehende Datenverkehr analysiert. Der zentrale Vorteil dieser Methode liegt darin, dass das Smartphone nur marginal präpariert werden muss. Die App kann also nur schwer erkennen, ob sie in einem Testszenario läuft. Ein Nachteil ist jedoch, dass der ausgehende Verkehr des Geräts nicht zwingend einzelnen Apps zuzuordnen ist. Prinzipiell sendet das Smartphone auch eigenständig Daten an Google, den Hersteller oder gar den Chip-Hersteller. Im Nachhinein müssen die Datenströme dann in diejenigen separiert werden, die der zu beobachtenden App zuzuordnen sind, und diejenigen, die dem Hintergrundrauschen des Smartphones zugeordnet werden müssen. Hierbei gibt es zwei Fehlerquellen: Zum einen können Datenströme als nicht app-spezifisch kategorisiert werden, obwohl sie es eigentlich wären (False Negatives), zum anderen können Datenströme als app-spezifisch kategorisiert werden, die eigentlich von dem Smartphone selber oder von anderen Apps stammen (False Positives).

Der Netzwerkverkehr erlaubt es meistens, die Besitzer der kontaktierten Server zu identifizieren. Dies geschieht entweder anhand der Whois-Datenbank oder anhand von Informationen im Netzwerkprotokoll. Darüber hinaus ist es – mit Einschränkungen – möglich, aus der IP-Adresse eines Servers auf dessen Standpunkt zu schließen. Ist der Verkehr zwischen dem Server und dem Smartphone verschlüsselt, wird zwischen zwei Methoden unterschieden. Im Allgemeinen verlassen sich Server-Betreiber auf die auf dem Telefon befindlichen Root-Zertifikate. Diese autorisieren andere Zertifikate (Schlüssel) als vertrauenswürdig. Wird nun händisch ein weiteres Root-Zertifikat eingespielt, so kann damit eigenen Zertifikaten die Vertrauenswürdigkeit bestätigt werden. Dies ermöglicht eine Entschlüsselung mittels einer sogenannten „Man-in-the-Middle-Attacke“. Einige Apps verlassen sich jedoch nicht auf die Bestätigung durch Root-Zertifikate, sondern verwenden ausschließlich eigene, eingebettete Zertifikate im Rahmen des sogenannten „Certificate Pinning“. Eine solche Netzwerkverbindung ist als nicht zu entschlüsseln zu betrachten. Da der Aufwand für Certificate

Pinning relativ hoch ist, benutzen nur solche Apps diese Methode, die entweder spezielle Sicherheitsanforderungen haben (Banking) oder deren Hersteller, wie z. B. Facebook, über signifikante Ressourcen verfügen. Ad-Networks und Spyware nutzen üblicherweise kein Certificate Pinning.

Der Inhalt der Netzwerkverbindungen ist entweder binär oder textuell kodiert. Binäre Formate übersetzen Daten in Abfolgen von Nullen und Einsen, sind menschlich nicht sinnvoll zu interpretieren und im Kontext dieser Studie als nicht zu entziffern zu betrachten. Textformate hingegen nutzen lange Buchstabenfolgen. Diese sind im Allgemeinen auch nicht für menschliche Leser gedacht, es können jedoch Teile der Buchstabenfolgen, wie etwa Namen oder Zahlen, identifiziert werden. Dies kann auch maschinell erfolgen, indem nach Teil-Folgen mit bestimmten (regulären) Mustern gesucht wird.

Trotz eines Black-Box-Verfahrens sind basale Einsichten in das Verhalten von Android Smartphones und iPhones für das Verständnis dieser Studie von Vorteil. Die beiden Plattformen unterscheiden sich technisch deutlich. Android ist höchst fragmentiert. Es gibt verschiedenste Hersteller von Android Smartphones sowie der darin verbauten Chips. Gemeinsam mit dem Mobilfunkanbieter installieren diese eine Vielzahl unterschiedlichster ROMs bzw. Firmware-Versionen. Von Android selber existieren verschiedenste Versionen parallel. Die Gerätehersteller ersetzen oft zentrale System-Apps (z. B. den Dialer) oder die Benutzeroberfläche (z. B. Samsungs TouchWiz). Auf den Smartphones werden teilweise durch Hersteller oder Mobilfunkanbieter Apps vorinstalliert. Sie selber verfügen über unterschiedliche Fähigkeiten bzw. Sensoren. Das iPhone ist im Vergleich deutlich homogener. Hardware und ROMs werden ausschließlich durch Apple beauftragt. Es existieren nur relativ wenige Modelle. Eine Fragmentierung ist nicht zu konstatieren. Die beiden Plattformen unterscheiden sich zudem in der Herkunft der installierbaren Apps. Unter Android können nicht nur Apps aus dem offiziellen Google Play Store installiert werden, sondern auch von beliebigen Drittanbietern. Darüber hinaus sind Apps bereits oft

werksseitig vorinstalliert. Diese lassen sich im Allgemeinen nicht deinstallieren. Es ist jedoch möglich, ihnen die Zugriffsberechtigung auf Sensoren zu entziehen und so ein Ausspionieren durch solche Apps zu erschweren. Auf iPhones sind vorinstallierte Apps hingegen selten und Apps von Drittanbietern lassen sich in der Regel nicht installieren.

Android lässt dem Smartphone-Hersteller, dem Programmierer und dem Nutzer mehr Freiheiten, um zum Beispiel Software zu installieren oder auf Funktionen des Gerätes zuzugreifen. Dies bedeutet jedoch, dass Android-Telefone im Gegensatz zu iPhones über ein größeres Potential für Schadsoftware verfügen, zum Beispiel für Tracker und Spyware. Im Gegensatz zu iOS erlaubt Android beispielsweise, einer App zu sehen, (1) welche anderen Apps installiert sind, (2) welche anderen Apps gerade aktiv sind, (3) wie das aktuelle WLAN heißt, (4) wenn sich dieses ändert und (5) wie MAC-Adresse und Seriennummer (IMEI) des Smartphones lauten. Auf iOS sind diese Operationen gar nicht oder nur unter bestimmten Bedingungen möglich. Darüber hinaus verhindert iOS, dass Apps im Hintergrund weiterlaufen (und dabei Daten über den Nutzer sammeln). Konkret bedeutet dies, dass eine App einige Stunden nach der letzten Nutzung durch das Smartphone beendet wird. Wenn ein Nutzer eine App nicht täglich verwendet, ist es dieser folglich nicht möglich, ihn langfristig zu tracken. Die Gründe für diese Restriktion mögen mannigfaltig sein, de facto unterbindet Apple somit jedoch Hintergrundaktivitäten (z. B. Tracking). Android erlaubt solche Hintergrundaktivitäten.

Ein besonderes Augenmerk gilt auch dem Erstellen von Mobilitätsprofilen durch Apps. Prinzipiell erlaubt das in Mobiltelefonen verbaute GPS-Modul eine hochpräzise Ortung des Nutzers. Allerdings muss dieser der App explizit eine Zugriffsberechtigung auf das GPS-Modul gewähren. Ist dies aber einmal geschehen, beispielsweise weil die App einen Filialfinder anbietet, kann sie über Monate hinweg ein präzises Bewegungsprofil erstellen. Die Ortung eines Nutzers ist jedoch nicht nur ausschließlich mittels des GPS-Moduls möglich. Selbst wenn die Zugriffsberechtigung auf dieses nicht

erteilt wurde, bleiben eine ganze Reihe an Möglichkeiten, den Standort des Smartphones zu ermitteln. So kann eine App die Position anhand der verfügbaren WLAN-Netzwerke und Bluetooth-Verbindungen bestimmen. Darüber hinaus kann ein Smartphone prinzipiell über die Signalstärke der Mobilfunkzelle den Standort eingrenzen. Anhand der durch den Mobilfunkbetreiber vergebenen IP-Adresse lässt sich der Standort zumindest auf eine Region eingrenzen. Des Weiteren lassen sich durch den DNS-Service Rückschlüsse auf den Standort schließen, mitunter auch bis zur Genauigkeit von Städten. Anhand des Mobilfunkbetreibers lässt sich zudem das Land bestimmen, in dem sich der Nutzer befindet. Das Erstellen von Mobilitätsprofilen ist also – mehr oder minder präzise – jeder App möglich.

4 Material und Methoden

4.1 Auswahl der Apps

Gemäß der Studienbeschreibung sollten jeweils 20 Apps aus 10 unterschiedlichen Angebotsgruppen untersucht werden. Auch die Prüfung kostenpflichtiger Apps war hierbei vorgesehen. Auf eine festgelegte Anzahl kostenpflichtiger Apps wurde jedoch in Abstimmung mit dem Auftraggeber verzichtet, da die Marktrelevanz je nach Kategorie sehr unterschiedlich ist und der Markt insgesamt von kostenfreien Apps dominiert wird.

Die sechs durch die Ausschreibung vorgegebenen Angebotsgruppen umfassten die folgenden Kategorien:

- Informationen
- Spiele
- Messenger, Mails und Soziale Netzwerke
- Shopping/E-Commerce
- Musik/Streaming
- Apps für Kinder

Diese wurden durch die folgenden Kategorien ergänzt:

- Fitness/Gesundheit
- Banking/Finanzdienstleistungen
- Utilities/Tools
- Travel/Navigation/Mobilität

Innerhalb der einzelnen Kategorien sollten die verschiedenen Apps sowohl eine hohe Marktrelevanz aufweisen als auch ein möglichst breites Spektrum an Nutzungsfunktionen abdecken. 17 Apps waren bereits durch die Ausschreibung festgelegt (siehe Abbildung 4 und 5). Zur Auswahl der weiteren Apps wurden sowohl die Ranglisten des Google Play Stores als auch die Rangliste des Unternehmens „App Annie“ herangezogen.

„App Annie“ gehört seit 2010 zu den weltweit führenden Unternehmen bei der Marktanalyse von Apps und digitalen Gütern. Die Onlineplattform des

Unternehmens stellt seinen Nutzern nach einmaliger Registrierung sogenannte „Top App-Charts“ zur Verfügung, in denen alle Apps über deren Downloadanzahl und Nutzungsgrad anhand eines Algorithmus gerankt werden. Optional kann nach verschiedenen Auswahlkriterien, zum Beispiel Betriebssystem, Land und Kategorie, gefiltert werden. Die Tagesaktualität der Rankings kann zu Schwankungen der App-Platzierungen führen, wodurch auch die Aktualität der Ranglisten während des gesamten Projektzeitraumes variierte. Deshalb wurden als weitere Kriterien zur Bestimmung der zu untersuchenden Apps die Angaben über weltweite Installationszahlen im Google Play Store als auch die inhaltliche Maßgabe nach möglichst hoher Varianz innerhalb der einzelnen Kategorien herangezogen.

Abbildung 4 Ausgewählte Apps Kategorien 1 bis 5

Apps nach Kategorien	Informationen	Spiele	Messenger/ Soziale Netzwerke	Shopping	Musik/TV/ Streaming
	BBC NEWS	Angry Birds Rio	Askfm	*Amazon**	Amazon Music
	BILD APP	*Candy Crush Saga**	E-POST	ASOS	Apple Music
	Der Postillon	Castle Crush	*Facebook*	CONRAD	ARD Mediathek
	finanzen.net	*Clash of Clans*	*Facebook Messenger*	eBay	Audible
*auch auf iOS getestet	Focus Online	Farming Simulator 18	Gmail	*Ebay Kleinanzeigen**	Deezer
	iKiosk	Hay Day	*Instagram**	Groupon	JustWatch
	KATWARN	Ich Einfach Unverbesserlich	Jodel	H&M	maxdome
	kicker	*Minecraft Pocket Edition*	LOVOO	Hornbach	Musical.ly
Blau markiert: kostenpflichtige Apps	meinestadt.de	Mini Metro	Parship	IKEA Store	Napster
	n-tv Nachrichten	Modern Combat 4: Zero	Pinterest	kaufDA	Netflix
	Promiflash News	*Piano Tiles 2*	QQ International	Kleiderkreisel	ProSieben
	Relay for reddit (PRO)	Plants vs. Zombies	*Skype*	Lidl	radio.de
Kursiv gesetzt: Apps laut Ausschreibung	Reuters News	*Pokémon GO*	*Snapchat*	LIEFERHELD	Samsung Smart View
	SPIEGEL ONLINE*	Pou	Threema	marktguru	Shazam
	Tagesschau	Quizduell Premium	Tinder	OTTO	Sky Go
	WeatherPro	*Solitaire*	Twitter	reBuy	*Spotify Music**
	wetter.com	*Subway Surfers*	WEB.DE Mail	Saturn Deutschland	Tv Spielfilm
	WetterOnline	The Amazing Spider-Man	WeChat	*Shpock*	Ultimate Guitar Tabs
	WetterOnline Pro	Wort Guru*	*WhatsApp**	Wish	YouTube*
	ZDFheute	Wort Meister	Wire	Zalando	ZDFmediathek

Verbraucherinformationen bei Apps – Empirie, November 2017

Abbildung 5 Ausgewählte Apps Kategorien 6 bis 10

Apps nach Kategorien	Apps für Kinder	Fitness/Gesundheit	Banking/Finanz-Dienstleisung	Tools	Travel/Navigation
	BRIO World	30 Tage Fitness Challenge	aboalarm	Adobe Acrobat Reader	ADAC Camping
	Conni lesen	7-Minuten-Training	Bruno	Avira Antivirus	Airbnb
	Cooking Fever*	Apothekenfinder	CHECK24 Vergleiche	Babyphone 3G	BlaBlaCar
	Die Eiskönigin	Arztsuche jameda	Clark Versicherungen	barcoo*	Booking.com
	DieMaus	Die TK-App	Deutsche Bank Mobile	Blitzer.de Plus	DB Navigator*
	Disney Magic Kingdoms	EAT SMARTER - Rezepte	Friendsurance	DHL Paket	DriveNow Carsharing
*auch auf iOS getestet	Dragon Ball Z Dokkan	Einzigartiges Pulsmessgerät	HUK Reise	Dropbox*	FlixBus Fernbus App
	Duolingo*	Erste Hilfe DRK	Klarna	facetune	Google Maps
	FIFA Mobile Fußball	Fitbit*	LVM	Google Chrome	komoot
Blau markiert:	Goodgame Empire	HiPP Baby App	Mein Haushaltsbuch	Google Übersetzer	Lufthansa
kostenpflichtige Apps	Kinder Gehintrainer	Lifesum	MeineFinanzen	ImmobilienScout24	Miles & More
	LEGO City My City 2	Menstruations-Kalender	Money Manager	LEO Wörterbuch	PeakFinder Earth
	Malen und Zeichnen!	MyFitnessPal	PAYBACK	Mein Wecker	Plane Finder
	Monopoly Game	Oje, ich wachse	PayPal*	Samsung Smart Switch	Ryanair
	Nickelodoen Play	Periodenkalender	paysafecard	SD Maid Pro	Skyscanner
	PAW Patrol	Runtastic Laufen	Sparkasse*	Speed View GPS Pro	TomTom GO Mobile*
	Scribblenauts Remix	Runtastic PRO	Sparkasse+	Super Cleaner	TripAdvisor*
	SimCity BuildIt	Sleep Cycle alarm clock	StarMoney Phone	Taschenlampe	trivago
	Temple Run	Weight Watchers Mobile	Währungsrechner	VPN Master	Uber*
	Toca Kitchen 2	YAZIO	WebIDent	Wasserwaage PRO	Urlaubspiraten

Verbraucherinformationen bei Apps – Empirie, November 2017

Nach der Auswahl der 200 Android-Apps wurden aus diesen 20 Apps für die zusätzliche iOS-Testung ausgewählt. Diese erfolgte, um zentrale Unterschiede zwischen Google und Apple hinsichtlich des Zugangs zu Verbraucherinformationen und des Datensendeverhaltens aufzuzeigen.

4.2 Vorbereitung und Durchführung der Inhaltsanalyse der Verbraucherinformationen sowie der Datenschutzerklärung

Bei der Erstellung des inhaltlichen Bewertungsschemas für die ausgewählten Apps war zu berücksichtigen, dass

- alle in der Ausschreibung relevanten Kriterien erfasst werden,
- alle zusätzlich durch Literaturrecherchen als wichtig eingestuften Kriterien erfasst werden,
- eine objektive Vorgehensweise bei der Bewertung ermöglicht wird, um subjektive Einschätzungen der Prüfer zu vermeiden sowie
- die einzelnen Kriterien mit einer einfachen, robusten Operationalisierung erfasst werden, damit die Prüfung von mehreren Personen parallel vorgenommen werden kann und replizierbar ist.

Insgesamt wurde bei der inhaltlichen Prüfung der Zugänglichkeit und Nutzerfreundlichkeit der Verbraucherinformationen die Perspektive durchschnittlicher Nutzer eingenommen, die weder über besondere technische noch juristische Kenntnisse verfügen. So konnten die Nutzung des App Stores, der Downloadprozess und das Zurechtfinden innerhalb der App möglichst realitätsnah simuliert werden (Stichwort „Adressatengerechtigkeit“). Bei der Erstellung des Kriterienkatalogs war das gesamte interdisziplinäre Projektteam beteiligt. So konnten alle Teammitglieder ein besseres Verständnis für die technischen Anforderungen bei der Programmierung von Apps, zum Beispiel hinsichtlich technisch notwendiger Zugriffsberechtigungen, entwickeln. Des Weiteren wurde die juristische Expertise des externen Beraters für die Operationalisierung der datenschutzrelevanten Aspekte und der zukünftigen Bedeutung der EU-Datenschutz-Grundverordnung hinzugezogen.

Die inhaltlichen Analysen der Verbraucherinformationen sowie der Datenschutzerklärung wurden anschließend von einem Projektteam durchgeführt, welches vorab durch die Projektleitung studienspezifisch geschult wurde. Nach der Schulung erfolgte eine mehrtägige Einarbeitungsphase, in der die gesamten Prüfkriterien bei verschiedenen Apps probeweise getestet wurden. Die Ergebnisse wurden im Anschluss mit der Projektleitung und dem Projektteam besprochen und mögliche Verständnisprobleme oder Besonderheiten beim Ablauf der Testung aufgeklärt.

Im Rahmen der inhaltlichen App-Prüfung wurden die folgenden Zeitpunkte der Informationsbereitstellung sowie unterschiedliche „Informationsorte" berücksichtigt:

Zeitpunkt 1: vor dem Download der App

- Ort der Information: im App Store
- Ort der Information: in der über den App Store verlinken Datenschutzerklärung

Zeitpunkt 2: beim ersten Öffnen der App

Zeitpunkt 3: nach dem Download zum Zeitpunkt der Nutzung

- Ort der Information: innerhalb der App
- Ort der Information: in der aus der App verlinkten Datenschutzerklärung.

Es wurde demnach nicht nur die Apps selbst für die Prüfungen herangezogen, sondern auch die im App Store hinterlegten Informationen. Hintergrund dieser Vorgehensweise ist der verbraucherfreundliche Ansatz sowie der datenschutzrechtliche Anspruch, die Nutzer bereits vor dem Download oder dem Kauf der App über alle relevanten Aspekte hinsichtlich der Nutzung der App zu informieren. Die geprüften Kriterien werden im Kapitel 4.5 vorgestellt.

Nach der Einarbeitungsphase fand die eigentliche Testung statt, die jeweils nach einem standardisierten Verfahren ablief:

1. Prüfung der festgelegten Kriterien im Google Play Store bzw. App Store

2. Installation und ggf. vorher Kauf der App
3. Anlegen eines Nutzerkontos, sofern erforderlich
4. Öffnen der App und Überprüfung der Zugriffsberechtigungen und/oder der Einwilligung in Datenschutzbestimmungen
5. Prüfung der Nutzeroberfläche im Hinblick auf Informationen zum Datenschutz sowie Support bzw. Kontaktmöglichkeiten zum App-Anbieter[4]
6. Inhaltsanalyse der Datenschutzerklärung aus der App (sofern vorhanden, ansonsten Prüfung der verlinkten Datenschutzerklärung im App Store)[5]

Falls die App nicht ausschließlich für Mobilfunkgeräte vorgesehen war, wurden für die Überprüfung der Kriterien im Google Play Store sowie der Datenschutzerklärung aufgrund der besseren Handhabbarkeit Android-Tablets verwendet. Anhand vielfacher Abgleiche kann ausgeschlossen werden, dass sich die dargestellten Informationen der Apps im Play Store zwischen Android-Tablets und Android-Smartphones unterscheiden. Optische Merkmale, wie beispielsweise die Schriftgröße, wurden nicht bewertet. Eine uneinheitliche Bewertung kann daher ausgeschlossen werden.

Nach der Überprüfung der inhaltlichen Kriterien fanden mehrere Qualitätssicherungsschritte statt, um fehlende Angaben zu ergänzen und unplausible Werte einer erneuten Prüfung zu unterziehen. Anschließend wurden die Ergebnisse automatisiert in das Bewertungsschema übertragen (siehe Kapitel 4.5).

[4] Die Bewertung der Nutzeroberfläche innerhalb der App konnte für „Samsung Smart View“, „TK-App“, „Weight Watchers Mobile“ und „WebIDent“ nicht vorgenommen werden, da hier spezifische Anforderungen zur Verifizierung der Mitgliedschaft erforderlich waren oder die Mitgliedschaft mit Kosten verbunden war.

[5] Die Apps „Apothekenfinder“, „Erste Hilfe DRK“ und „HiPP Baby App“ hatten weder im Google Play Store noch in der App eine Datenschutzerklärung, sodass diese nicht ausgewertet werden konnte. Dies gilt ebenso für die App „WeChat“, deren Datenschutzerklärung auf Chinesisch ist.

4.3 Vorbereitung und Durchführung der technischen Messung

Für die Durchführung der technischen Messung wurde zunächst die notwendige Hardware beschafft. Dabei wurde darauf geachtet, weit verbreitete Marken zu wählen, die auch sonst keine Auffälligkeiten aufweisen. Konkret wurden 6 iPhone 5s und 36 Android Smartphones vom Typ LG-K3 beschafft. Die LG-K3 verfügen über die gängige Android Version 6.0.1, die iPhones über das neueste iOS (10.3.3). Da manche Apps auf dem LG-K3 ihren Dienst versagten, wurden sie alternativ auf einem Samsung S5 getestet. Als Mobilfunkvertrag wurde mit Congstar-Prepaidkarten ebenfalls eine gängige Lösung gewählt.

Vorbereitung der Testumgebung

Die Verbindung der Telefone mit dem Internet erfolgte über einen dazwischen geschalteten Laptop, mit dem sich das Telefon über WLAN verband. Auf ihm wurden die Verbindungen mitgeschnitten. Die mobile Datenverbindung der Telefone (UMTS/LTE) war deaktiviert. Zunächst wurden alle Apps einmal installiert, um zu sehen, an welche Netzwerkports sie kommunizieren (Port-Mapping mittels Wireshark). Dabei wurde ebenfalls ermittelt, ob eine Man-in-the-Middle-Attacke möglich ist oder ob die App den Dienst verweigert. Im späteren Testbetrieb operiert SSLsplit entlang dieser Erkenntnisse. Wenn nötig und möglich, wurde eine Man-in-the-Middle-Attacke durchgeführt. In jedem Fall leitet SSLsplit den Netzwerkverkehr der identifizierten Ports in das Internet weiter und speichert sie parallel auf dem einsetzten Laptop.

Durchführung der Messungen

Jede App durchlief einen dreitägigen Messzyklus. Am ersten Tag war die App zwar installiert, jedoch nicht geöffnet. In dieser Phase sollte sie keine Daten senden. Am zweiten Tag wurde die App dreimal für 20 Minuten genutzt, um eine natürliche Nutzung zu simulieren. Am dritten Tag wurde sie wiederum nicht verwendet, weswegen im Allgemeinen auch keine Daten

hätten gesendet werden sollen. Die Messungen fanden im August und September 2017 statt.

Wie bereits erwähnt, wurde versucht, einen normalen Umgang mit dem Gerät zu simulieren. Dies war aus zwei Gründen wichtig: Zum einen sollte die App nicht bemerken, dass sie in einer Testumgebung läuft, zum anderen mussten Daten generiert werden, die ein Tracker auch mitschreiben kann. Hierzu wurden Google- und Apple-Accounts angelegt (weibliche Person, geb. 01.01.1990) und das Adressbuch des Smartphones gefüllt. Darüber hinaus wurden alle Telefone täglich außerhalb des Labors bewegt, um realistische Bewegungsdaten zu erzeugen. Für die Nutzung etlicher Apps war es notwendig, Benutzerkonten zu erstellen. In einigen Fällen wurden auch kostenpflichtige Mitgliedschaften angelegt (z. B. Maxdome und Weight Watchers) oder wir baten Kunden der entsprechenden Firmen, die App mit ihren Accounts nach Vorgaben zu testen (Banken und Bezahldienste).

Aufbereiten der Netzwerkdaten

Nach dem Mitschneiden galt es zunächst, die Datenströme zu separieren. Es wurde zwischen Datenströmen unterschieden, die von der jeweiligen App ausgehen und denjenigen, die auf das Gerät oder auf vorinstallierte Apps zurückgeführt werden konnten. Zunächst wurden alle Datenverbindungen identifiziert, die eindeutig auf Ad- oder Tracking-Services zurückgeführt werden konnten. Entsprechende Verzeichnisse (EasyList) solcher Dienste sind frei im Internet zugänglich, sodass die Datenverbindungen zu diesen Diensten eindeutig identifiziert werden konnten.

In einem ersten Schritt wurden anschließend diejenigen Datenverbindungen entfernt, die bekanntermaßen dem Gerät zuzuordnen sind. Hierzu zählen Verbindungen zu dem Apple- und LG-Updater sowie zu den Servern von Chipherstellern (Mediathek). Im Anschluss wurden Verbindungen entfernt, von denen absehbar war, dass sie keiner speziellen App zuzuordnen sind. Hierzu zählten sämtliche Google Services (Gmail, Calendar, Tracking, Analytics, Connections, nicht jedoch Youtube). Google ist ein derart allge-

genwärtiger Anbieter, dass es nicht möglich ist, festzustellen, ob die Kommunikation zu einem Server auf eine App zurückzuführen ist oder auf das Betriebssystem des Telefons.

Als nächstes wurden solche Netzwerkverbindungen entfernt, die so präsent sind, dass sie mit hoher Wahrscheinlichkeit auf das Betriebssystem oder dritte Apps zurückzuführen sind. Konkret wurden 70 Netzwerkverbindungen entfernt, die bei mindestens 50 Prozent der 200 Messungen auftraten. Dieser Parameter wurde nach händischem Verifizieren als ausreichend robust bewertet. Wird dieser höher angesetzt, schnellt die Anzahl der False Positives in die Höhe. Wird er niedriger angesetzt, wachsen die False Negatives überproportional. Nach diesen Filterschritten verblieben nur diejenigen Netzwerkverbindungen, die mit hoher Wahrscheinlichkeit auf die zu messende App zurückzuführen sind. Diese wurden anschließend strukturell und inhaltlich analysiert.

Die Analyse des Datenverkehrs erfolgte zunächst strukturell. Zu allen Netzwerkverbindungen wurden die Richtung des Datenverkehrs (in/out), das gesendete Datenvolumen und die IP-Adresse sowie der Port verzeichnet. Mittels des Whois-Services wurde der Server bzw. Hostname ermittelt. Tatsächlich erfolgte diese Analyse schon als Nebenprodukt der vorigen Schritte, um z. B. die Google Server zu identifizieren.

4.4 Inhaltliche Analyse der Datenströme

Um die Datenströme inhaltlich zu analysieren, mussten diese teilweise zunächst entschlüsselt werden. Wird Certificate Pinning genutzt, ist eine inhaltliche Analyse nicht möglich. Dies gilt ebenso beim Vorliegen eines Binärformates. Des Weiteren muss festgestellt werden, mit welchen Regeln Text in dem Nachrichtenstrom abgespeichert wurde (Encoding).

Nach diesen Schritten erfolgte die inhaltliche Analyse mittels regulärer Ausdrücke. Dabei wurde nach den folgenden Punkten gesucht:

- Mail-Adressen (entsprechend den Gmail-Accounts der Telefone),

- Telefonnummern der Congstar-Prepaidkarten,
- IMEI (Seriennummer der Telefone),
- MAC Adressen, der in den Telefonen verbauten Netzwerkadaptern,
- UUIDs (oft von Ad-Trackern generierte Identifier) sowie
- geographische Positionen in Bonn (50,74 Grad Nord und 7,09 Grad Ost) und den entsprechenden UTM-Koordinaten.

Es wurde nach allen erdenklichen Schreibweisen gesucht. Zudem wurde die Verwendung von Kommata, Trennstrichen sowie Leerzeichen an beliebigen Stellen in der Suche berücksichtig. Jeder Fund wurde im Nachgang händisch verifiziert.

4.4.1 Technische Grenzen der Messung

Die das Smartphone verlassenden Datenströme müssen nicht zwangsweise von der zu untersuchenden App stammen, sondern könnten auch auf das Betriebssystem oder vorinstallierte Apps zurückzuführen sein. Die gewählte Heuristik und ihre Parameter waren jedoch sehr konservativ. Es kann daher sein, dass Datenströme fälschlicherweise nicht der App zugeordnet wurden, obwohl dies korrekt gewesen wäre. Im Umkehrschluss sind die identifizierten Datenströme mit sehr hoher Wahrscheinlichkeit auf die untersuchte App zurückzuführen. Weiterhin kann es sein, dass aufgrund der Verwendung von Binärformaten und der Verschlüsselung von Netzwerkprotokollen, Spähverhalten in Datenströmen nicht erkannt wurde. Insbesondere die Kommunikation zu zwei zentralen Anbietern – Google und Facebook – konnte nur selten mitgelesen werden.

Wie die Studie zeigt, nutzen Firmen mittlerweile massiv Cloud-Dienste wie Amazon-Web-Services oder ähnliche Plattformen von Google, IBM oder Microsoft. Dies führt dazu, dass die Analyse des Netzwerkverkehrs zu dem Ergebnis kommt, dass zum Beispiel Amazon über den Amazon-Server in Frankfurt kontaktiert wurde, obwohl der Service tatsächlich von einer anderen Firma mit Sitz in den USA betrieben wird. Sogenannte „Content-Delivery-Networks“, wie beispielsweise Akamai, führen zu ähnlichen

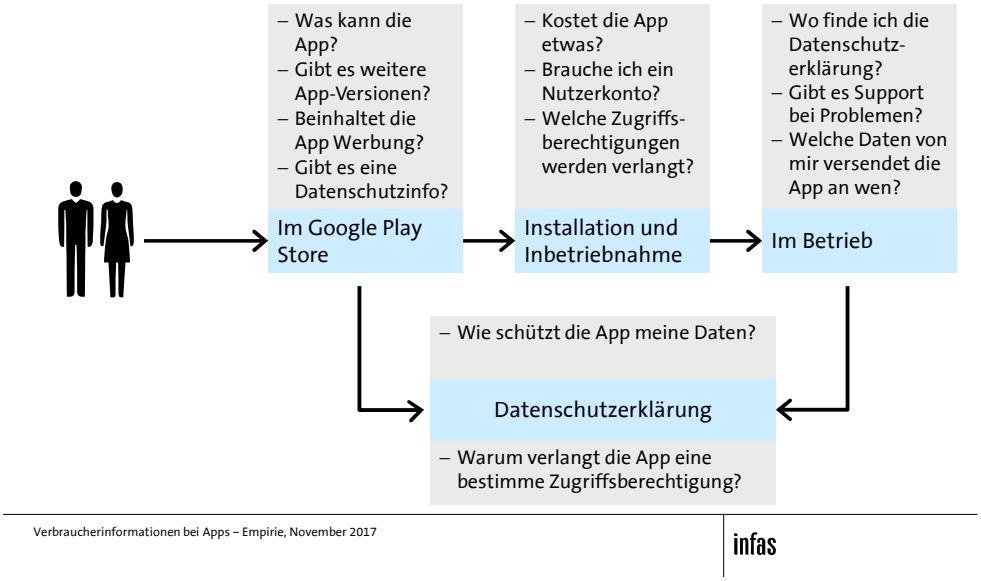
Effekten. Es ist im Allgemeinen nicht die Absicht der Cloud-Anbieter, Namen und Herkunft der Dienstanbieter zu verheimlichen. Im Kontext dieser Studie bleibt dies jedoch ein signifikanter Nebeneffekt. Der Umfang, mit dem Cloud-Plattformen eingesetzt werden, und die starke Zentralisierung auf nur einige wenige Anbieter waren durchaus überraschend.

Die Kommunikation von Telefonen mit der Firma Google ist nicht einzelnen Apps zuzuordnen. Google ist nicht nur Hersteller des Betriebssystems Android, sondern sammelt gleichzeitig selber in hohem Umfang Daten, ist im Werbemarkt aktiv, betreibt Cloud-Services und bietet Entwicklern eine ganze Reihe Toolkits an, die wiederum alle mit Google-Servern kommunizieren. Diese Datenströme konnten deshalb nicht einzelnen Apps zugeordnet werden. Insgesamt verfolgt die Studie eine konservative Strategie. Im Zweifelsfall wurde „zu Gunsten“ der App entschieden. Daher kann es zu gehäuften False Negatives kommen (Tracking, das nicht erkannt wurde), während False Positives selten sein sollten (gutartiges Verhalten, das als Tracking eingestuft wurde). Letztendlich im Testverfahren als auffällig identifiziertes Verhalten ist jedoch mit größter Wahrscheinlichkeit der getesteten App zuzuordnen und wurde folglich korrekt als Tracking eingeordnet.

4.5 Erstellung eines umfassenden Bewertungsschemas

Die Ergebnisse der inhaltlichen Analyse sowie der technischen App-Messungen wurden im Anschluss an die Erhebungsphase in ein detailliertes Bewertungsschema überführt. Da die inhaltliche Zielsetzung des Projektes die Überprüfung der Verbraucherinformationen bei Apps ist, wurde das Bewertungsschema dem Blickwinkel der Verbraucher folgend konzipiert. Dabei wurden die Schritte vom App Store über den Installationsprozess bis hin zur Orientierung innerhalb der App abgebildet und jede App anhand dieser Schritte bewertet. Die Datenschutzerklärung wurde als gesonderte Dimension beurteilt, da sie eine wichtige Grundlage für transparente und vollumfängliche Verbraucherinformationen bildet.

Abbildung 6 Weg des Verbrauchers vom App-Kauf zur Nutzung



Die untersuchten Apps erhielten für jede der vier dargestellten Dimensionen „Im Google Play Store“, „Datenschutzerklärung“, „Installation und Inbetriebnahme“ sowie „Im Betrieb“ eine Bewertung. Aus diesen Einzelbewertungen ergab sich für jede App eine Gesamtnote. In den folgenden Unterkapiteln wird erläutert, welche Überlegungen und Kriterien bei der Beurteilung der einzelnen Dimensionen relevant waren und somit in die Benotung der App eingeflossen sind. Im Anhang findet sich eine Übersicht, in der die Operationalisierung für jedes einzelne Kriterium zu finden ist (siehe Tabelle 11). Die detaillierte Auflistung aller getesteten Kriterien für jede einzelne App befindet sich aufgrund des Umfangs auf der beigefügten CD-ROM.

4.5.1 Die Dimension „Im Google Play Store“

Der erste Schritt eines Verbrauchers vor dem Download und der Nutzung einer App führt zum jeweiligen App Store. Da 200 Apps für Android-Betriebssysteme getestet wurden, war der Ausgangspunkt für die Bewertung jeder App ihre Präsentation im Google Play Store. Die grundlegenden Unterschiede zwischen dem Google Play Store und dem App Store von Apple werden in Kapitel 5.5 erläutert. Ausgangspunkt für die Beurteilung

der Dimension „Im Google Play Store“ waren die folgenden Fragestellungen:

- Werden die Funktion und der Zweck der App verständlich übermittelt?
- Werden dem Nutzer alle relevanten Informationen für die Installation an die Hand gegeben?

Die beiden sich daraus ergebenden Bewertungskategorien wurden in weitere Kriterien untergliedert (siehe Tabelle 1).

Tabelle 1 Bewertungskriterien „Im Google Play Store“

Im Google Play Store	
Erläuterung der Funktion und des Zwecks der App	**Angabe von relevanten Informationen vor der Installation/dem Kauf**
Beschreibung der App	Demoversionen oder werbefreie Versionen
Beschreibung in deutscher Sprache	Datenschutzerklärung zur App
Informationen zum Online-/Offline-Modus	Kontaktinformationen
Vorwissen über die App wird vorausgesetzt	

Die Kriterien bilden die Grundlage für die Benotung der App in der Dimension „Im Google Play Store“. Die Bewertung auf der Ebene von Einzelkriterien war wichtig, um zu einem möglichst objektiven und replizierbaren Ergebnis zu kommen. In Kapitel 4.5.4 wird genauer erläutert, wie die Operationalisierung und Codierung der einzelnen Kriterien zu einer quantitativ abgeleiteten Benotung führt.

Ausschlaggebend für eine verständliche Verbraucherinformation ist die jeweilige Beschreibung der App im Google Play Store, die vom App-Anbieter selbst gestaltet wird. Aus der Darstellung im Google Play Store sollte ersichtlich werden, welches Unternehmen oder welcher Entwickler die App anbietet. Zudem sollte ein Nutzer nach dem Lesen der Beschreibung wissen, welchen Zweck die App erfüllt und welche Funktionalitäten sie beinhaltet. Dazu gehört auch die Information, ob die App immer oder nur zu bestimmten Zwecken mit dem Internet verbunden sein muss. Dies ist aus datenschutzrechtlicher Sicht ein wichtiger Verbraucherhinweis, da eine Internetverbindung Voraussetzung für die Übermittlung von Nutzerdaten

zum jeweiligen App-Anbieter ist. Für eine verständliche Beschreibung ist außerdem wichtig, dass der App-Anbieter kein Vorwissen über den angebotenen Dienst voraussetzt. Des Weiteren sind App-Beschreibungen auf Englisch oder einer anderen Fremdsprache für den deutschen App-Markt problematisch, da dies verhindert, dass auch Nutzer ohne Fremdsprachenkenntnisse die Möglichkeit haben, sich über die App zu informieren. Um eine informierte Entscheidung vor der Installation oder dem Kauf treffen zu können, wäre auch eine Information über weitere App-Versionen des Anbieters (kostenfreie oder werbefreie Demoversionen) ratsam. Schließlich gehört zu einer vollständigen Verbraucherinformation auch die Möglichkeit, sich über die Datenschutzbestimmungen des App-Anbieters informieren zu können. Alle genannten Einzelkriterien flossen in die Benotung der Dimension „Im Google Play Store“ ein.

4.5.2 Die Dimension „Datenschutzerklärung“

Die Datenschutzerklärung bildet eine wichtige Grundlage für umfängliche Verbraucherinformationen. Daher ist es sinnvoll, wenn Nutzer sich bereits vor der Installation einer App über die Datenschutzbestimmungen des App-Anbieters im Google Play Store informieren können. Aber auch innerhalb der App ist eine Datenschutzerklärung zweckmäßig, um die Verbraucher über den Umgang des App-Anbieters mit den Nutzerdaten aufzuklären. Bei einigen Anbietern unterscheidet sich die im Google Play Store verlinkte Datenschutzerklärung von der Datenschutzerklärung innerhalb der App. Dabei besteht der Unterschied in der Regel darin, dass die Datenschutzerklärung innerhalb der App einen direkten Bezug zu dieser aufweist, während die Datenschutzerklärung im Play Store zumeist auf die Website des Anbieters verlinkt und dort alle Dienste des Anbieters – teilweise ohne konkrete Nennung der App – umfasst. Aufgrund des hohen Umfangs an geprüften Apps sowie der zeitlichen Restriktion des Projektes, wurde in solchen Fällen nur die in der App verfügbare Datenschutzerklärung analysiert. Bei der Bewertung der Datenschutzerklärung standen die folgenden Überlegungen im Vordergrund:

- Sind die vorhandenen Informationen zum Datenschutz vollständig oder fehlen relevante Hinweise?
- Wie datenschutzfreundlich agiert der App-Anbieter?
- Ist die Datenschutzerklärung verständlich aufbereitet?

Aus diesen Fragestellungen wurden die drei Kategorien „Vollständigkeit", „Datenschutzfreundlichkeit" und „Darstellung" abgeleitet, die wiederum jeweils in verschiedene Bewertungskriterien unterteilt wurden (siehe Tabelle 2).

Tabelle 2 Bewertungskriterien „Datenschutzerklärung"

Datenschutzerklärung		
Vollständigkeit	**Datenschutzfreundlichkeit**	**Darstellung**
Art und Zweck der Nutzung von personenbezogenen Daten	Genauigkeit der Angaben zu Dritten	Trennung von AGB und Datenschutzerklärung
Weitergabe an Dritte	Opt-In oder Opt-Out	Datenschutzerklärung auf Deutsch
Löschung und Speicherung der Daten	Einbindung von Ad-Networks	Inhaltsverzeichnis
Zugriffsberechtigungen	Begrenzung der Speicherdauer	Kapitelüberschriften
Aktualisierung der Datenschutzerklärung	Löschung der Daten nach App-Löschung	Anzahl der Wörter
Anwendung des deutschen oder europäischen Datenschutzrechts	Aktiver Hinweis bei Aktualisierung der Datenschutzerklärung	Lesbarkeit der Datenschutzerklärung
	Informationen über Portabilität von Daten	Verständlichkeit und Eindeutigkeit der Datenschutzerklärung

Die Bewertung der Kategorie „Vollständigkeit" fällt dabei umso positiver aus, je mehr relevante Informationen der App-Anbieter in der Datenschutzerklärung aufführt. Dazu gehören unter anderem Angaben über Art und Zweck der Nutzung personenbezogener Daten, die Weitergabe von Daten an Drittparteien, Angaben zur Löschung und Speicherung von Nutzerdaten und die Beschreibung der in der App erforderlichen Zugriffsberechtigungen.

In die Beurteilung der Kategorie „Datenschutzfreundlichkeit" wurden verschiedene Kriterien einbezogen, die einerseits die Präzision und Transparenz der Aussagen in der Datenschutzerklärung und andererseits die datenschutzrechtlichen Praktiken des App-Anbieters sowie deren Folgen betreffen. Hierzu gehören konkrete Informationen des App-Anbieters zu Drittparteien sowie die Opt-In- und Opt-Out-Möglichkeiten in Bezug auf die

Weitergabe der Nutzerdaten. Auch Angaben zur Begrenzung der Speicherdauer oder zur Löschung der personenbezogenen Daten wurden in dieser Kategorie bewertet. Je sparsamer und datenschutzfreundlicher ein App-Anbieter mit den personenbezogenen Daten der Nutzer umgeht, desto besser fällt die Beurteilung in der Kategorie „Datenschutzfreundlichkeit“ aus.

In der Kategorie „Darstellung“ wurde die Verständlichkeit und Aufbereitung der Datenschutzinformationen beurteilt, da dies einen wesentlichen Anteil zur Transparenz beiträgt. Hier kommt es zum Beispiel darauf an, dass die Lesbarkeit der Datenschutzerklärung adressatengerecht ist und die Datenschutzhinweise nicht in den AGBs des Anbieters „versteckt“ werden.

4.5.3 Die Dimension „Installation und Inbetriebnahme“

Nachdem sich Verbraucher für die Nutzung einer App entschieden haben, erfolgen die Installation und die erste Inbetriebnahme. Auch hier gibt es unterschiedliche Faktoren, die zur Datenschutzfreundlichkeit einer App beitragen und sich im Wesentlichen in den folgenden drei Fragen widerspiegeln:

- Welche Zugriffsberechtigungen benötigt die App und sind diese für die Nutzung wirklich erforderlich?
- Wie wird die Einwilligung in die Nutzung der personenbezogenen Daten gehandhabt?
- Muss für die Nutzung der App ein Nutzerkonto eingerichtet werden?

Diese Kategorien wurden wiederum in Einzelkriterien untergliedert (siehe Tabelle 3).

Tabelle 3 Bewertungskriterien „Installation und Inbetriebnahme“

Installation und Inbetriebnahme		
Zugriffsberechtigungen	**Einwilligung in Nutzung der personenbezogenen Daten**	**Nutzerkonto**
Überflüssige Zugriffsberechtigungen vorhanden	Einwilligung in Datenschutzerklärung oder AGB beim Öffnen der App	Notwendigkeit eines Nutzerkontos
Start der App ohne Erlaubnis der überflüssigen Zugriffsberechtigungen	Erfordernis einer Lesebestätigung	Anzahl der Pflichtangaben bei Anmeldung
		Notwendigkeit eines Drittanbieter-Nutzerkontos
		Information zur Löschung des Nutzerkontos

Aus Gründen der Datensparsamkeit sollte ein App-Anbieter nur solche Berechtigungen einholen, die für die Funktionalität der App benötigt werden. Auch wenn die Beurteilung nicht ganz einfach ist (siehe dazu Kapitel 5.3), wurde in der Kategorie „Zugriffsberechtigungen“ negativ bewertet, wenn der App-Anbieter Zugriffsberechtigungen im Google Play Store angibt oder beim Öffnen der App einholt, die sich nicht aus der Funktionalität der App erklären. Negativ wurde ebenfalls beurteilt, wenn das Starten der App ohne das Zulassen solcher nicht notwendigen Berechtigungen nicht möglich ist und Nutzer somit zur Zustimmung der Berechtigung gedrängt werden.

Bei der Verarbeitung personenbezogener Daten ist die Einwilligung der betroffenen Personen in der Regel verpflichtend. Da die Definition von personenbezogenen Daten im Rahmen der App-Nutzung problematisch ist (siehe Kapitel 5.2), wäre es sinnvoll, wenn jeder App-Anbieter – unabhängig davon, welche Art von Daten dieser verarbeitet – beim ersten Öffnen der App auf seine Datenschutzbestimmungen hinweist oder sogar eine aktive Zustimmung beim Nutzer einholt. Da anzunehmen ist, dass nur wenige Verbraucher die Datenschutzerklärungen der App-Anbieter lesen, wird ein solches Vorgehen im Hinblick auf die höhere Informiertheit der Nutzer im Rahmen der Bewertung begrüßt.

Etwa ein Drittel der getesteten Apps kann nur mit einem Nutzerkonto verwendet werden. Das Einrichten eines Nutzerkontos geht in der Regel mit der Eingabe personenbezogener Daten, wie zum Beispiel einem Namen und einer E-Mail, einher. Für eine transparente Verbraucherinformation sollten Nutzer vom App-Anbieter möglichst vor der Installation darüber informiert werden, ob das Einrichten eines Nutzerkontos für die App-Nutzung erforderlich ist. Ebenso wichtig ist eine Information darüber, wie das Nutzerkonto und die damit verbundenen personenbezogenen Daten gelöscht werden können, wenn der Dienst nicht mehr benötigt wird. Im Rahmen des Projektes wurde in der Kategorie „Nutzerkonto“ negativ bewertet, wenn das Anlegen eines Benutzerkontos mit dem Kundenstatus bei einem Drittanbieter (z. B. Google, Facebook oder Amazon) verbunden ist. Nutzer, die nicht bereits Kunde bei dem jeweiligen Drittanbieter sind, müssen ihre Daten somit gezwungenermaßen bei einem zusätzlichen Unternehmen hinterlegen, um den Dienst nutzen zu können.

4.5.4 Die Dimension „Im Betrieb“

Die Dimension „Im Betrieb“ setzt sich aus den beiden Kategorien „Datensendeverhalten“ und „Serviceorientierung in der App“ zusammen. In diesem Zusammenhang waren folgende Fragestellungen zentral:

- An welche Dritte sendet die App Daten und ist der Datenversand in der Datenschutzerklärung begründet? Stehen die versendeten Daten in Zusammenhang mit der Funktionalität der App?
- Sind alle wichtigen Verbraucherinformationen innerhalb der App zu finden?

Die sich daraus ergebenden Kategorien und Kriterien werden in der folgenden Tabelle dargestellt.

Tabelle 4 Bewertungskriterien „Im Betrieb“

Im Betrieb	
Datensendeverhalten	**Serviceorientierung in der App**
Datenversand an Dritte (Abgleich mit der Datenschutzerklärung)	Werbeinhalte
Datenversand an Ad-Services (Abgleich mit der Datenschutzerklärung)	Datenschutzerklärung in App verfügbar
Datenversand ins Nicht-EU-Ausland (Abgleich mit der Datenschutzerklärung)	Impressum in App verfügbar
Kommunikation der App im Ruhezustand ohne Nutzen für die App-Funktion	Kontaktmöglichkeiten zum Anbieter
Versendung von Adressbuch ohne Nutzen für die App-Funktion	Support/Beschwerdemanagement
Versendung von Standortdaten ohne Nutzen für die App-Funktion	
Versendung von Identifiern ohne Nutzen für die App-Funktion	

Bei der Kategorie „Datensendeverhalten“ wurden sowohl das Sendeverhalten der App als solches bewertet, als auch ein Abgleich des tatsächlichen Sendeverhaltens mit den Aussagen innerhalb der Datenschutzerklärung vorgenommen. Hierbei wurden drei Faktoren berücksichtigt: Versendung von Daten (1) an Dritte, (2) an Ad-Services und (3) ins Nicht-EU-Ausland. Alle drei Kriterien wurden negativ bewertet, wenn diesbezüglich keine Angaben in der Datenschutzerklärung gemacht wurden. Daneben gibt es aber auch Faktoren, die – unabhängig von der Datenschutzerklärung – aus Verbrauchersicht als bedenkliches Sendeverhalten identifiziert werden können. Dies betrifft beispielsweise die Versendung von Adressbucheinträgen, Standortdaten und Identifiern ohne ersichtlichen Nutzen für die App-Funktionen.

Die Kategorie „Serviceorientierung in der App“ wurde mit der Überlegung angelegt, was aus Nutzersicht während der App-Nutzung als störend oder als wünschenswert empfunden wird. In den vorgenommenen Bewertungen stehen jedoch keine Merkmale der App-Usability im Vordergrund, sondern die Verfügbarkeit und Darstellung von Verbraucherinformationen sowie der Umgang des App-Anbieters mit den Daten der Nutzer. Daher wurde grundsätzlich positiv beurteilt, wenn die App keine Werbung beinhaltet

sowie wenn sie über eine Datenschutzerklärung, Kontaktinformationen, ein Impressum und Supportmöglichkeiten verfügt.

4.5.5 Codierung und Gewichtung der Bewertungskriterien

Um eine objektive und replizierbare Bewertung durch verschiedene Prüfer vornehmen zu können, wurden zu jeder Dimension Einzelkriterien abgeleitet, die möglichst eindeutig entweder positiv oder negativ bewertet werden konnten. Daher wurden bis auf wenige Ausnahmen alle Kriterien im Rahmen der inhaltlichen Bewertung zunächst mit den Codes „ja“, „nein“, „keine Angabe“ oder „trifft nicht zu“ erfasst. Diese wurden anschließend – je nachdem, welche Angabe als positiv oder negativ bewertet wurde – in die binären Codes 1 und 0 überführt.[6] Kriterien, für die ein anderer Bewertungsmaßstab angewendet werden musste, wie zum Beispiel bei der Anzahl der Wörter der Datenschutzerklärungen, wurde die Operationalisierung im Projektteam diskutiert und eine entsprechende Bewertungsregel aufgestellt. Im Anhang sind alle Kriterien und die jeweilige Operationalisierung dokumentiert (siehe Tabelle 11).

Jede App konnte in jeder Kategorie eine bestimmte Maximalanzahl an Punkten erreichen. Dabei flossen die jeweiligen Einzelkriterien mit einer unterschiedlichen Gewichtung in die Kategorien ein. Kriterien, die als besonders relevant eingestuft wurden, erhielten eine höhere Gewichtung (Gewichtungsfaktor: 2). Kriterien, die als weniger relevant eingestuft wurden oder die sich bei der Testung als uneindeutig beziehungsweise schwer zu bewerten herausstellten, wurden heruntergewichtet (Gewichtungsfaktor: 0,5). Dieses Vorgehen wird beispielhaft in Tabelle 5 veranschaulicht.

[6] Während beispielsweise das Vorhandensein einer Datenschutzerklärung in deutscher Sprache (codiert „ja“) einen Punkt erhielt, wurde bei der Einbindung von Ad-Networks (codiert „ja“) kein Punkt vergeben, sondern die Antwort „nein“ erhielt in diesem Fall die positive Bewertung.

Tabelle 5 Beispielbewertung der Kategorie „Vollständigkeit der Datenschutzerklärung“

Kategorie „Vollständigkeit der Datenschutzerklärung“ Informationen über	Bewertung	Codierung	Gewichtungs-faktor	tatsächlich erreichte Punktzahl
Art und Zweck der Nutzung von personenbezogenen Daten	ja	ja = 1 nein = 0	2	2
Weitergabe an Dritte	ja	ja = 1 nein = 0	2	2
Löschung und Speicherung der Daten	nein	ja = 1 nein = 0	2	0
Zugriffsberechtigungen	ja	ja = 1 nein = 0	2	2
Aktualisierung der Datenschutz-erklärung	ja	ja = 1 nein = 0	0,5	0,5
Anwendung des deutschen oder europäischen Datenschutzrechts	nein	ja = 1 nein = 0	1	0
Erreichte Punktzahl	**6,5 von 9,5 Punkten = 68 %**			

Da alle Kategorien eine unterschiedliche maximale Punktzahl aufwiesen, wurden die erreichten Punkte in einen Prozentwert umgewandelt. Die Maximalanzahl der Punkte innerhalb der Kategorie entspricht einem Prozentwert von 100. Für die Gesamtbewertung einer Dimension wurde anschließend der Mittelwert über alle Kategorien gebildet. In Tabelle 6 wird dieses Vorgehen beispielhaft anhand der Dimension „Datenschutzerklärung“ dargestellt.

Tabelle 6 Beispielbewertung der Dimension „Datenschutzerklärung“

Dimension „Datenschutzerklärung“	erreichte Prozent-zahl in der Kate-gorie
Vollständigkeit	68 %
Datenschutzfreundlichkeit	55 %
Darstellung	80 %
Gesamtbewertung der Dimension (Ø)	**68 %**

4.5.6 Benotung der Dimensionen und Gesamtnote der App

Die Benotung der Dimensionen und der gesamten App folgte aus der Übertragung der erreichten Prozentwerte in eine Notenskala von „sehr gut“ bis „mangelhaft“.

Tabelle 7 Notenschlüssel

Prozentwert	Note	Legende
100 bis 95 Prozent	sehr gut	
94 bis 80 Prozent	gut	
79 bis 65 Prozent	befriedigend	
64 bis 50 Prozent	ausreichend	
unter 50 Prozent	mangelhaft	

Jeder App erhielt für jede Dimension eine Note. Aus den vier Einzelnoten wurde anschließend die Gesamtnote der App errechnet. Aufgrund der aus den Projektzielen abgeleiteten Relevanz der unterschiedlichen Dimensionen sowie der Anzahl an bewerteten Einzelkriterien, floss die Bewertung der beiden Dimensionen „Datenschutzerklärung“ sowie „Im Betrieb“ stärker in die Gesamtnote ein (jeweils 35 %) als die Dimensionen „Im Google Play Store“ und „Installation und Inbetriebnahme“ (15 %). In Tabelle 8 wird dies beispielhaft gezeigt.

Tabelle 8 Anteil der Dimensionen an Gesamtnote am Beispiel der App „Focus Online“

Dimension	Prozentanteil der Dimension an der Gesamtnote der App	erreichter Prozentwert der Dimension	Note
Im Google Play Store	15 %	86 %	
Datenschutzerklärung	35 %	68 %	
Installation und Inbetriebnahme	15 %	50 %	
Im Betrieb	35 %	87 %	
Gesamtnote	**100 %**	**74 %**	

5 Darstellung der Ergebnisse

Im Folgenden werden die Ergebnisse der App-Testungen innerhalb der einzelnen Dimensionen sowie auf Gesamtebene dargestellt, relevante Erkenntnisse hervorgehoben und erste Empfehlungen für eine bessere Verbraucherinformation abgeleitet.[7] Wie bereits eingangs erwähnt, zielen die Bewertungen der Apps auf einen Gesamtüberblick zu den Verbraucherinformationen der App-Anbieter sowie deren Umgang mit dem Thema Datenschutz ab. Die Usability und die internen Funktionalitäten der einzelnen Apps werden im Rahmen dieser Studie nicht bewertet.

5.1 Ergebnisse der Dimension „Im Google Play Store“

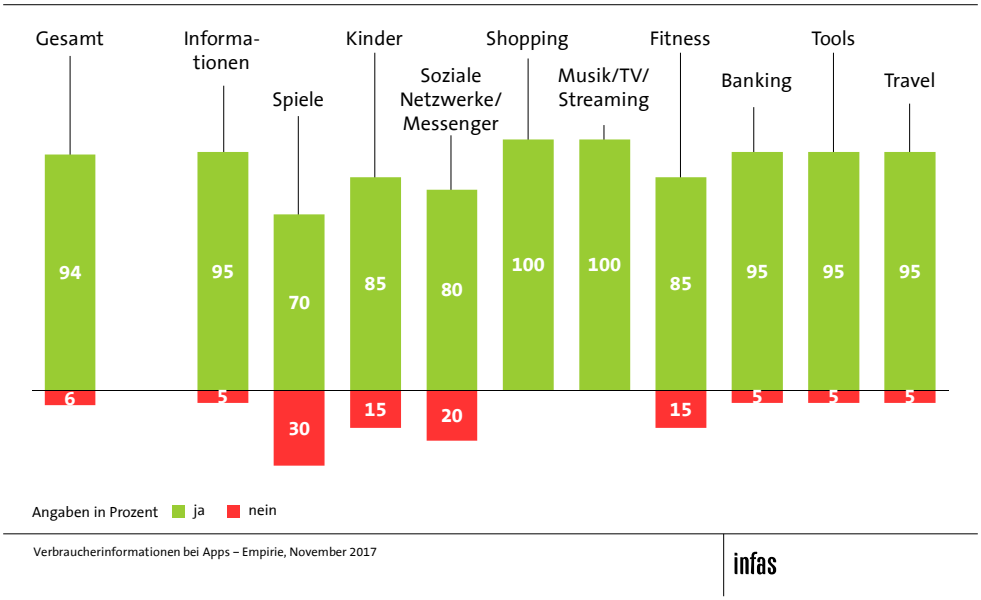
Die Präsentation einer App im App Store ist das wichtigste Aushängeschild eines App-Anbieters. Sofern ein Nutzer sich nicht schon vorab zur Installation beziehungsweise zum Kauf einer App entschieden hat, sollen die Informationen im jeweiligen App Store Orientierung bieten und eine informierte (Kauf-)Entscheidung ermöglichen. Demnach sollten im App Store alle relevanten Informationen zur App vorhanden sein. Dazu gehört beispielsweise eine verständliche Beschreibung über den Zweck und die Funktionalität der App.

Google und Apple stellen an App-Entwickler, die ihre Dienste in ihrem Store anbieten wollen, verschiedene Anforderungen. Dies führt zu einem unterschiedlichen Maß an Transparenz.[8] Im Folgenden werden ausschließlich solche Informationen der App-Anbieter bewertet, die von diesen selbst gestaltet werden können. Dazu gehört in erster Linie die Beschreibung der jeweiligen App. Die Unterschiede zwischen den App-Anbietern hinsichtlich des Umfangs und der Qualität der Texte sind groß. Sie reichen von

[7] Eine Gesamtübersicht der Ergebnisse für jede einzelne App (Steckbrief) findet sich im Anhang (Tabelle 10). Die detaillierten Bewertungen aller Kriterien für jede einzelne App befinden sich aufgrund des Umfangs auf der beigefügten CD-ROM.
[8] Im Kapitel 5.5 wird auf die diesbezüglichen Unterschiede zwischen dem Google Play Store und dem App Store von Apple genauer eingegangen.

kreativen Beschreibungen im Stil eines Werbetextes bis hin zu sehr detaillierten und sachlichen Texten. Im Rahmen des Projektes wurde bewertet, ob die Funktionalität der App und die Voraussetzungen zur App-Nutzung vom App-Anbieter verständlich dargestellt werden.

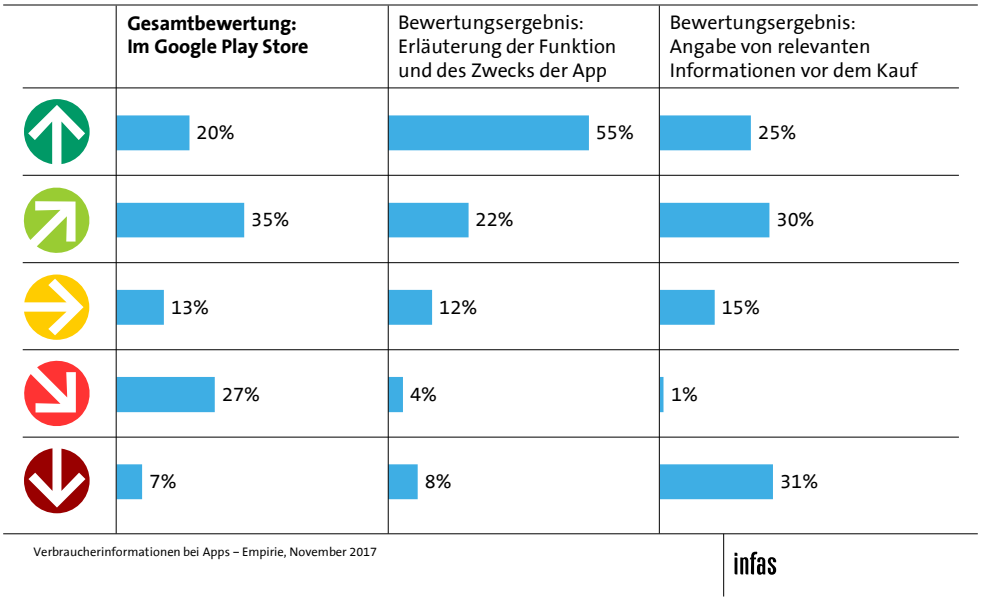
Abbildung 7 Verständliche Beschreibung der App im Google Play Store



Wie Abbildung 7 zeigt, stellt nach den Ergebnissen unserer Bewertung die überwiegende Mehrheit der App-Anbieter im Google Play Store eine verständliche Information über Zweck und Funktionalität der App zur Verfügung. Etwas schlechter schneiden hier nur die Apps aus den Bereichen „Spiele“´, „Soziale Netzwerke/Messenger“, „Kinder“ und „Fitness“ ab. Beschreibungen auf Englisch (z. B. „Twitter“, „Super Cleaner“) wurden generell schlecht bewertet, da diese für den deutschen App-Markt nicht adressatengerecht aufbereitet wurden. Als besonders positive Beispiele sind solche App-Beschreibungen hervorzuheben, die sich durch relevante Zusatzinformationen vom Standard abheben. Dies ist beispielsweise durch eine Angabe der benötigten Zugriffsberechtigungen und ihrer Zwecke (z. B. „Bild News“, „Amazon Shopping“), durch Informationen zum Datenschutz (z. B. „Lidl – Prospekte & Angebote“) oder durch den Hinweis auf Supportmöglichkeiten (z. B. „Goodgames Empire“) der Fall.

Die in vielen Fällen positive Bewertung der App-Beschreibung trägt maßgeblich zu dem insgesamt positiven Fazit bei der Kategorie „Erläuterungen der Funktionen der App“ bei (siehe Abbildung 8). Über die Hälfte der Apps erhält hier die Note „sehr gut“. Der Durchschnitt über alle getesteten Apps liegt bei „gut“.

Abbildung 8 Bewertung der Dimension „Im Google Play Store“



Etwas ungünstiger fällt die Bewertung für die Kategorie „Relevante Informationen vor dem Kauf“ aus. Insbesondere der fehlende Link zu einer Datenschutzerklärung führt hier zu einer äußerst schlechten Beurteilung (z. B. „Promiflash“). Obwohl inzwischen alle App-Anbieter den Link zu einer Datenschutzerklärung angeben müssen, um ihre App im Google Play Store überhaupt anbieten zu dürfen, haben einige „ältere“ Apps diese Vorgabe noch nicht rückwirkend umgesetzt. Englische Datenschutzerklärungen werden für den deutschen Markt wiederum als nicht adäquat eingestuft. Positiv werden in dieser Kategorie ausführliche Kontaktinformationen und Hinweise auf kosten- oder werbefreie Demoversionen des App-Anbieters bewertet. Rund ein Viertel der Apps erfüllt diese Anforderungen rundum, immerhin ein Drittel erreicht noch eine gute Note. Allerdings fällt knapp ein Drittel der Apps in dieser Kategorie durch.

Insgesamt zeigt sich in der „Dimension „Im Google Play Store“ ein recht gemischtes Bild. Während gut die Hälfte aller Apps mit „sehr gut“ und „gut“ bewertet werden, erhält ein gutes Drittel der Apps schlechte Bewertungen.

Was uns auffällt:

- Die Präsentation der Apps im Google Play Store ist das Aushängeschild für die jeweiligen App-Anbieter. Dementsprechend gibt sich ein Großteil der App-Anbieter Mühe bei der Darstellung und Informationsaufbereitung – insgesamt kann ein positives Fazit bei der Kategorie „Erläuterung von Zweck und Funktionen“ der Apps gezogen werden.
- Vor allem das Fehlen von verlinkten Datenschutzerklärungen oder fehlende Kontaktinformationen des App-Anbieters trüben das Gesamtbild.

Was wir raten:

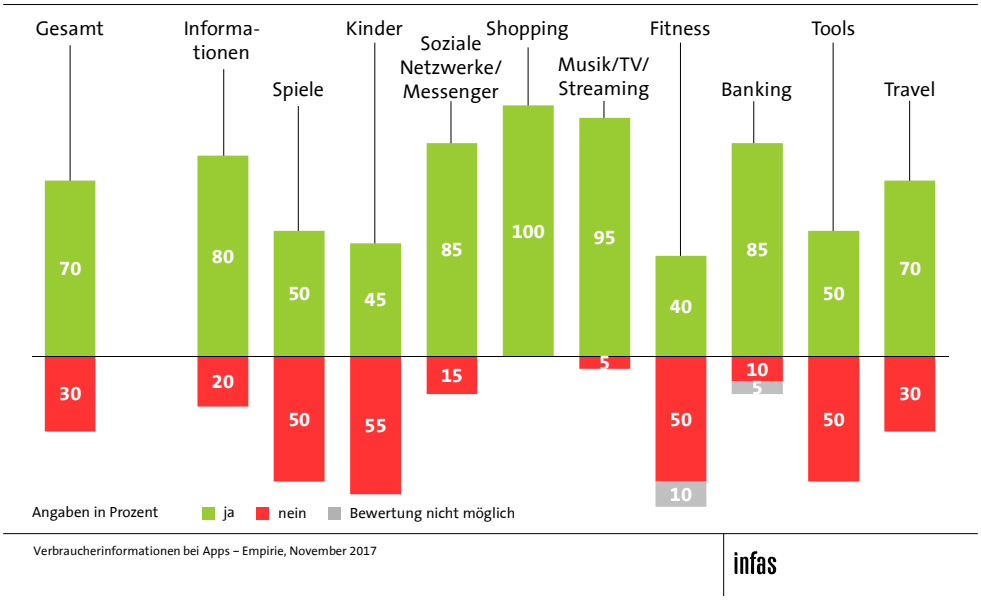
- ALLE Anbieter sollten eine Datenschutzerklärung im Google Play Store hinterlegen.
- Insbesondere große Unternehmen machen es sich oft zu einfach, indem sie die Datenschutzerklärung ihres Gesamtunternehmens im Google Play Store verlinken. Teilweise wird in dieser nur auf „alle Dienste“ des Unternehmens verwiesen, die Informationen zur App-Nutzung sind versteckt oder nicht vorhanden. Dies verhindert, dass sich Nutzer vor dem Download über den Datenschutz bei der App-Nutzung hinreichend informieren können.
- Es wäre zu empfehlen, dass App-Anbieter eine Datenschutzerklärung hinterlegen, die sich ausschließlich oder zumindest eindeutig auf ihre App(s) bezieht.

5.2 Ergebnisse der Dimension „Datenschutzerklärung“

Damit Verbraucher die Möglichkeit haben, sich schon vor der Installation einer App über alle datenschutzrechtlichen Aspekte zu informieren, erscheint es sinnvoll, wichtige Datenschutzhinweise direkt im App Store zu platzieren und die Datenschutzerklärung des App-Anbieters dort zu verlinken. Doch auch die Bereitstellung einer Datenschutzerklärung innerhalb der App ist wünschenswert, damit die Nutzer jederzeit darauf zugreifen können. Hiervon ausgenommen sind wenige Apps, die aufgrund ihrer Funktio-

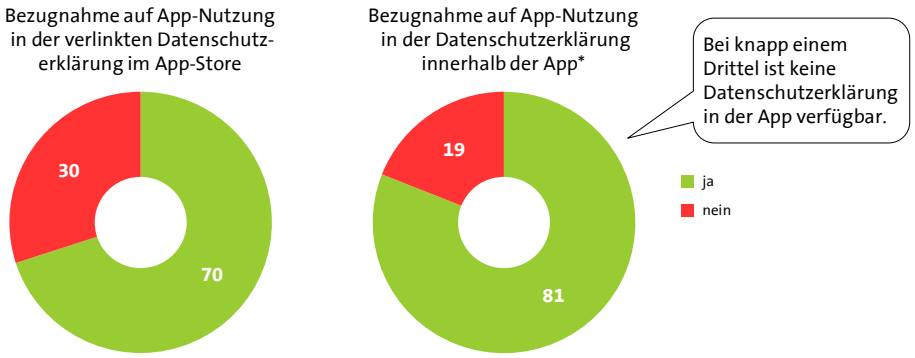
nalität kein Menü besitzen (z. B. „Wasserwaage PRO“). Die Ergebnisse zeigen jedoch, dass ein Drittel der ausgewählten App-Anbieter auf eine Datenschutzerklärung in der App verzichtet. Während die Kategorie „Shopping“ hier insgesamt vorbildlich abschneidet, können besonders in den Bereichen „Spiele“, „Kinder“ und „Fitness/Gesundheit“ deutliche Defizite bei der Verfügbarkeit der Datenschutzerklärung festgestellt werden. Vor allem bei Apps, die sensible Daten nutzen, wie beispielsweise viele Gesundheits-Apps, ist dieses Resultat bedenklich.

Abbildung 9 Verfügbarkeit der Datenschutzerklärung in der App



Leider bedeutet das Vorhandensein einer Datenschutzerklärungen nicht per se, dass die Verbraucher sich auch gut über die jeweilige App informieren können. Nur rund 70 Prozent der Datenschutzerklärungen im Google Play Store und 80 Prozent der Datenschutzerklärungen innerhalb der Apps beziehen sich direkt auf die App-Nutzung oder schließen die App zumindest durch den Verweis auf „alle Dienste“ mit ein (siehe Abbildung 9). Eine Verbraucherinformation kann allerdings nur dann adäquat sein, wenn Verbraucher nachvollziehen können, welche Angaben der Datenschutzerklärung für die App-Nutzung relevant sind.

Abbildung 10 Bezugnahme auf App in der Datenschutzerklärung



Angaben in Prozent; *n=140, wenn Datenschutzerklärung in App verfügbar

Verbraucherinformationen bei Apps – Empirie, November 2017 infas

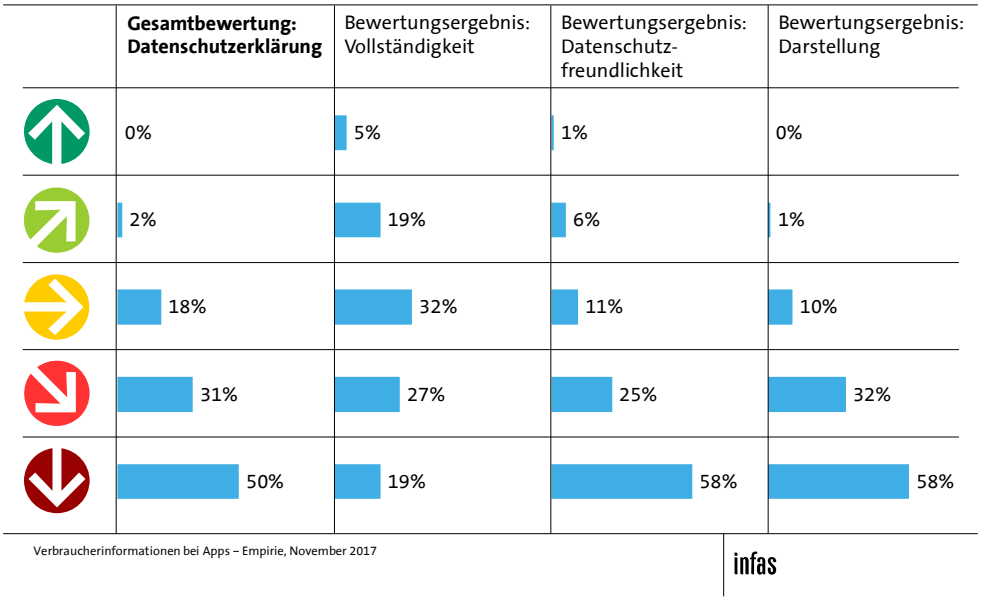
Die inhaltliche Prüfung der Datenschutzerklärungen stellte sich im Rahmen der Analysen als besonders schwierig und zeitintensiv heraus, da die Datenschutzhinweise bei den geprüften 200 App-Anbietern sowohl im Hinblick auf Inhalte, Sprache als auch Darstellung sehr unterschiedlich umgesetzt wurden. Das vom BMJV Ende 2015 vorgestellte Muster zur Darstellung von Datenschutzhinweisen in Form eines One-Pagers wird im App-Bereich bisher nicht angewendet. Die Spannweite bei der Anzahl der Wörter aller geprüften Datenschutzerklärungen liegt zwischen 30 und 33.000 Wörtern. Allein dies zeigt, wie wenig standardisiert die Umsetzung von Datenschutzhinweisen von den Anbietern gehandhabt wird.

Ein durchschnittlicher Leser liest etwa 200 bis 250 Wörter pro Minute.[9] Die durchschnittliche Länge aller geprüften Datenschutzerklärungen liegt bei etwa 2.900 Wörtern. Damit benötigt ein Leser im Mittel bereits über 12 Minuten für das Lesen einer solchen Datenschutzerklärung. Wird die sprachliche Komplexität berücksichtigt, liegt der zeitliche Aufwand vermutlich noch höher. Da sich im Durchschnitt 30 bis 40 Apps auf dem

[9] https://de.wikipedia.org/wiki/Lesegeschwindigkeit

Smartphone eines Nutzers befinden, bräuchte dieser etwa 6 bis 8 Stunden, um alle entsprechenden Datenschutzerklärungen zu lesen. Dieser hohe Aufwand schreckt viele Nutzer jedoch ab, sodass bekanntermaßen nur wenige Verbraucher die Datenschutzerklärungen lesen. Der eigentliche Sinn dieser Texte – nämlich die Verbraucher verständlich zu informieren – wird damit verfehlt. Bei einer zu geringen Anzahl an Wörtern ist wiederum die Angemessenheit der Datenschutzhinweise in Bezug auf die Vollständigkeit der Informationen fraglich. Im Rahmen dieses Projektes wurde eine Länge von 1.000 bis 1.500 Wörtern, was etwa 4 bis 6 Minuten Lesezeit entspricht, als angemessen bewertet.

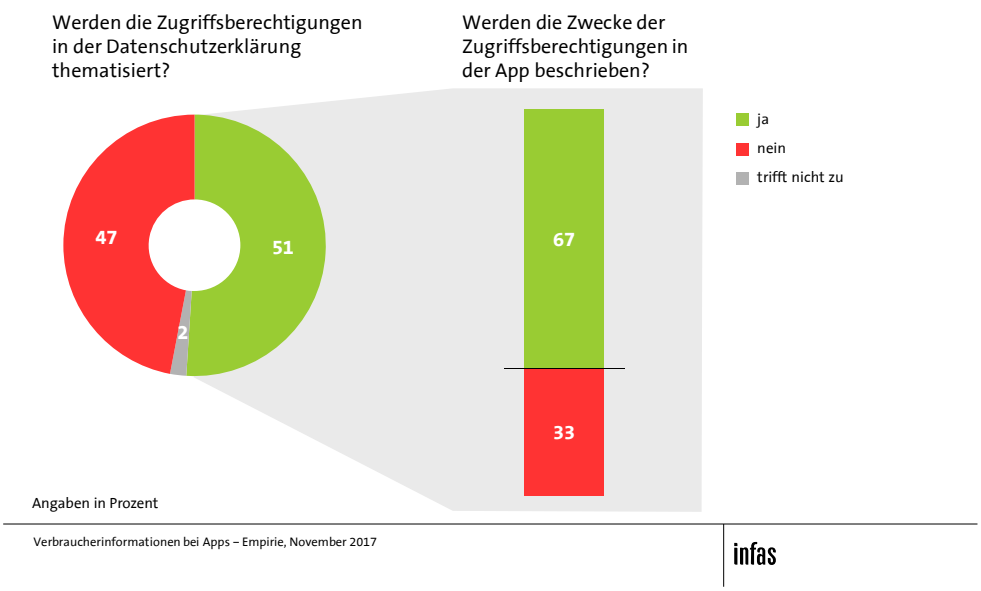
Abbildung 11 Bewertung der Dimension „Datenschutzerklärung“



Die Dimension „Datenschutzerklärung“ ist in drei Kategorien unterteilt (siehe Abbildung 11). Die Bewertung fällt für alle Kategorien und dementsprechend auch für die Gesamtnote der Dimension sehr schlecht aus. In Bezug auf die Vollständigkeit der Angaben schneiden die Apps der Bereiche „Soziale Netzwerke/Messenger“, „Shopping“ sowie „Kinder“ etwas besser ab als der Gesamtdurchschnitt. Besonders schlecht werden die Datenschutzerklärungen der Fitness- und Gesundheits-Apps beurteilt (siehe Anhang, Tabelle 10).

Ein Themenbereich der zur Vollständigkeit der Datenschutzerklärung beiträgt, jedoch von den meisten App-Anbietern vernachlässigt wird, ist die Beschreibung der eingeholten Zugriffsberechtigungen und deren Zwecke. Diese sollten in der Datenschutzerklärung jedoch Erwähnung finden, sofern die Zugriffsberechtigung zur Erhebung personenbezogener Daten führt. Dies ist beispielsweise beim Zugriff auf das Kontaktbuch des Nutzers, aber auch auf Standortdaten und Fotos der Fall. Nur die Hälfte der App-Anbieter thematisieren die „Zugriffsberechtigungen“ in ihrer Datenschutzerklärung.

Abbildung 12 „Zugriffsberechtigungen“ in der Datenschutzerklärung



Im Rahmen der Kategorie „Datenschutzfreundlichkeit“ wurden vor allem die Inhalte der Datenschutzerklärung bewertet. Die Unterschiede zwischen den Apps aus den unterschiedlichen Bereichen fallen hier im Gegensatz zur Kategorie „Vollständigkeit“ weniger gering aus – alle Apps weisen hier deutliche Defizite auf, zum Beispiel bezüglich der Angaben zu Dritten sowie der Begrenzung der Speicherdauer. Auch die Ergebnisse für die Kategorie „Darstellung“ fallen nicht positiv aus. Beurteilt wurden hier Kriterien wie die bereits beschriebene Länge der Datenschutzerklärung, der „Flesch-

Lesbarkeits-Index“[10] und das Vorhandensein eines Inhaltsverzeichnisses sowie von Kapitelüberschriften. 90 Prozent der Apps werden hier mit den Noten „ausreichend“ oder „mangelhaft“ bewertet.

Unabhängig von der Vollständigkeit und Darstellung der geprüften Datenschutzerklärungen fällt auf, dass die App-Anbieter den Begriff „personenbezogene Daten“ teilweise sehr unterschiedlich verwenden. Die Einordnung von Daten als „personenbezogen“ ist nach allen datenschutzrechtlichen Bestimmungen (DSGVO, BDSG und den sektoralen Datenschutzbestimmungen) entscheidend für die Anwendbarkeit des Datenschutzrechts. In der Praxis – vor allem bei digitalen Diensten und Anwendungen – ist diese Einordnung jedoch sehr schwierig. Nach der EU-Datenschutz-Grundverordnung sind alle Daten personenbezogen, die „sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“. Dies trifft im digitalen Zeitalter längst nicht mehr nur auf die klassischen Personenmerkmale wie beispielsweise Name, Telefonnummer oder Adresse zu, die vom Gesetzgeber ursprünglich bedacht wurden. Auch die eindeutige Zuordnung zu einer Online-Kennung (z. B. IMEI, Ad-IDs oder IP-Adresse) oder die Ermittlung genauer Standortdaten werden durch die DSGVO als personenbezogene Daten definiert.

Durch die Aggregation von Daten lassen sich jedoch auch Informationen über vom Datenverarbeiter nicht namentlich bekannte Personen generieren, die jedoch einer bestimmten Kategorie von Nutzern zugeordnet werden können. Diese digitalen Profile, die zum Beispiel auf App-Nutzungsdaten in Kombination mit anderen Identifikatoren des Nutzers basieren, sind für die Betreiber von Online-Diensten oft wertvoller als die „klassischen“ originären Personenmerkmale. Die Frage nach dem Personenbezug ist daher möglicherweise im Hinblick auf den Schutz der Verbraucher gar nicht das

[10] Der Wiener Rudolf Flesch hat den Flesch-Index entwickelt. Der Indikator hilft einzuschätzen, wie eingängig ein Text ist. Der Flesch-Index basiert auf einer Formel. In diese fließen die Anzahl der Sätze, Wörter und Silben ein. Durchläuft der gewählte Text die Formel, steht am Ende ein Wert (flesch reading ease score) zwischen 0 und 100; in Extremfällen kann sich ein Negativwert ergeben. Je höher der errechnete Wert, desto verständlicher ist der Text. (http://fleschindex.de/formel)

vorrangige Kriterium. Vielmehr sind verständliche Angaben der App-Anbieter zu den konkreten Datenverarbeitungsprozessen und deren Folgen entscheidend für die Nutzer.

In Datenschutzerklärungen spielt die Unterscheidung zwischen den „Datentypen“ jedoch oft eine zentrale Rolle. Hier finden App-Nutzer häufig lange Definitionen über die Einordnung der erhobenen Daten, wie in diesem zur Veranschaulichung zufällig ausgewählten Beispiel: „*Nicht-personenbezogene Daten sind Daten, die Sie nicht identifizieren und die nicht dazu verwendet werden können, Sie persönlich zu kontaktieren, z. B. Ihr Geburtstag, Alter, Ihre Postleitzahl, ungefähre Standortdaten (Stadt usw.) und Ihr Geschlecht sowie Informationen über Ihren Computer bzw. Ihr Mobilgerät wie die spezifische Geräte-Kennnummer, IP-Adresse oder andere unveränderliche Kennzeichen und die Hardware/Software/Firmware. Zu den nicht personenbezogenen Informationen zählen ebenfalls die "Nutzungsdaten".* Diese oder ähnliche Ausführungen suggerieren den Verbrauchern, dass die von ihnen erhobenen Merkmale harmlos sind und verleiten zu einem freigiebigeren Umgang mit den eigenen Daten. Wünschenswert wäre, wenn Verbraucher sich auf den verantwortungsbewussten Umgang der Unternehmen mit ihren Daten verlassen und die Folgen der Datenpreisgabe abschätzen könnten – unabhängig davon, ob die App-Anbieter diese als personenbezogen oder nicht definieren.

Auch die Angaben der App-Anbieter zu sogenannten „Drittparteien“, an die Daten weitergegeben werden, fallen sehr unterschiedlich aus. Während einige Anbieter alle Drittparteien konkret benennen, verschleiert ein Großteil der App-Anbieter diese mit Sammelbegriffen, wie beispielweise „Dienstleister“ oder „Werbetreibende“. Ebenso unterschiedlich wird der Umgang mit Opt-In- oder Opt-Out-Möglichkeiten gehandhabt. Diese beziehen sich in der Praxis meist auf die Einbindung von Tracking-Tools oder Werbenetzwerken. Während das Einholen einer aktiven Zustimmung (Opt-In) zur Weitergabe an Werbepartner oder für statistische Analysen eine Ausnahme darstellt, kann bei einigen Apps der Nutzung der Daten zu die-

sen Zwecken zumindest widersprochen werden (Opt-Out). Im Optimalfall kann der Nutzer dies innerhalb der App ganz einfach durch das Anklicken eines Buttons pauschal bestimmen. In den meisten Fällen müssen die Nutzer jedoch für jeden einzelnen Werbetreibenden einen Link in der Datenschutzerklärung anklicken oder sogar eine E-Mail an die entsprechende Drittpartei schicken. Diese Vorgehensweise ist nach unserer Einschätzung jedoch weder verbraucher- noch datenschutzfreundlich.

Was uns auffällt:

- Sowohl die Quantität als auch die Qualität der meisten Datenschutzerklärungen ist mangelhaft.
- Zahlreiche Datenschutzerklärungen sind so lang, dass die Nutzer daraus nicht mit angemessenem Aufwand Informationen ziehen können. Zudem verhindern die mangelnde Verfügbarkeit von Datenschutzhinweisen in den Apps und die schlechte Darstellung vieler Datenschutzerklärungen die nötige Transparenz.
- Die Einordnung von Daten als „personenbezogen“ ist datenschutzrechtlich relevant, ist aber aufgrund ihrer Komplexität für Verbraucher ungeeignet, um die Prozesse der Datenverarbeitung und deren Folgen nachzuvollziehen.

Was wir raten:

- Wichtige Datenschutzhinweise sollten direkt im App Store platziert werden.
- Die Datenschutzerklärungen sollten sich inhaltlich auf die App-Nutzung beziehen.
- Die Länge der Datenschutzerklärungen sollte etwa zwischen 1.000 und 1.500 Wörtern betragen, um alle wichtigen Informationen enthalten zu können und eine angemessene Lesezeit nicht zu überschreiten.
- Die Datenverarbeitungsschritte sollten den Nutzern – unabhängig vom Personenbezug der Daten – besser vermittelt werden.

5.3 Ergebnisse der Dimension „Installation und Inbetriebnahme“

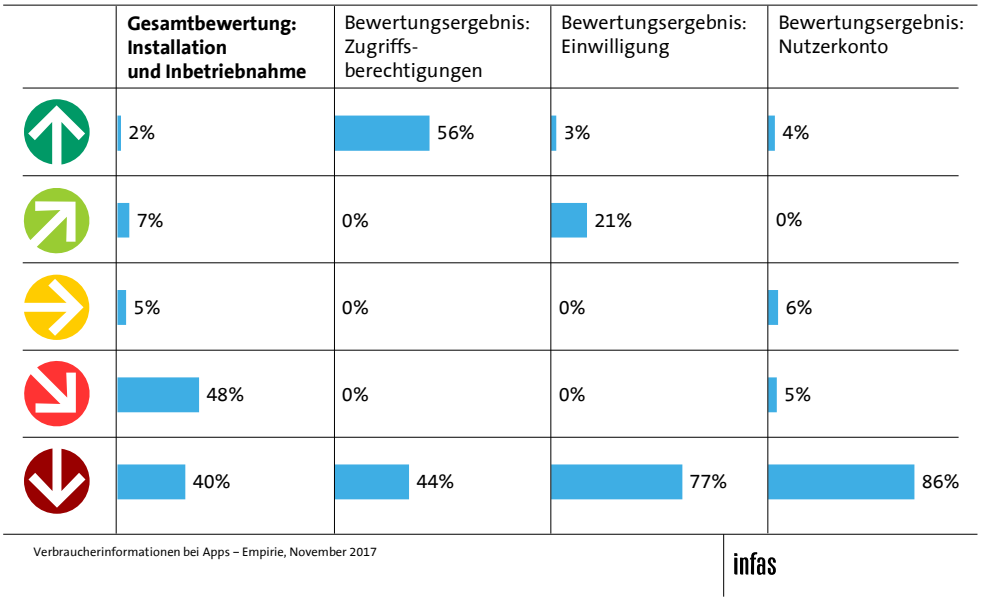
Nachdem sich ein Verbraucher für eine App entschieden hat, folgt der Prozess der Installation und ersten Inbetriebnahme. Apps sollten bei der Installation und auch während der Nutzung nur solche Zugriffsberechtigungen einholen, die für die Funktionalität der App benötigt werden. Dies entspricht dem Grundsatz der Datenvermeidung und Datensparsamkeit nach § 3a des BDSG. Alle Zugriffberechtigungen, das heißt auch diejenigen, die nur bei der Nutzung spezieller Funktionen der App relevant werden, sind im Google Play Store dokumentiert und können vom Nutzer vor der Installation eingesehen werden. Auch können Android-Nutzer seit der Version 6.0 einzelne Zugriffsberechtigungen, genau wie bei iOS, wieder entziehen.

Dies ist zwar insgesamt transparenter und nutzerfreundlicher als noch in den vergangenen Jahren, die Schwierigkeit im Hinblick auf den Datenschutz liegt jedoch woanders. Verbraucher, die nicht über entsprechende Vorkenntnisse verfügen, können anhand der technischen Bezeichnungen den tatsächlichen Zweck der jeweiligen Zugriffsberechtigung vermutlich oft nicht nachvollziehen. Beispielsweise benötigen viele Apps den Zugriff auf die Berechtigung „Fotos/Medien/Dateien“, um auf USB-Speicherinhalte (auch microSD-Karten) zurückgreifen zu können, wenn der interne Speicher des Smartphones aufgrund der benötigten großen Speicherkapazitäten der App nicht ausreicht. Dieser aus Datenschutzsicht unproblematische Zweck ist für den Nutzer nicht ohne Zusatzinformationen nachvollziehbar. Bei vielen Zugriffsberechtigungen wäre daher eine inhaltliche „Übersetzung“ notwendig, um die Folgen einschätzen zu können.

Darüber hinaus herrscht von Seiten der App-Anbieter häufig eine Intransparenz im Hinblick auf Daten, die unabhängig von den Zugriffsberechtigungen eingeholt werden. Dies betrifft insbesondere Standortdaten. Die Ablehnung der Zugriffsberechtigung „Standort“ bedeutet nicht zwangsläufig, dass die App nicht trotzdem den ungefähren Standort des Smartphones (z. B. durch das Auslesen der genutzten WLAN-Netzwerke) ermittelt. In die-

sem Fall täuscht die scheinbar abgelehnte Berechtigung über die tatsächliche Handhabung des App-Anbieters in der Praxis hinweg. Dies ist sowohl aus Sicht des Datenschutzes als auch aus Gründen der Verbraucherfreundlichkeit problematisch, denn es verhindert, dass Verbraucher die Nutzung und Verarbeitung ihrer Daten einschätzen können.

Abbildung 13 Bewertung der Dimension „Installation und Inbetriebnahme“



* Da die Apps bei dieser Kategorie ausschließlich mit den Noten „sehr gut“ oder „mangelhaft“ bewertet wurden, ist die Ausweisung eines Mittelwertes hier nicht sinnvoll.

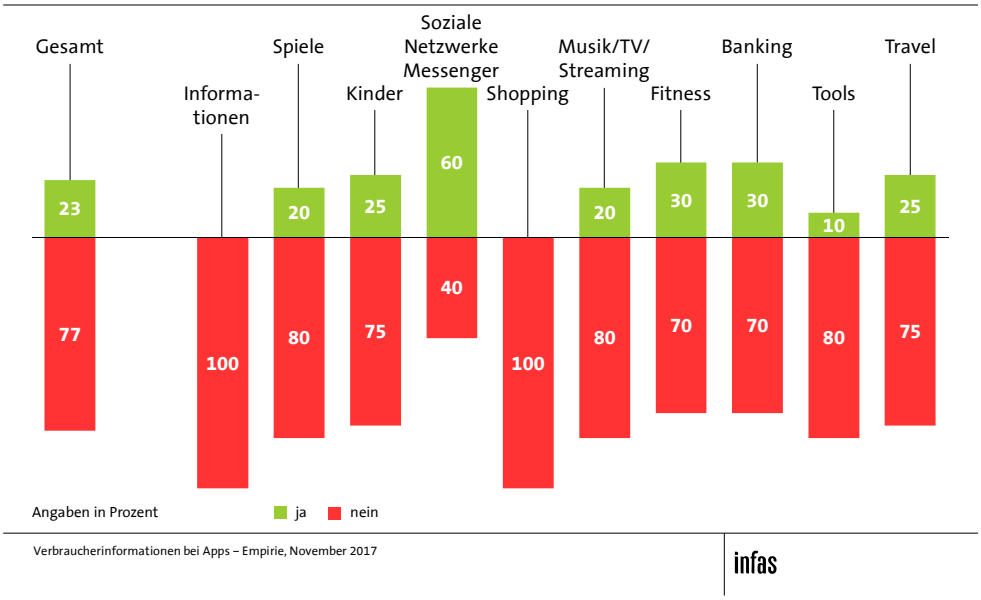
Im Rahmen dieses Projektes wurde mittels einer inhaltlichen Testung geprüft, welche Zugriffsberechtigungen vom App-Anbieter im Google Play Store angegeben und ob diese als erforderlich für die Funktionalität der jeweiligen App eingeschätzt werden. Wenn dies nicht der Fall war, wurde darüber hinaus getestet, ob die App auch ohne die jeweilige Zugriffsberechtigung geöffnet werden kann. Der tatsächliche Zugriff der App auf Standortdaten, Kontakte sowie „Identifier“ wurde im Rahmen der technischen Messung geprüft (siehe Kapitel 5.4).

Bei knapp der Hälfte der Apps sind die im Google Play Store dargestellten Zugriffsberechtigungen für die Zwecke der App nach unserer Einschätzung ohne zusätzliche Erläuterungen nicht verständlich. Entscheidend für die Beurteilung war ausschließlich, ob Berechtigungen aus Nutzersicht nach-

vollziehbar sind oder der App-Anbieter darüber im App Store verständlich aufklärt. Die Anzahl der eingeholten Berechtigungen spielte keine Rolle – Apps, die besonders viele unterschiedliche Funktionalitäten aufweisen (z. B. Facebook oder TripAdvisor), müssen zwangsläufig zahlreiche technische Berechtigungen einholen. Hier zeigen sich deutliche Unterschiede zwischen den App-Bereichen. Besonders schlecht schneiden die Apps aus der Kategorie „Streaming/Musik“, „Fitness" und „Tools“ ab, während erfreulicherweise nur sehr wenige der geprüften Kinder-Apps überflüssige Zugriffsberechtigungen einholen.

Für die Bewertung der Dimension „Installation und Inbetriebnahme“ wurde außerdem geprüft, ob der Nutzer beim ersten Öffnen der App aktiv auf die Datenschutzbestimmungen hingewiesen wird und/oder diesen zustimmen muss, um die App zu nutzen. Dies ist mehrheitlich nicht der Fall.

Abbildung 14 Aktive Einwilligung in die Datenschutzbedingungen beim ersten Öffnen der App



Die meisten App-Anbieter setzen demnach eine stillschweigende Einwilligung des Nutzers zu ihren Datenschutzbestimmungen voraus. Ausnahmen bilden hierbei Apps, bei denen ein Nutzerkonto angelegt werden muss. In den meisten Fällen geht dies mit der Einwilligung in die Nutzungs- und Datenschutzbestimmungen des App-Anbieters einher. Da bei vielen Apps

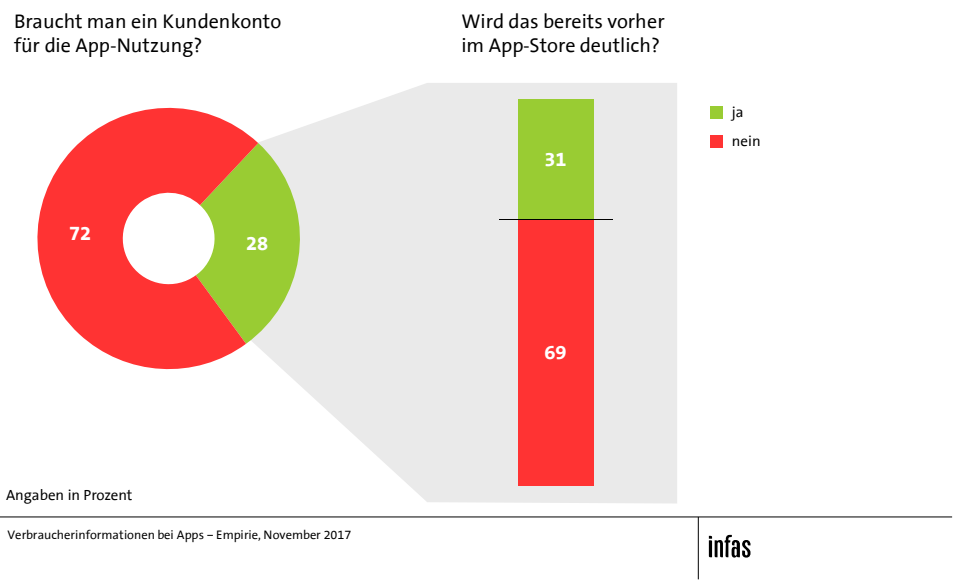
im Bereich „Soziale Netzwerke“, „Fitness“ oder „Banking“ zunächst ein Kundenkonto angelegt werden muss, ergeben sich hier mehr positive Bewertungen innerhalb der Kategorie „Einwilligung“ (siehe Abbildung 14).

An dieser Stelle sei noch einmal auf die im vorangegangen Kapitel beschriebene Problematik hinsichtlich der Nutzung von personenbezogenen Daten hingewiesen. Solange App-Anbieter nach eigenen Angaben keine personenbezogenen Daten erheben, ist eine Einwilligung der Nutzer in die Verarbeitung und Weitergabe ihrer Daten rechtlich nicht erforderlich. Im Rahmen des Projektes wird jedoch eine transparente Aufklärung zur Verarbeitung und Nutzung aller erhobenen Daten und deren Zwecke als wichtige Voraussetzung angesehen, damit Nutzer eine informierte Entscheidung treffen können. Ein fehlender Hinweis auf die Datenschutzhinweise wird im Rahmen dieses Projektes daher grundsätzlich als schlecht bewertet. 77 Prozent aller Apps erhalten daher die Note „mangelhaft“.

Im Rahmen der Dimension „Installation und Inbetriebnahme“ wurde bei Apps, die das Anlegen eines Nutzerkontos erfordern, geprüft, ob diese Erfordernis bereits im Google Play Store ersichtlich ist, wie viele Pflichtangaben dabei vorgenommen werden müssen und ob die App-Anbieter die Möglichkeit der Account-Löschung erläutern. Letzteres wurde als wichtig erachtet, da für eine datenschutzfreundliche Gestaltung solcher Apps zwingend die Möglichkeit für Verbraucher zur dauerhaften Löschung ihrer (personenbezogenen) Daten gegeben sein sollte.

Bei knapp einem Drittel der Apps muss ein Nutzerkonto angelegt werden. Negativ aufgefallen ist hierbei der Umstand, dass dies von zwei Dritteln der App-Anbieter im Google Play Store nicht erläutert wird (siehe Abbildung 15).

Abbildung 15 Notwendigkeit eines Nutzerkontos zur App-Nutzung



Eine solche Anforderung, die mit der Eingabe personenbezogener Daten einhergeht, sollte bereits vor dem Installationsprozess ersichtlich sein. Die Bewertung der Kategorie „Nutzerkonto“ fällt daher insgesamt sehr schlecht aus, da gleichzeitig die Nutzer bei der Mehrzahl der Apps nach unserer Einschätzung zu viele Pflichtangaben machen müssen und die Möglichkeit der Datenlöschung zu wenig thematisiert wird. Insgesamt wurde der gesamte Prozess der Installation und Inbetriebnahme über alle Apps betrachtet im Rahmen der Testung als mangelhaft bewertet.

Was uns auffällt:

- Für die Verbraucher sind viele Zugriffsberechtigungen nicht nachvollziehbar, da diese nur eine technische Anforderung formulieren – der eigentliche Zweck wird jedoch nicht ersichtlich.
- Bei knapp der Hälfte aller Apps werden Zugriffsberechtigungen eingeholt, die für die Funktionalität der App nicht erforderlich sind.
- Die meisten App-Anbieter weisen nicht aktiv auf ihre Datenschutzbestimmungen hin – Ausnahmen bilden notwendigerweise solche Apps, bei denen zunächst ein Nutzerkonto angelegt werden muss.

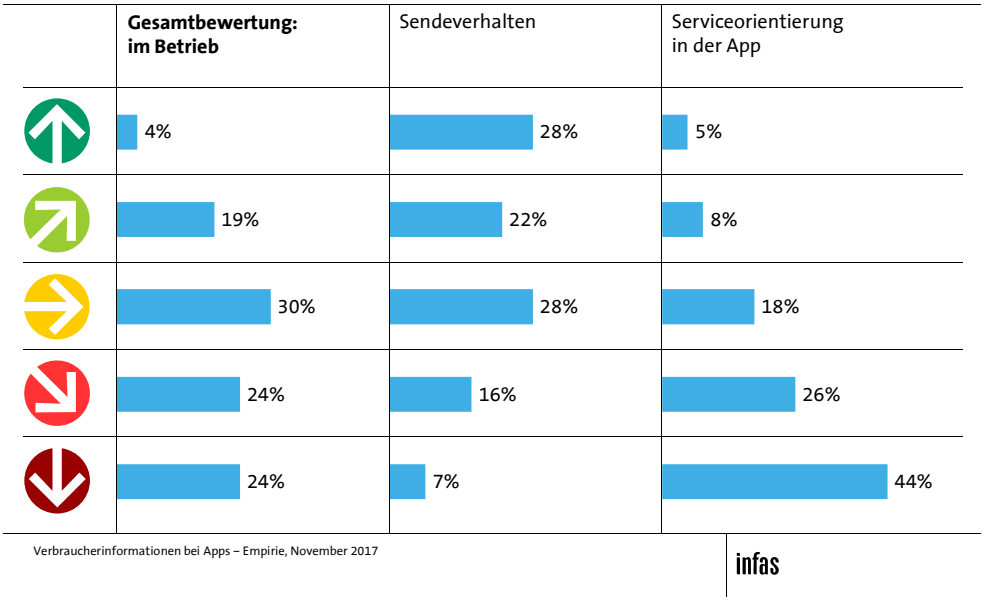
Was wir raten:

- Die Zwecke der technischen Zugriffsberechtigungen sollten bereits im Google Play Store bzw. im App Store erläutert werden.
- Die App-Anbieter sollten transparenter darlegen, wozu sie welche Zugriffsberechtigungen benötigen, damit die Nutzer die Folgen für den Datenschutz besser abschätzen können.
- Beim Öffnen der App sollten App-Anbieter aktiv auf ihre Datenschutzbestimmungen hinweisen.

5.4 Ergebnisse der Dimension „Im Betrieb“

Die Bewertung des Datensendeverhaltens erfolgte für die drei Kriterien „Datenversand an Dritte“, „Datenversand an Ad-Services“ sowie „Datenversand ins Nicht-EU-Ausland“ anhand eines Abgleichs des gemessenen Verhaltens mit den Angaben des App-Anbieters in der Datenschutzerklärung. Zusätzlich wurden die Kommunikation der App im Ruhezustand und die Versendung des Adressbuches, von Standortdaten und anderer „Identifyer“, wie beispielweise der E-Mail-Adresse oder der IMEI des Smartphones, überprüft. Alle Messergebnisse wurden händisch verifiziert und negativ bewertet, wenn kein offenbarer sinnhafter Zweck für die Funktionalität der App festgestellt werden konnte.

Abbildung 16 Bewertung der Dimension „Im Betrieb“



Aufgrund der in Kapitel 4.4 beschriebenen technischen Grenzen der Messung, insbesondere hinsichtlich der Kommunikation des Smartphones mit Google, ist insgesamt von mehr negativem Sendeverhalten bei Apps auszugehen als im Rahmen dieser Studie festgestellt werden konnte. Von den 200 getesteten Android-Apps waren 41 durch Certificate Pinning geschützt und nicht zu entschlüsseln.[11] Bei den getesteten iPhone-Apps waren es 12 von 20[12]. Es wäre irreführend, daraus abzuleiten, dass iPhone-Apps häufiger durch Certificate Pinning abgesichert sind als Android-Apps. Vielmehr beschränkte sich die Auswahl der iPhone-Apps auf Marktführer (Facebook, WhatsApp, Dropbox) oder auch kritische Dienste (Paypal, Sparkassen). Genau diese Dienste sind aber im Allgemeinen auf beiden Plattformen durch Certificate Pinning geschützt.

Leider sind unter den nicht zu entschlüsselnden Apps auch solche, deren Datensammelverhalten von besonderem Interesse gewesen wäre. Beispielsweise sind sämtliche Apps der Firma Facebook (Facebook, Facebook Messenger, WhatsApp, Instagram) durch Certificate Pinning geschützt. Dies ist im Rahmen der Studie zwar bedauerlich, ansonsten jedoch lobenswert, da die Kommunikation der Facebook-Nutzer vor Angriffen durch Dritte geschützt ist. Selbiges gilt in besonderem Maße für Banking- oder Gesundheits-Apps. Zwischen den unterschiedlichen App-Bereichen zeigen sich dennoch deutliche Unterschiede. Besonders negativ fallen die Apps aus den Bereichen „Shopping“, „Tools“ und „Travel“ auf. Hier konnte besonders häufig ein sehr auffälliges Sendeverhalten nachgewiesen werden (z. B. bei „H&M“, „Kleiderkreisel“, „Airbnb“ und „TripAdvisor“).

[11] Dazu gehören: Amazon Music, Apple Music, Audible, Babyphone 3G, Clark Versicherungen managen, Clash of Clans, Deutsche Bank Mobile, Die TK-App, DriveNow Carsharing, Dropbox, Einzigartiges Pulsmessgerät, E-POST Briefe und Faxe, Facebook, Facebook Messenger, FIFA Mobile Fußball, Goodgame Empire: Four Kingdoms, Google Chrome, Hay Day, Instagram, Jodel, Katwarn, Lidl - Prospekte und Angebote, maxdome, Musical.ly , Netflix, PAW Patrol, Payback, paysafecard, Pokémon GO, QQ International, Samsung Smart Switch Mobile, Skype, Snapchat, Threema, TomTom GO Mobile, Twitter, Uber, VPN Master-Free, Weight Watchers Mobile, WhatsApp Messenger, Wire

[12] DB Navigator, Dropbox, Fitbit, Instagram, Paypal, Sparkasse, Spotify Music, Tripadvisor, Youtube, WhatsApp

5.4.1 Strukturelle Analyse der Datenverbindungen

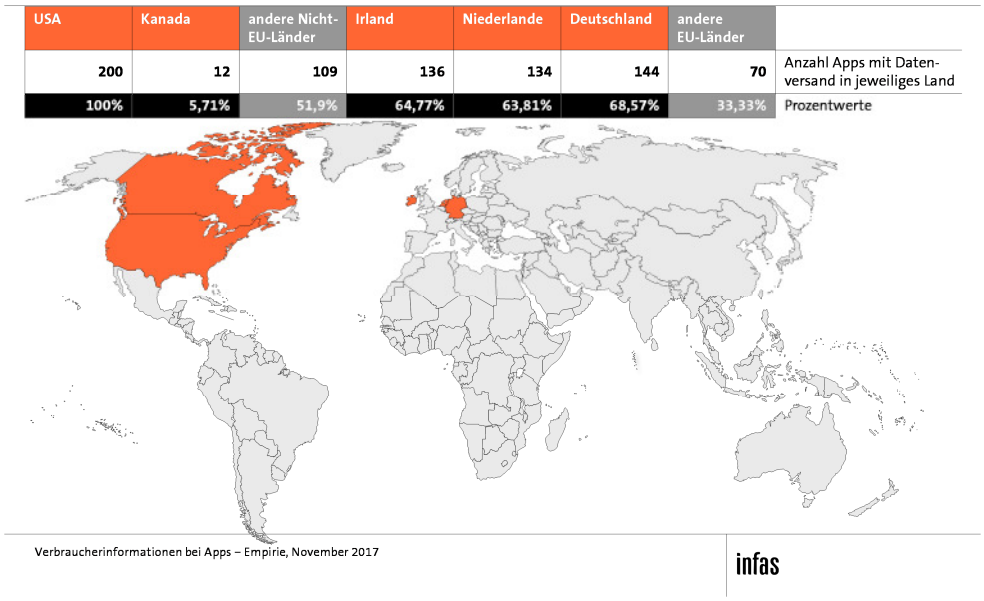
In den 200 App-Tests, die im Rahmen der vorliegenden Studie durchgeführt wurden, wurden insgesamt 1,2 Millionen Internetverbindungen gespeichert. Davon waren 99,6 Prozent einer App zuzuordnen, abhängig von der Parametrisierung (siehe 4.4.1). Unverschlüsselt oder zu entschlüsseln waren 89,5 Prozent der Verbindungen; die restlichen waren durch Certificate Pinning geschützt. Es konnten prinzipiell für alle Datenverbindungen die adressierten Server zugeordnet werden, unabhängig vom Einsatz einer Verschlüsselung. Die so entstandenen 75GB Daten wurden anschließend analysiert.

Entgegen landläufiger Meinungen ergibt es beim Betrachten einer einzelnen App wenig Sinn, über die Anzahl der ausgehenden Verbindungen oder das Herkunftsland der kontaktierten Server zu berichten. Der Grund hierfür ist, dass die Anzahl der Datenverbindungen einer App zunächst keinerlei Informationswert besitzt. Hat eine App erst einmal Daten gesammelt, ist es irrelevant, ob sie diese zeitnah in Form vieler hochfrequenter Datenverbindungen oder einmal wöchentlich in einer einzigen Datenverbindung versendet, da die Daten in jedem Fall dieselben bleiben. Auch ist es ohne Belang, ob ein einziger Server eines Dienstes kontaktiert wird oder mehrere, denn in Summe erhält der Betreiber des Dienstes immer dieselben Daten. Tatsächlich ist es sogar nebensächlich, ob lediglich mit einem einzigen Dienst aus einem einzigen Herkunftsland kommuniziert wird, da ein einziger kontaktierter Server die Daten an hunderte andere Dienste in beliebig vielen Ländern weiterreichen kann. Es genügt also bereits eine einzige Datenverbindung, um die Daten global zu verbreiten.

Das statistische Mittel über viele Apps gibt jedoch durchaus Aufschluss über Größe und Struktur der globalen Datenökonomie. Wie erwartet, kommunizieren die meisten Apps (144) mit deutschen Servern. Ebenso wenig überraschend ist, dass sämtliche getesteten Apps Verbindungen mit amerikanischen Servern unterhalten. Innerhalb Europas zeigt sich jedoch ein unerwartetes Bild. Die ausgehenden Datenverbindungen stehen in keinem

Verhältnis zu der Wirtschaftskraft der Länder. Insbesondere die hohe Anzahl der Apps mit Verbindungen nach Irland (136) und in die Niederlande (134) fallen auf. Dies steht in keinem Verhältnis z. B. zu der Anzahl der Apps, die mit Servern in Frankreich (40) oder Spanien (1) kommunizieren.

Abbildung 17 Datensendeverhalten der Apps nach Ländern



Bezüglich der kontaktierten Server kann festgestellt werden, dass ein Großteil der Verbindungen immer wieder auf dieselben Firmen entfällt: Amazon, Facebook, Google und Microsoft. Jede dieser Firmen betreibt eine globale Infrastruktur, die die jeweilige Firma nicht nur selber nutzt, sondern auch kleineren Entwicklern in Form von Cloud-Services zur Verfügung stellt. Die extreme Markt-Konzentration ist dabei sowohl für den originären Dienst der Betreiber zu konstatieren, als auch für den abgeleiteten Cloud-Markt. Daneben kommunizieren Apps häufig mit sogenannten Content-Delivery-Networks (z. B. Akamai oder Fastly). Deren verteilte Server-Farmen halten große Mediendateien, wie Video- und Musikdateien, an verschiedenen Stellen im Netz vor. Wenn ein Nutzer auf eine solche Mediendatei zugreift, wird sie von dem nächsten benachbarten Server abgespielt.

Unter allen Betreibern einer solchen globalen Infrastruktur fällt einzig Google eine Sonderfunktion zu. Die Firma ist in mehreren Anwendungsfel-

dern gleichzeitig zentraler Marktteilnehmer und größter Datensammler. Sie entwickelt sowohl das Android-Betriebssystem als auch entsprechende Apps. Mit DoubleClick betreibt Google zudem einen der größten Online-Werbedienste. Die Services der Firma basieren zu einem Großteil auf der Auswertung von nutzergenerierten Daten. Darüber hinaus stellt sie mit Google Analytics Dritten einen Tracker-Service zur Verfügung und ist einer der größten Cloud-Anbieter. Von den hundert im Rahmen der Studie am häufigsten kontaktierten IP-Adressen entfielen alleine 90 Prozent auf Google. Bei einer derart breit agierenden Firma fiel es daher schwer, zu differenzieren, in welcher konkreten Rolle eine einzelne Netzwerkverbindung Daten an einen Google-Server übermittelt.

Im Rahmen der Studie fiel außerdem auf, dass ein Großteil der Apps mittels Entwickler-Kits (SDKs) kommuniziert. Diese Softwarekomponenten werden von Drittanbietern zur Verfügung gestellt und erlauben den Zugriff auf deren Dienste. App-Entwickler integrieren SDKs in ihre Apps, um diese Dienste zu nutzen, beispielsweise das Ermöglichen des Logins über Facebook oder die Analyse abstürzender Apps mittels CrashLytics. Da ein SDK jedoch eine eigenständige Softwarekomponente ist, die vollumfänglich in eine App integriert wird, kann es prinzipiell neben der offiziellen noch andere Funktionalitäten ausführen. Im schlimmsten Fall kann ein SDK als eine Art Spyware fungieren. Dabei verfügt das SDK über sämtliche Berechtigungen, die auch der App selber zur Verfügung gestellt wurden. Die im Rahmen der Studie am häufigsten aufgefallenen SDKs sind Amazon-Ads, CrashLytics, DoubleClick, Facebook, Flurry, Google Analytics, HockeyApp, Microsoft-Insights, MoPub, Semasio und Sizmek.[13]

Bereits in den im Rahmen der vorliegenden Studie analysierten Datenverbindungen zu SDKs fiel auf, dass mitunter Daten gesendet werden, die für die bereitgestellte Funktionalität nicht vonnöten sind. So sendet beispiels-

[13] Die Studie „Exodus Privacy“ bietet eine komplette Übersicht der gängigsten SDKs: https://reports.exodus-privacy.eu.org/trackers/

weise Facebook-Login auch die Advertisement-ID des Mobiltelefons. Diese Information ist für die Login-Funktionalität gänzlich unnötig, für einen Werbetreibenden oder jede Form von Tracking jedoch von immenser Bedeutung. Dem einzelnen App-Entwickler sind solche Nebeneffekte der eingesetzten SDKs in der Regel nicht bekannt. Er wird daher ihren Einsatz nicht weiter hinterfragen und sie in der Datenschutzerklärung nicht gesondert ausweisen.

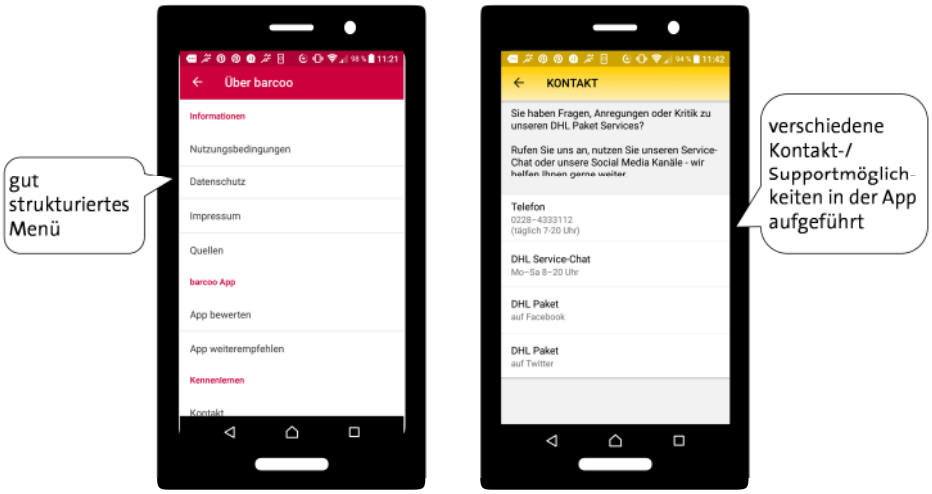
5.4.2 Serviceorientierung in der App

Bei der Kategorie „Serviceorientierung in der App“ wurde unter anderem negativ bewertet, wenn die App über Werbung verfügt, es keine Datenschutzerklärung in der App gibt und dem Nutzer keine Kontakt- oder Supportmöglichkeiten angeboten werden. Das Thema In-App-Werbung wird mit hoher Wahrscheinlichkeit in Zukunft weiter an Bedeutung gewinnen und ist – mehr noch als bei Browser-Werbung am Desktop-PC – aus Datenschutzsicht mit verschiedenen Problemen verbunden. Zum einen sind Smartphones deutlich schlechter geschützt als PCs oder Notebooks. Schadsoftware, z. B. Trojaner, die durch mobile Werbeanzeigen in Apps auf das Smartphone gelangen, kann somit leichter Schaden anrichten. Bisher haben nur wenige Nutzer professionelle Virenschutzprogramme auf ihrem Smartphone installiert. Zum anderen sind auf dem Smartphone viele persönliche Daten (z. B. Adressbuch, Kalender, E-Mail-Postfächer) gespeichert. Zudem ist es aufgrund der Touchscreen-Bedienung deutlich wahrscheinlicher, ungewollt auf Werbebanner zu klicken als dies beispielsweise am PC der Fall ist. Aus diesen Gründen wird In-App-Werbung im Rahmen dieses Projektes als negativ bewertet.

Die Kosten von In-App-Käufen werden nicht bewertet, da die Apps auch innerhalb der zehn geprüften Bereiche zu unterschiedlich waren. Dementsprechend konnte kein einheitlicher Maßstab angewendet werden, um die Kosten von In-App-Käufen als akzeptabel oder inakzeptabel zu beurteilen. Auffällig ist jedoch, dass die In-App-Kosten insbesondere bei den geprüften Spiele-Apps – auch denen für Kinder – oftmals sehr hoch sind. Hier

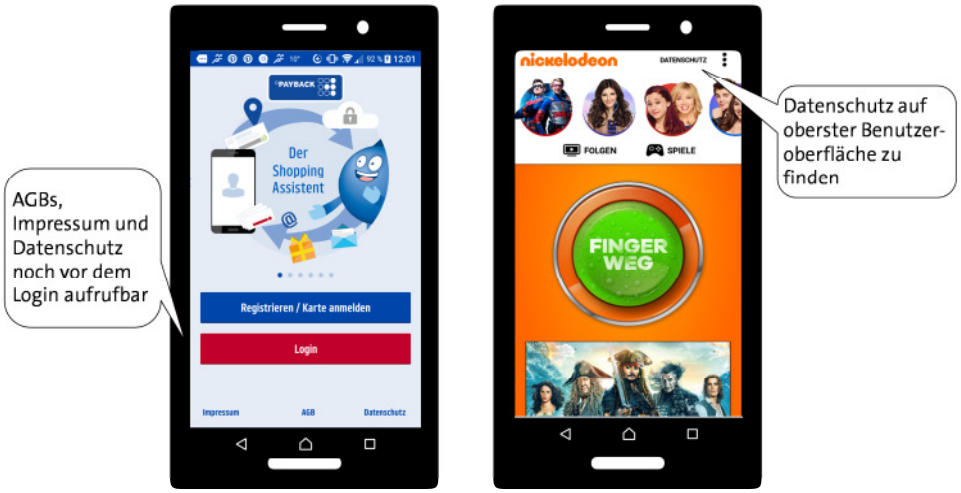
reicht die Spannweite von 1,99 € bis 109,99 €. Gerade bei Apps, die auch von Kindern genutzt werden, sind Kosten im zwei- oder sogar dreistelligen Bereich sehr bedenklich. Zu ähnlichen Ergebnissen kommt auch die Stiftung Warentest in ihrer Kinder-Apps-Testung.[14]

Abbildung 18 Beispiele für Nutzerfreundlichkeit in der App I



Verbraucherinformationen bei Apps – Empirie, November 2017 | infas

Abbildung 19 Beispiele für Nutzerfreundlichkeit in der App II



Verbraucherinformationen bei Apps – Empirie, November 2017 | infas

[14] Stiftung Warentest (2017): Pokémon Go, Minecraft & Co

44 Prozent der Apps erhalten die Note „mangelhaft“. Für die Dimension „Im Betrieb“ ergibt sich daher ein gemischtes Bild – jedoch mit insgesamt mehr schlechten Beurteilungen. Ein Drittel der Apps werden mit der Note „mangelhaft“ bewertet, während knapp ein Viertel die Noten „gut“ oder „sehr gut“ erhält.

Was uns auffällt:

- Das Sendeverhalten ist insbesondere bei vielen Apps aus den Bereichen „Travel“, „Shopping“ und „Tools“ auffällig. Bei Apps aus dem Bereich „Banking“ und „Soziale Netzwerke“ ist die Kommunikation am häufigsten verschlüsselt.
- In-App-Werbung ist mit verschiedenen datenschutzrechtlichen Problemen verbunden, die insgesamt noch zu wenig thematisiert werden.
- Die Kosten für In-App-Käufe sind vor allem bei Apps, die von Kindern genutzt werden, häufig nicht angemessen.

Was wir raten:

- Apps, die personenbezogene Daten verarbeiten und/oder Werbung enthalten, sollten verpflichtend über eine Datenschutzerklärung in der App verfügen.
- Auch Kontaktangaben, zumindest über einen Kontaktkanal (z. B. per E-Mail oder Telefon), erhöhen aus unserer Sicht die Nutzerfreundlichkeit innerhalb der App.
- Verbraucher sollten bezüglich der Folgen der Einbindung von Werbung innerhalb von Apps stärker sensibilisiert werden.

5.5 Exkurs: Google versus Apple

Mit einem weltweiten Marktanteil von 87,7 Prozent ist Android von Google das bedeutendste Betriebssystem für Smartphones. Der Konkurrent iOS von Apple kommt auf einen Marktanteil von knapp unter 12,1 Prozent.[15] Zusammen stellen beide Unternehmen die wichtigsten Plattformen zur Verfügung, auf denen Apps angeboten werden können. Ein großer Teil der App-Anbieter bietet seinen Nutzern für beide Betriebssysteme ein nahezu gleiches Produkt an, welches sich bezüglich der Funktionalität und Bedienung nicht unterscheidet. Beim Vergleich der 20 ausgewählten iOS-Apps mit den jeweiligen Android-Pendants konnten daher im Hinblick auf die Kriterien der Zugänglichkeit der Verbraucherinformationen innerhalb der App keine Unterschiede festgestellt werden. Auch hinsichtlich des Umgangs mit Zugriffsberechtigungen hat Google inzwischen auf Kritik reagiert und seine Android-Version 6.0 verbraucherfreundlicher gestaltet. Seitdem werden Zugriffsrechte wie beim Betriebssystem iOS einzeln eingeholt und können individuell verwaltet werden. So können Nutzer die Rechte auch im Nachhinein wieder entziehen. Dies löst dennoch nicht die in Kapitel 5.3 erläuterte Problematik der Verständlichkeit der technischen Zugriffsberechtigungen.

Google und Apple stellen jedoch unterschiedliche Anforderungen an die App-Anbieter, was den Umfang und die Qualität der Verbraucher- und Datenschutzinformationen in ihren Stores betrifft. Aus diesem Grund ist ein grundsätzlicher Vergleich zwischen den beiden App Stores für die Fragestellung dieser Studie relevant. Diesen liefert die folgende Abbildung in einer Übersicht.

[15] ZDNet: „Android steigert weltweiten Marktanteil auf 87,7 Prozent“, online unter: http://www.zdnet.de/88308701/gartner-android-steigert-weltweiten-marktanteil-auf-877-prozent/?inf_by=59d4f273681db8bb5d8b4604 (zuletzt abgerufen: 14.11.2017)

Abbildung 20 Unterschiede: Google Play Store und App Store

Kategorie	Google Play Store	App Store (seit iOS11)
In-App-Käufe	✔ Angabe der Kosten-Spanne pro Artikel	✔ Auszug der häufigsten In-App-Käufe
Anzeige: Werbeinhalte	✔	✖
Altersfreigabe	USK 0/6/12/16/18	4+, 9+, 12+, 17+
Kontaktinformation	Anbieter, Website, E-Mail, Adresse optional	Anbieter, Website
Widerruf und Erstattung	2 Std. → direkte Rückgabe möglich 48 Std. → Online-Formular nach 48 Std. → nur über App-Anbieter	14 Tage → automatische Rückerstattung
Datenschutzerklärung	verpflichtend	nur unter best. Bedingungen verpflichtend (z. B. Kinder-App, App m. Nutzer-Account)
Zugriffsberechtigungen	verpflichtend	✖
Aktualisierung/Version der App	✔	✔
Kompatibilität	✔	✔
Nutzerbewertung	✔	✔

Verbraucherinformationen bei Apps – Empirie, November 2017 | infas

In-App-Käufe und Angabe über Werbeinhalte

Ob eine App In-App-Käufe anbietet, ist sowohl im Google Play als auch im App Store bereits vor dem Download erkennbar. Die Angabe dazu findet sich in beiden Stores gut sichtbar beim Installations-Button. Die Angabe zur Höhe der Kosten für die In-App-Käufe ist bei Google an einer etwas prominenteren Stelle als im App Store platziert. Die Information über die Kosten der In-App-Käufe handhaben Google und Apple jedoch völlig unterschiedlich. Während bei Google die Preisspanne der möglichen In-App-Käufe pro Artikel angegeben wird, führt Apple die zehn häufigsten In-App-Käufe mit Angabe der Kosten auf. Beide Angaben sind für den Verbraucher nur bedingt nützlich, da sie keinen Aufschluss darüber geben, ob und welcher In-App-Kauf für bestimmte Funktionalitäten oder Zwecke der App notwendig ist.

Eine realistische Angabe über die Kosten bei In-App-Käufen spielt jedoch aus Verbraucherschutzsicht eine wichtige Rolle. Noch bedeutender ist dies bei Apps, die von Kindern genutzt werden. Beim Spiel „Cooking Fever“ gibt der Google Play Store beispielsweise eine Preisspanne von 0,99 bis 99,99 € pro Artikel als In-App-Kauf an, während bei den zehn häufigsten

Käufen im App Store keiner der Top-Käufe über 22,00 € liegt. Ein iOS-Nutzer könnte an dieser Stelle fälschlicherweise davon ausgehen, die Maximal-Kosten für In-App-Käufe liegen bei 22,00 €. Aber die Preisspanne von Google gibt keinen Aufschluss darüber, dass In-App-Käufe im Spielverlauf teilweise, aus subjektiver Sicht zu schnell erforderlich sind, um ein nächsthöheres Level zu erreichen und die Nutzung fortzusetzen.

Ein weiterer relevanter Aspekt bei der Bewertung der Nutzerfreundlichkeit der App Stores ist die Information über Werbung. Im Google Play Store ist an zentraler Stelle, gemeinsam mit der Information zu In-App-Käufen, gekennzeichnet, ob eine App Werbung enthält. Apple schneidet diesbezüglich schlechter ab – hier fehlt eine Angabe zur Einbindung von Werbeanzeigen. Auch Apps für Kinder enthalten häufig Werbung. Problematisch ist, dass die Altersfreigabe der App keine Auskunft darüber gibt, ob im Rahmen der App-Nutzung ausschließlich jugendfreie Werbung gezeigt wird. Bei der Testung von Kinder-Apps hat die Stiftung Warentest hier deutliche Mängel festgestellt.[16]

Informationen zu den Zugriffsberechtigungen und dem Datenschutz

Im Google Play Store muss jeder App-Anbieter Informationen über die möglicherweise im Rahmen der App-Nutzung benötigten Zugriffsberechtigungen zur Verfügung stellen. Auch wenn die Information aus Sicht der Verbraucher über einen zusätzlich Klick in der Kategorie „weitere Informationen“ wenig hervorsticht, hebt sich Google mit dieser Vorgabe für seine App-Anbieter positiv von seinem Konkurrenten Apple ab – dort sind im Store keine Angaben über die benötigten Zugriffsberechtigungen zu finden.

Auch bei Informationen zum Thema Datenschutz liegt Google nach unserem Urteil aus Verbraucherperspektive vor Apple. Apps, die im Google Play Store eingestellt werden, müssen verpflichtend eine Datenschutzerklärung bei Google hinterlegen. Leider gibt es immer noch ältere Apps, die bis

[16] Stiftung Warentest (2017): Pokémon Go, Minecraft & Co

dato keine Datenschutzerklärung hinterlegt haben. Der Ankündigung, diese Apps aus dem Google Play Store entfernen zu wollen, ist Google bisher nicht nachgekommen. Apple verpflichtet seine App-Anbieter nur unter bestimmten Bedingungen zur Verlinkung einer Datenschutzerklärung, zum Beispiel wenn es sich um eine Kinder-App oder eine App mit Nutzerkonto handelt.

Widerruf und Erstattungen

Den Widerruf eines App-Kaufes direkt über den App-Anbieter abzuwickeln, gestaltet sich für den Verbraucher häufig umständlich. Die Anbieter haben ihren Sitz oft im Ausland, geben keine oder nur schwer auffindbare Informationen zu Widerrufmöglichkeiten in ihren AGBs an und Kontaktangaben laufen nach unserer Beobachtung teilweise ins Leere. Apple kommt seinen Nutzern hierbei deutlich entgegen und erspart ihnen das umständliche Vorgehen. App-Käufer können Fehlkäufe innerhalb von 14 Tagen per Knopfdruck zurückgeben und bekommen ihr Geld von Apple wieder.

Anders sieht es beim Google Play Store aus. In den meisten Fällen gewährt Google keine Erstattungen für Apps, wenn der Kauf länger als zwei Stunden zurückliegt. Der Nutzer kann laut AGB von Google „möglicherweise“ innerhalb von 48 Stunden eine Erstattung erhalten, wenn er ein bereitgestelltes Online-Formular ausfüllt. Nach Ablauf dieser Frist kann sich der App-Käufer nur noch direkt an den App-Anbieter wenden. Apple bietet demnach hinsichtlich des Widerrufs von App-Käufen einen wesentlich verbraucherfreundlicheren Service.

Kontaktinformationen und Altersfreigabe

Im Google Play Store ist die Angabe einer E-Mail-Adresse zum App-Anbieter verpflichtend und der Verbraucher kann über die verlinkte E-Mail-Adresse direkt Kontakt zum Anbieter aufnehmen. Als optionale Einträge können bei Google auch der Name des App-Anbieters, ein Link zur Website und eine Adresse im Google Play Store hinterlegt werden. Im

App Store wird vor der Installation einer App lediglich der Name des App-Anbieters und der Link zu dessen Website zur Verfügung gestellt. Eine direkte Kontaktaufnahme über den App Store ist daher nicht möglich. Bei bereits heruntergeladenen Apps bietet Apple einen Link „App Support“ an, der direkt zum Support des App-Anbieters führen sollte.

Die Alterseinstufung von Apps nimmt für den Google Play Store die Unterhaltungssoftware Selbstkontrolle (USK) vor. Insgesamt gibt es dort fünf Einstufungsebenen: USK ab 0 Jahren, ab 6 Jahren, ab 12 Jahren, ab 16 Jahren und ab 18 Jahren. Die USK ist im Rahmen des Jugendschutzgesetzes in Deutschland verantwortlich für die Altersfreigabe von Videospielen. Die Alterseinstufung nach USK ist bei Apps jedoch nur als grobe Richtlinie zu verstehen und passt nicht immer zu den konkreten Angaben der App-Anbieter. Sie ist daher teilweise irreführend und gerade im Hinblick auf kinder- oder jugendfreundliche Apps aufgrund der groben Einteilung unserer Ansicht nach nicht gut geeignet.

Apple nimmt eine eigene Einteilung der Altersfreigabe vor. Diese beschränkt sich auf die vier Unterteilungen: 4+, 9+, 12+ sowie 17+. Apps, die nur für die Nutzung durch Erwachsene (18+) vorgesehen sind, dürfen nicht im App Store angeboten werden. Wenn die Altersfreigabe der App von Apple auf 9+ festgelegt wird, kann diese als „kinderfreundlich“ in der Kinderkategorie des App Stores angeboten werden. Obwohl Apple auf eine Altersstufe verzichtet, erscheint die Einteilung im Hinblick auf den Jugendschutz deutlich besser an der Realität ausgerichtet als die USK-Einstufungen von Google, da sie sich stärker an den entscheidenden Entwicklungsstufen eines Kindes orientiert.

Was uns auffällt:

- Der Google Play Store stellt insgesamt mehr Verbraucherinformationen zur Verfügung als der App Store.
- Gerade in Bezug auf das Anzeigen von Werbeinhalten, benötigten Zugriffsberechtigungen und Kontaktmöglichkeiten zum App-Anbieter punktet Google im Vergleich zu Apple.
- Apple wiederrum hat einen verbraucherfreundlicheren Service bei Rückerstattungen und sinnvollere Stufen bezüglich der Altersfreigabe.

Was wir raten:

- Im Hinblick auf Umfang und Qualität der bereitgestellten Informationen vor oder während der App-Installation tragen Google und Apple durch ihre Vorgaben maßgeblich zur Transparenz bei.
- Die in den letzten Jahren erfolgten Verbesserungen des Google Play Stores zeigen, dass Richtlinien die App-Anbieter zu Gunsten der Verbraucher zu einer höheren Nutzerfreundlichkeit „disziplinieren“ können.
- Problematisch sind insbesondere (unvollständige) Angaben, die Verbraucher in die Irre führen können. Gerade in Bezug auf In-App-Käufe sollte hier nachgebessert werden. Beide App Store-Betreiber sollten eigene Vorschriften (z. B. zum Vorhandensein einer Datenschutzerklärung) besser durchsetzen und „schwarze Schafe“ konsequenter von der Plattform entfernen.

5.6 Gesamtbewertung der Apps

Während in den vorangehenden Abschnitten die Einzelergebnisse innerhalb der Bewertungsdimensionen jeweils übergreifend über alle App-Bereiche dargestellt wurden, werden im Folgenden die Gesamtergebnisse differenziert nach diesen inhaltlichen Gruppen („Spiele“, „Shopping“ usw.) dargelegt. Wie bereits in Kapitel 4.5.6 dargestellt, wurden dazu die Ergebnisse der vier Dimensionen gewichtet zusammengeführt.

Das gewählte Gewicht bildet den Stellenwert der jeweiligen Dimension in der vorliegenden Untersuchung ab:

- 15 % für die Dimension „Im Google Play Store“
- 35 % für die Dimension „Datenschutzerklärung“
- 15 % für die Dimension „Installation und Inbetriebnahme“
- 35 % für die Dimension „Im Betrieb“

Das Ergebnis und die Verteilung über die fünf Bewertungsstufen werden in den folgenden Abbildungen sowohl innerhalb der 10 App-Bereiche (Abbildungen 21 und 22) als auch als Gesamtverteilung (Tabelle 9) dargestellt. Keine der bewerteten Apps erreicht die höchste Bewertungskategorie „sehr gut“. Nur 4 Prozent erhalten ein „gut“, weitere 29 Prozent ein „befriedigend“. Damit verbleiben etwa 7 von 10 bewerteten Apps in einer der beiden schlechtesten Bewertungsstufen: 40 Prozent schneiden mit „ausreichend“ und 27 Prozent mit „mangelhaft“ ab.

Abbildung 21 Gesamtbewertung Kategorien 1 bis 5

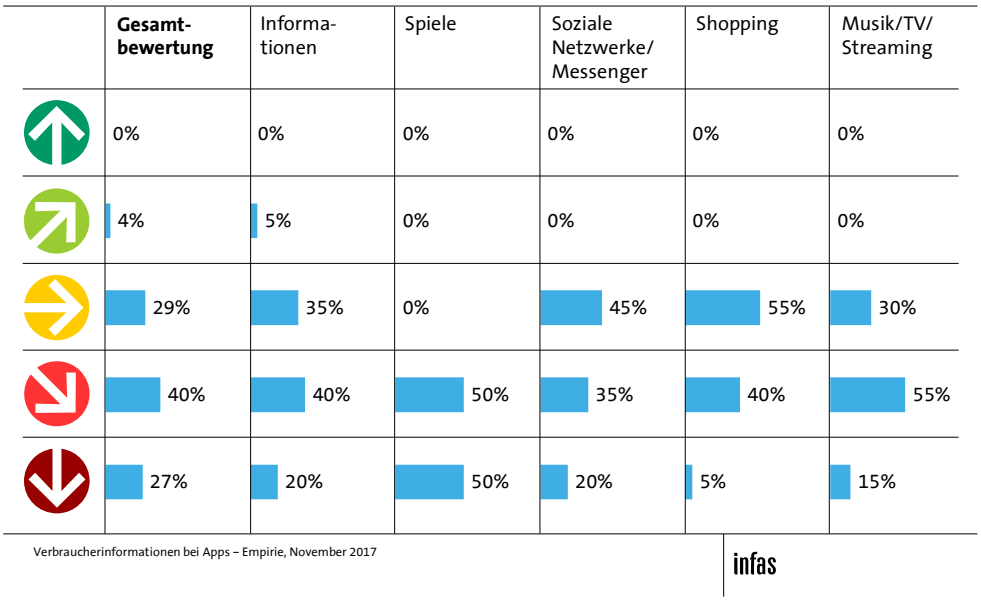
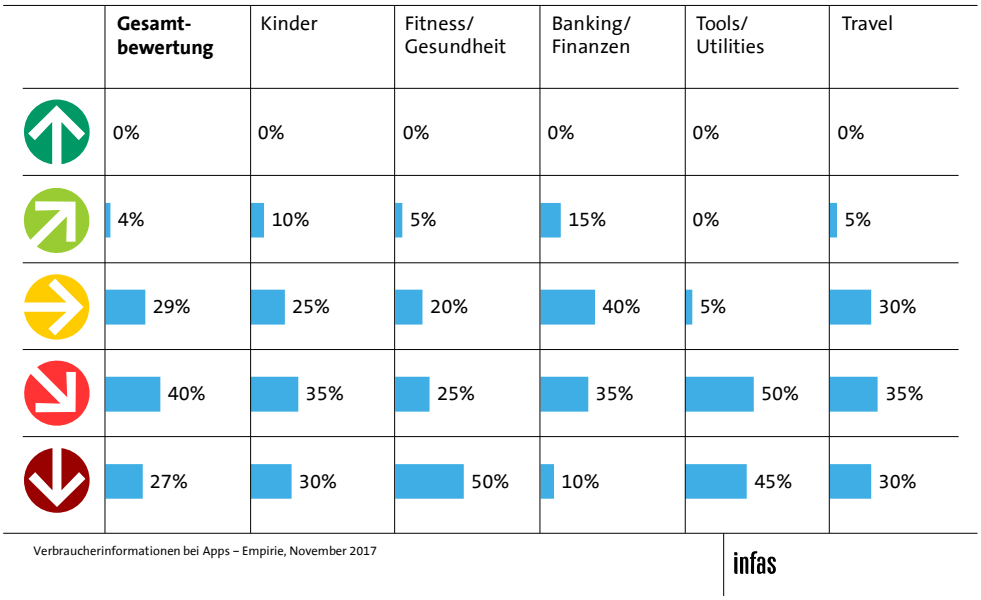


Abbildung 22 Gesamtbewertung Kategorien 6 bis 10



Diese ungünstige Bewertung bestätigt, wie bereits angeführt, das Ergebnis bisheriger anderer App-Bewertungen (vgl. Kapitel 3.1). Trotz gewisser Niveauunterschiede zwischen den App-Bereichen müssen fast durchgängig Defizite konstatiert werden. Besonders auffällig ist dies in den Segmenten „Spiele“ und „Fitness/Gesundheit“. Hier fällt die Hälfte der untersuchten Apps in die schlechteste Bewertungskategorie.

Werden die Bewertungen noch einmal im Überblick betrachtet (siehe dazu Tabelle 9) und die zusätzlich nach App-Bereichen untergliederte Auflistung im Anhang (Tabelle 10), zeigen sich die Ursachen für das Gesamtergebnis. Ausschlaggebend für das ungünstige Gesamturteil sind vor allem die bereits dargestellten Defizite in den Dimensionen „Datenschutzerklärung“ sowie „Installation und Inbetriebnahme“. Dort wiederum fallen diejenigen Aspekte negativ auf, die im weitesten Sinne zu den Ansprüchen an die Serviceorientierung und an eine transparente und möglichst gut verständliche Darstellung des Datenumgangs innerhalb der Apps zu rechnen sind. Ebenso zählt in einigen Fällen das Datensendeverhalten dazu, auch wenn dies aufgrund der geschilderten technischen Begrenzungen und dem im Rahmen dieses Projektes nur eingeschränkt möglichen Prüfaufwand nicht immer vollständig beurteilt werden konnte. Dabei fallen weniger die Abweichungen zwi-

schen den vom Nutzer eingeholten Zustimmungen und dem tatsächlichen Sendeumfang negativ auf, als vielmehr die nicht ausreichende Transparenz, zu welchen Zwecken welche Daten vom Anbieter genutzt werden. Unabhängig davon, ob dieser Umfang jeweils tatsächlich erforderlich oder sinnvoll ist, fehlt es diesbezüglich oft an ausreichenden Begründungen, um als Anwender „informiert" einwilligen zu können. Auch dies fällt in den übergreifenden Schwerpunkt „Nutzerkommunikation", dem die Mehrzahl der bemängelten Aspekte zugerechnet werden können.

Tabelle 9 Gesamtbewertung der App-Bereiche

	Bewertung				
Kategorien					
Erläuterung der Funktion und des Zwecks der App	55 %	22 %	12 %	4 %	8 %
Angabe von relevanten Informationen vor dem Kauf	25 %	30 %	15 %	1 %	31 %
Bewertung: Im Google Play Store	**20 %**	**35 %**	**13 %**	**27 %**	**7 %**
Vollständigkeit	5 %	19 %	32 %	27 %	19 %
Datenschutzfreundlichkeit	1 %	6 %	11 %	25 %	58 %
Darstellung	0 %	1 %	10 %	32 %	58 %
Bewertung: Datenschutzerklärung	**0 %**	**2 %**	**18 %**	**31 %**	**50 %**
Zugriffsberechtigungen	56 %	0 %	0 %	0 %	44 %
Einwilligung	3 %	21 %	0 %	0 %	77 %
Nutzerkonto	4 %	0 %	6 %	5 %	86 %
Bewertung: Installation und Inbetriebnahme	**2 %**	**7 %**	**5 %**	**47 %**	**39 %**
Sendeverhalten	28 %	22 %	28 %	16 %	7%
Serviceorientierung in der App	5 %	8 %	18 %	26 %	44 %
Bewertung: Im Betrieb	**4 %**	**19 %**	**30 %**	**24 %**	**24 %**
Gesamtbewertung über alle Kategorien	**0 %**	**4 %**	**29 %**	**40 %**	**27 %**

Eine gute Verbraucherinformation beginnt bei einem angemessenen Umfang und einer guten Erreichbarkeit der Datenschutzinformation und reicht über die Handhabung und Erläuterungen der Informationen bis hin zum Einhalten der Datensparsamkeit. Auch gehören das Vermeiden von Sachzwängen bei der Installation und Inbetriebnahme und die Kommunikation mit dem Nutzer nach der App-Installation dazu. Positiv wirken sich dabei strukturierende Eingriffe der App-Store-Betreiber aus. Obwohl auch hier Verbesserungspotenzial besteht, zwingen die dort gesetzten Vorgaben die

App-Anbieter zu einer im Schnitt guten bis akzeptablen Darstellung ihres Angebots, der Arbeitsweise und dem Datenverhalten ihrer Apps. Dies stellt die Grundlage für einen informierten App-Nutzer dar, ist jedoch nicht ausreichend. Die Darstellungen und Abläufe innerhalb der Apps bezogen auf ihre Schnittstellen zum Anwender haben in der Regel noch kein zufriedenstellendes Niveau erreicht. Den rechtlichen oder oft auch nur zu erwartenden Informationspflichten wird also nicht genügend nachgekommen. In der Konsequenz vernachlässigt dies die Aufklärung und Information der App-Kunden.

Was uns auffällt:

- Die Mehrheit der Apps schneidet insgesamt schlecht ab. Keine App erreicht die Note „sehr gut“ und nur 4 Prozent die Note „gut“.
- Ausschlaggebend für schlechte Gesamtbewertung sind vor allem Informationsdefizite auf den Ebenen nach der Nutzungsentscheidung. Es wird nicht ausreichend erläutert, was wozu erfolgt. Sinnvolle Begrenzungen fehlen zu häufig, obwohl rein formal korrekt informiert wird. Dies betrifft vor allem die Bereiche Installation, Inbetriebnahme und die Betriebssituation.
- Die vorhandenen Datenschutzerklärungen sind in der Regel zu komplex bzw. nicht app-spezifisch. Dies erschwert die Zugänglichkeit. Zudem sind sie nicht immer dort erreichbar, wo sie zu erwarten und für den Nutzer leicht auffindbar sind.
- Der jeweilige App Store sichert ein Mindestmaß an strukturierter Information bei der dortigen Präsentation der Apps. Innerhalb vieler Apps ist dies jedoch nicht zufriedenstellend gelöst.

Was wir raten:

- Die unbefriedigende Informationsbereitstellung und -aufbereitung erschwert dem Nutzer die Orientierung. Im Ergebnis führt sie zu einer relativ uninformierten Nutzungssituation. Dies widerspricht der Idee einer „informierten Einwilligung“ und stellt diese insgesamt eher in Frage.
- Soweit das Instrument einer „Datenschutzerklärung“ in Kombination mit AGBs überhaupt dazu geeignet ist, den damit verbundenen Ansprüchen und der dahinter liegenden Komplexität gerecht zu werden, müssen diese kompakter, spezifischer und besser zugänglich aufbereitet werden. Perspektivisch sollten andere Informationsformen entwickelt werden.

6 Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse

Die Ergebnisse liefern einen Überblick über den Umgang der App-Anbieter mit Verbraucherinformationen und Datenschutz. Obwohl im Rahmen dieser Studie einzelne Apps bewertet werden, liegt das primäre Ziel darin, auf Problematiken bei der Bereitstellung, Aufbereitung und Zuverlässigkeit von Informationen innerhalb der gesamten App-Landschaft aufmerksam zu machen und erste Empfehlungen für Änderungsbedarfe abzuleiten. Die Erkenntnisse der Studie können dazu verwendet werden, evidenzbasierte Handlungsempfehlungen abzuleiten, die sich in erster Linie an den Gesetzgeber und/oder die App Stores, aber auch an die App-Betreiber und -Nutzer richten können.

Im Ergebnis wird die große Mehrheit der bewerteten Apps relativ schlecht beurteilt. Die Begründung liegt in einer verbesserungswürdigen Informationsbereitstellung, wobei Kriterien der Zugänglichkeit, Verständlichkeit und Zuverlässigkeit zugrunde gelegt werden. Dazu gehört auch die Einführung von mehr Standards, die sowohl den Nutzern als auch den App-Betreibern mehr Sicherheiten bieten könnten. Aus den Ergebnissen dieser Studie lassen sich verschiedene Handlungsbereiche für die Zukunft ableiten, die im Folgenden näher erläutert werden.

Vereinfachung der Datenschutzbestimmungen

Die vorgefundene Heterogenität der Datenschutzbestimmungen, mit deutlichen Mängeln bei einer Vielzahl von Apps, ist weder für die Nutzer noch für die App-Entwickler eine zufriedenstellende Situation. Zum einen sind die Nutzer mit der Unübersichtlichkeit, Unverständlichkeit oder Länge der Datenschutzbestimmungen überfordert oder es ist ihnen gar nicht erst möglich, sich vor dem App-Download ausreichend zu informieren. Gleichzeitig fehlt es auch den Unternehmen teilweise an Rechtssicherheit. Bei den geprüften Apps konnte keine Datenschutzerklärung identifiziert werden, die

einem App-Entwickler als Best-Practice für die optimale Umsetzung der Datenschutzbestimmungen dienen könnte – selbst wenn dieser die besten Intentionen für eine optimale Umsetzung hätte. Dabei unterscheidet sich das Datensammelverhalten der allermeisten Apps nur wenig von dem anderer Apps mit ähnlicher Funktionalität. Automatische Datenschutz-Generatoren, in denen die App-Entwickler keine eigens formulierten Texte mehr im App-Store verlinken müssen, wären ein möglicher Lösungsansatz. Die App-Entwickler könnten dann auf bestehende Formulare zurückgreifen, bei denen sie entsprechende Häkchen setzen bzw. erforderliche Angaben eintragen müssten. So könnten korrekte, vollständige und verständliche Datenschutzbestimmungen generiert werden, die für die Nutzer zusätzlich mit Hilfe von Farbsystemen oder Suchfunktionen optimiert werden könnten. Unabhängig davon, sollten die App Store-Betreiber stärker in die Pflicht genommen werden, Sorge dafür zu tragen, dass Datenschutzerklärungen im App Store zugänglich sind. Obwohl Google die Überprüfung vor einiger Zeit angekündigt hat, sind immer noch Apps ohne Datenschutzerklärung oder mit fehlerhaften Links im Google Play Store verfügbar.

Altersfreigabe für Datendienste

Obwohl der Jugendschutz in dieser Studie nicht im Fokus der Untersuchung stand, fällt diesbezüglich auf, dass sich die Jugendfreigabe von Apps bislang vor allem an den Inhalten der App (insbesondere in Bezug auf Sex oder Gewalt) orientiert oder Bezahldienste bzw. In-App-Käufe in die Bewertung einbezieht. Das Datensammelverhalten einer App erhält hingegen keinen Eingang in die entsprechenden Bewertungsschemata. Da die zukünftigen Folgen des entstehenden Datenschattens noch gar nicht abzusehen sind, kann der Schaden theoretisch deutlich höher sein, als ein einmaliger In-App-Kauf. Daher sollten Kinder und Jugendliche vor der leichtfertigen Preisgabe ihrer Daten gesondert geschützt werden. Als Orientierung könnten dabei die Bestimmungen zur Geschäftsfähigkeit gelten (keine Geschäftsfähigkeit bis zum 7. Lebensjahr, beschränkt bis zum vollendeten 18. Lebensjahr). Es sollte folglich über Lösungen nachgedacht werden, wie

auch der Aspekt der Datenpreisgabe im Rahmen von App-Nutzungen stärker in die Jugendschutz-Bewertung einbezogen wird.

Zweckgebundenheit bei Zugriffsberechtigungen

Problematisch in Bezug auf den Datenschutz ist auch die momentane Praxis hinsichtlich der für viele Apps erforderlichen Zugriffsberechtigungen. Der Zugriff auf Daten und Sensoren des Telefons wird momentan vom Nutzer pauschal anstatt zweckbezogen gewährt. Sofern der Nutzer einer App beispielsweise Zugriff auf das Adressbuch für eine bestimmte Funktionalität erteilt, hat die App theoretisch die Möglichkeit, auf das gesamte Adressbuch zuzugreifen und es zu versenden. Auch die teils sehr technischen Bezeichnungen der Berechtigungen können zu Fehleinschätzungen auf Seiten der Nutzer führen. Der Zugriff auf Berechtigungen sollte daher eindeutig und mit der Nennung des Zweckes einhergehen. Grundsätzlich könnten Verstöße gegen solche zweckgebundenen Einwilligungen auch durch die App Store-Betreiber kontrolliert werden, da sie Zugriff auf den Programmcode der App haben und deren Sende- und Nutzungsverhalten nach der Installation analysieren können. Zumindest bei missbräuchlichen Apps mit mehreren tausend Installationen sollten hierbei verdächtige Muster zu erkennen sein, die dann einer entsprechenden Stelle gemeldet werden könnten.

Datenschutzbestimmungen von SDKs

Im Rahmen der Studie fiel außerdem auf, dass ein Großteil der Apps mittels Entwickler-Kits (SDKs) kommuniziert. Diese Programm-Module werden in Apps eingebunden und sammeln für Drittanbieter Daten. Für den Nutzer ist dabei nicht klar, welche SDKs in der von ihm genutzten App zum Einsatz kommen. Allerdings kann auch ein App-Entwickler in seiner Datenschutzauskunft zumeist nur bedingt Informationen über das Datensammelverhalten der von ihm eingesetzten SDKs geben, da ihm dieses in der Regel nicht bekannt ist. Dies führt zu einer Informationslücke, die in Zukunft geschlossen werden sollte. Ein möglicher Ansatz wäre eine vom App Store-

Betreiber vorgegebene Registrierung, bei der die SDKs ihre eigenen Datenschutzbestimmungen vorlegen müssen. In den Beschreibungen des App Stores könnten in der Folge die von einer App genutzten SDKs angezeigt sowie deren Datenschutzbestimmungen verlinkt werden. Der Nutzer würde somit detaillierte Auskunft über das Sammelverhalten der von ihm genutzten Apps sowie der darin enthaltenen SDKs erhalten. Die wachsende Transparenz und Rechtssicherheit wäre auch für die App-Entwickler von Vorteil.

De-Anonymisierung

Wie die Studie gezeigt hat, greifen viele App-Anbieter auf dieselben Cloud-Plattformen, beispielsweise von Google oder Amazon, zurück. Diese wirken de-facto als Anonymisierungsdienste, da sie verhindern, dass Betreiber entsprechender Services auf diesen Plattformen identifiziert werden können. Damit konterkarieren sie den Grundsatz, Betreiber von Servern und Diensten mittels Whois-Einträgen offenzulegen. Dieser Dienst gibt für eine gegebene Domain Auskunft über Name und Anschrift des Betreibers des Servers sowie (falls abweichend) über den inhaltlich Verantwortlichen. Diese Art der Transparenz wäre auch bei Cloud-Anbietern denkbar, um die Betreiber der Dienste auf ihren Plattformen identifizierbar zu machen. Dies könnte ähnlich zu dem existierenden Whois-Service auch voll-digital mittels strukturierter Daten und in Echtzeit erfolgen.

7 Zusammenfassung

Im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) führte infas von Juni bis November 2017 die Studie „Verbraucherinformationen bei Apps – Empirie“ durch.

Im Rahmen der empirischen Studie untersuchte infas 200 für den deutschen Markt relevante Apps für Android-Betriebssysteme im Hinblick auf die Verbraucherinformationen und den Datenschutz. Zusätzlich wurden 20 der ausgewählten Apps auch auf einem iOS-Betriebssystem getestet.

Im Rahmen einer Inhaltsanalyse wurde überprüft, ob die Verbraucher vollständige, richtige und verständliche Informationen zum Datenschutz und zur Funktionalität der App vor dem Download im App Store und innerhalb der App erhalten. Zusätzlich wurden alle Apps im Rahmen eines Labortests zu unterschiedlichen Zeitpunkten hinsichtlich ihres Datensendeverhaltens untersucht. Die Bewertung erfolgte anhand der vier Dimensionen „Im Google Play Store“, „Datenschutzerklärung“, „Installation und Inbetriebnahme“ sowie „Im Betrieb“. Jede Dimension setzte sich wiederum aus verschiedenen Einzelkriterien zusammen. Die Ergebnisse der vier Dimensionen flossen nach ihrer Relevanz gewichtet in das Gesamtergebnis der jeweiligen App ein.

Insgesamt schneidet keine der getesteten Apps mit „sehr gut“ ab und nur 4 Prozent werden mit der Note „gut“ bewertet. Zwei Drittel der Apps erhalten eine schlechte Bewertung (40 Prozent „ausreichend“, 27 Prozent „mangelhaft“). Dabei fallen besonders Spiele- und Fitness-Apps negativ auf. Während die Bereitstellung von Nutzerinformationen im Google Play Store bei vielen Apps noch zufriedenstellend ist, tragen insbesondere die schlechte Aufbereitung und Intransparenz hinsichtlich der Datenschutzbestimmungen der App-Anbieter sowie die schlechte Zugänglichkeit von Verbraucherinformationen innerhalb der App zu diesem Ergebnis bei. Die Studienresultate zeigen einen erheblichen Verbesserungsbedarf bezüglich der Verbraucherinformation bei Apps.

8 Gegenüberstellung der ursprünglich geplanten zu den tatsächlich erreichten Zielen

Ziel der Studie war eine empirische Bestandsaufnahme der Zugänglichkeit und Verständlichkeit von Verbraucherinformationen und Datenschutzhinweisen von relevanten Smartphone-Apps auf dem deutschen Markt. Darüber hinaus sollte die tatsächliche Praxis des Datensendeverhaltens von 200 Apps überprüft und mit den Angaben aus den Datenschutzerklärungen verglichen werden. Die Studie soll damit die empirische Basis für die verbraucherpolitische Arbeit des BMJV in diesem Bereich bilden. Das angewendete Projektdesign, bestehend aus einer Inhaltsanalyse und einer technischen Messung anhand eines „Black-Box-Ansatzes“, stellte sich für die Erfüllung der Zielsetzung als angemessen heraus. Die Analyse der Datenströme hinsichtlich der versendeten Inhalte (z. B. Standortdaten oder Adressbucheinträge) unterlag dabei verschiedenen, aktuell zunehmenden Beschränkungen, die vor allem durch die Kommunikation der Betriebssysteme mit Google oder anderen Cloud-Servern entstanden. Dadurch konnten einige Datenströme nur bis in die Cloud und nicht bis zu den eigentlichen Ziel-Servern verfolgt werden. Dennoch konnte die Analyse der Datenströme für 159 der 200 Android-Apps und 12 der 20 iOS-Apps durchgeführt werden. Neben der inhaltlichen Analyse der Datenströme konnten gemäß der Aufgabenstellung grundlegende Erkenntnisse zu den Strukturen der Datenkommunikation, zum Beispiel im Hinblick auf die Rolle von Cloud-Servern und Entwickler-Kits (SDKs), gesammelt und bewertet werden. Die 200 getesteten Apps bilden den deutschen App-Markt adäquat ab, sodass die Ergebnisse auf die grundlegenden Problematiken bezüglich der Verbraucherinformationen in diesem Zusammenhang hinweisen und wie beabsichtigt eine empirische Grundlage für weitere Schritte liefern.

Literaturverzeichnis

Albrecht, U.-V. (Hrsg.) (2016): Chancen und Risiken von Gesundheits-Apps. Medizinische Hochschule Hannover. Online unter:
http://www.charismha.de/, abgerufen am 15.06.2017.

Balebako, Rebecca; Marsh, Abigail; Lin, Jialiu; Hong, Jason I. & (2014): The Privacy and Security Behaviors of Smartphone App Developers. Workshop on Usable Security. San Diego, California, 23.-26. February 2014. Online unter:
http://repository.cmu.edu/cgi/viewcontent.cgi?article=1278&context=hcii, abgerufen am 15.06.2017.

Balebako, Rebecca; Schaub, Florian; Adjerid, Idris; Acquisti, Alessandro & Cranor, Lorrie F. (2015): The Impact of Timing on the Salience of Smartphone App Privacy Notices. 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices. Denver, Colorado, 12.-16. Oktober. Online unter:
http://dl.acm.org/citation.cfm?id=2808119, abgerufen am 15.06.2017.

Bitkom e.V. (2016): Was muss ich wissen zur EU-Datenschutzgrundverordnung? FAQ. Online unter:
https://www.bitkom.org/Presse/Anhaenge-an-PIs/2016/160909-EU-DSGVO-FAQ-03.pdf, abgerufen am 26.08.2017.

Bundesministerium für Justiz und Verbraucherschutz (Hrsg.) (2017): Verbraucherfreundliche Best-Practice bei Apps: Eine Orientierungshilfe für die Praxis. Erstellt unter Mitwirkung von App Store-Betreibern, App-Entwicklern, App-Anbietern, App-Testern sowie Verbraucher-, Daten- und Jugendschützern. Berlin. Online unter:
https://www.bmjv.de/SharedDocs/Downloads/DE/StudienUntersuchungenFachbuecher/Apps_Best_Practise_StiWa_DE.html?nn=6704238, abgerufen am 15.06.2017.

Düsseldorfer Kreis (Hrsg.) (2014): Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter. Online unter:
http://www.fechner.eu/wp-content/uploads/2014/06/Orientierungshilfe-Datenschutzanforderungen-an-App-Entwickler-und-App-Anbieter.pdf, abgerufen am 15.06.2017.

ePrivacy (Hrsg.) (2015): Datensicherheit und Datenschutz von Apps. Whitepaper. Online unter:
https://www.eprivacy.eu/datensicherheit-und-datenschutz-von-apps/, abgerufen am 17.08.2017.

Forbrukerrådet (Hrsg.) (2016): Appfail. Threats to consumers in mobile apps. Online unter:
URL: https://fil.forbrukerradet.no/wp-content/uploads/2016/03/Appfail-Report-2016.pdf, abgerufen am 15.06.2017.

Future of Privacy Forum (Hrsg.) (2016): FPF Mobile App Study. Online unter:
https://fpf.org/wp-content/uploads/2016/08/2016-FPF-Mobile-Apps-Study_final.pdf, abgerufen am 15.06.2017.

Future of Privacy Forum (Hrsg.) (2012): FPF Mobile App Study. Online unter:
https://fpf.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf, abgerufen am 15.06.2017.

Herrmann, Dominik & Lindemann, Jens (2016): Obtaining personal data and asking for erasure: do app vendors and website owners honour your privacy rights? Sicherheit 2016, Bonn, 5.-7. April. Online unter:
https://svs.informatik.uni-hamburg.de/publications/2016/2016-01-19-Herrmann-Lindemann-Sicherheit2016-preprint.pdf, abgerufen am 15.06.2017.

Kelley, Patrick Gage; Cranor, Lorrie F. & Sadeh, Norman (2013): Privacy as Part of the App Decision-Making Process. In: CHI '13 proceedings of the SIGCHI conference on human factors in computing systems. Tagungsband-Aufsatz, S. 3393-3402. Online unter: URL: http://dl.acm.org/citation.cfm?id=2466466, abgerufen am 17.08.2017.

MOBILSICHER (2017): Smartphone souverän nutzen. Wie man im Handydschungel die Kontrolle behält. Online unter: https://mobilsicher.de/app/uploads/2017/02/smartphones_souveraen_nutzen.pdf , abgerufen am: 26.08.2017

Moll, Ricarda; Schulze, Anne; Rusch-Rodosthenous, Miriam; Kunke, Christopher & Scheibel, Lisa (2017). Wearables, Fitness-Apps und der Datenschutz: Alles unter Kontrolle?. Verbraucherzentrale NRW e. V. (Hrsg.). Online unter: http://www.marktwaechter.de/digitale-welt/marktbeobachtung/wearables-und-fitness-apps, abgerufen am 15.06.2017.

Niemitz, Marcus; Somorovsky, Juraj; Mainka, Christian & Schwenk, Jörg. (2015): Not so Smart: On Smart TV Apps. Horst Görtz Institute for IT-Security. Online unter: https://www.hgi.ruhr-uni-bochum.de/media/nds/veroeffentlichungen/2015/08/31/SmartTvAttacks.pdf, abgerufen am 26.08.2017.

Schaub, Florian; Rebecca Balebako; Durity, Adam L. & Cranor, Lorrie F. (2015): A Design Space for Effective Privacy Notes. Eleventh Symposium On Usable Privacy and Security. Ottawa, Kanada, 22.-24. Juli. Online unter: https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf, abgerufen am 15.06.2017.

Siebert, Sören (2017): Datenschutzerklärung für Apps: Alles, was Entwickler wissen müssen. Online unter: https://www.e-recht24.de/artikel/hardware-software/10475-datenschutzerklaerung-fuer-apps.html, abgerufen am 15.06.2017.

Stiftung Warentest (Hrsg.) (2017): Connected Cars: Die Apps der Autohersteller sind Datenschnüffler. In: test, Heft 10/2017, S.70-75.

Stiftung Warentest (Hrsg.) (2017): Pokémon Go, Minecraft & Co: So werden Kids mit Apps abgezockt. In: test, Heft 7/2017, S.26-32.

Zang, Jinyan; Dummit, Krysta; Graves, James; Lisker, Paul & Sweeney, Latanya (2015): Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps. In: Journal of Technology Science, Working Paper 1/2015. Online unter: http://techscience.org/a/2015103001, abgerufen am 15.06.2017.

Anhang

Tabelle 10 Bewertungsschritte und Notenskala

Schritt 1: Punktevergabe für Erfüllung von Einzelkriterien und Umrechnung der in einer Kategorie erreichten Punktzahl in Prozentwert	**Schritt 2: Bildung des Prozentwerts der jeweiligen Dimension aus dem Mittelwert der Prozentwerte der zugehörigen Kategorien**	**Schritt 3: Berechnung des Gesamtprozentwertes der App aus Bewertung der Dimensionen mit unterschiedlicher Gewichtung**	**Schritt 4: Überführung der Prozentwerte in Notenskala**
Kategorien:	*Dimension:*	*Zusammensetzung der Gesamtnote:*	*Notenskala:*
Erläuterung im App Store (z. B. Verständlichkeit Funktionsbeschreibung der App) **Info vor Kauf** (z. B. Datenschutzerklärung zur App vorhanden)	**„Im Google Play Store“**	**15 Prozent** Anteil der Dimension „Im Google Play Store“ an der Gesamtnote	100 bis 95 Prozent: sehr gut 94 bis 80 Prozent: gut 79 bis 65 Prozent: befriedigend 64 bis 50 Prozent ausreichend unter 50 Prozent mangelhaft
Vollständigkeit (z. B. Informationen über Weitergabe von Daten an Dritte, Zweck der Nutzung, Löschung der Daten) **Datenschutzfreundlichkeit** (z. B. Detailgrad bei Beschreibung von Drittparteien, Opt-In oder Opt-Out, Begrenzung der Speicherdauer, Information über Portabilität der Daten) **Darstellung** (z. B. Struktur der Datenschutzerklärung, angemessene Länge der Datenschutz-erklärung, Flesch-Lesbarkeitsindex)	**„Datenschutzerklärung“**	**35 Prozent** Anteil der Dimension „Datenschutzerklärung“ an der Gesamtnote	
Zugriffsberechtigungen (z. B. nur notwendige Zugriffsberechtigungen) **Einwilligung** (z. B. Einwilligung in Datenschutzerklärung beim Öffnen der App) **Nutzerkonto** (z. B. Notwendigkeit eines Nutzerkontos ohne Ankündigung, Anzahl Pflichtangaben)	**„Installation/Kauf“**	**15 Prozent** Anteil der Dimension „Installation/Kauf“ an der Gesamtnote	
Sendeverhalten (z. B. Weitergaben von Daten an Dritte/Ad-Networks/ins Nicht-EU-Ausland ohne Angabe in der Datenschutzerklärung, Versendung von Inhalten ohne erkennbaren Zweck) **Serviceorientierung in der App** (z. B. einfacher Zugang zur Datenschutz-erklärung in der App, Kontaktkanäle zum App-Anbieter)	**„Im Betrieb“**	**35 Prozent** Anteil der Dimension „Im Betrieb“ an der Gesamtnote	

Tabelle 11 **Gesamtübersicht App-Bewertungen**
(Methodische Erläuterungen siehe Kapitel 4.1 bis 4.5)

App	Erläuterung im App Store	Info vor Kauf	1. Im Google Play Store	Vollständigkeit	Datenschutzfreundlichkeit	Darstellung	2. Datenschutzerklärung	Zugriffsberechtigungen	Einwilligung	Nutzerkonto	3. Installation/Kauf	Sendeverhalten	Serviceorientierung in der App	4. Im Betrieb	Gesamtergebnis
Kategorie: Information															
BBC NEWS	70%	86%	78%	77%	50%	43%	57%	100%	0%	0%	50%	80%	43%	61%	60%
BILD APP	100%	100%	100%	77%	29%	71%	59%	100%	0%	0%	50%	80%	79%	79%	71%
Der Postillon	30%	14%	22%	46%	29%	29%	34%	100%	0%	0%	50%	95%	50%	73%	48%
finanzen.net	100%	29%	64%	54%	28%	57%	46%	100%	0%	0%	50%	95%	64%	80%	61%
Focus Online	100%	71%	86%	85%	61%	57%	68%	100%	0%	0%	50%	95%	79%	87%	74%
iKiosk	90%	100%	95%	92%	44%	64%	67%	43%	80%	0%	61%	95%	93%	94%	80%
0KATWARN	100%	83%	92%	15%	38%	0%	18%	100%	0%	0%	50%	65%	0%	33%	39%
kicker	90%	100%	95%	69%	39%	57%	55%	43%	0%	0%	21%	80%	79%	79%	64%
meine-stadt.de	90%	29%	59%	57%	50%	53%	53%	43%	0%	0%	21%	95%	14%	55%	50%
n-tv	100%	86%	93%	77%	39%	57%	58%	100%	0%	0%	50%	60%	64%	62%	63%
Promiflash	100%	0%	50%	0%	0%	0%	0%	43%	0%	0%	21%	40%	21%	31%	22%
Relay for reddit (PRO)	40%	29%	34%	0%	0%	0%	0%	100%	0%	0%	50%	60%	0%	30%	23%
Reuters News	60%	71%	66%	79%	50%	43%	57%	100%	0%	0%	50%	75%	57%	66%	60%
SPIEGEL ONLINE	100%	86%	93%	77%	50%	29%	52%	100%	0%	0%	50%	95%	64%	80%	67%
Tagesschau	100%	17%	58%	46%	56%	71%	58%	100%	0%	0%	50%	40%	79%	59%	57%
WeatherPro	100%	100%	100%	85%	19%	57%	54%	43%	0%	0%	21%	95%	79%	87%	67%
wetter.com	100%	86%	93%	85%	50%	57%	64%	100%	0%	0%	50%	55%	79%	67%	67%
WetterOnline	100%	100%	100%	77%	61%	14%	51%	43%	0%	0%	21%	95%	79%	87%	66%
WetterOnline Pro	100%	100%	100%	77%	83%	14%	58%	43%	0%	0%	21%	85%	93%	89%	70%
ZDFheute	100%	17%	58%	46%	50%	57%	51%	100%	0%	0%	50%	70%	93%	81%	63%

App	Erläuterung im App Store	Info vor Kauf	1. Im Google Play Store	Vollständigkeit	Datenschutzfreundlichkeit	Darstellung	2. Datenschutzerklärung	Zugriffsberechtigungen	Einwilligung	Nutzerkonto	3. Installation/Kauf	Sendeverhalten	Serviceorientierung in der App	4. Im Betrieb	Gesamtergebnis
Kategorie: Spiele															
Angry Birds Rio	70%	86%	78%	46%	50%	43%	46%	100%	0%	0%	50%	80%	50%	65%	58%
Candy Crush	40%	33%	37%	62%	17%	57%	45%	100%	0%	33%	44%	95%	43%	69%	52%
Castle Crush	100%	86%	93%	92%	14%	0%	36%	100%	0%	0%	50%	75%	0%	38%	47%
Clash of Clans	100%	33%	67%	46%	33%	14%	31%	100%	80%	0%	90%	100%	43%	71%	59%
Farming Simulator 18	100%	100%	100%	54%	17%	43%	38%	43%	0%	0%	21%	80%	0%	40%	45%
Hay Day	100%	29%	64%	46%	28%	14%	29%	100%	80%	0%	90%	100%	43%	71%	58%
Ich Einfach Unverbesserlich	100%	86%	93%	69%	17%	0%	29%	43%	80%	0%	61%	95%	0%	48%	50%
Minecraft Pocket Edit.	30%	86%	58%	77%	72%	0%	50%	43%	0%	0%	21%	75%	0%	38%	42%
Mini Metro	90%	14%	52%	92%	50%	0%	47%	100%	0%	0%	50%	70%	0%	35%	44%
Modern Combat 4: Zero Hour	30%	100%	65%	69%	17%	0%	29%	43%	0%	0%	21%	95%	71%	83%	52%
Piano Tiles 2	70%	86%	78%	69%	22%	0%	30%	43%	0%	0%	21%	60%	57%	59%	46%
Plants vs. Zombies	90%	71%	81%	77%	17%	71%	55%	0%	80%	100%	60%	75%	29%	52%	58%
Pokémon GO	60%	100%	80%	57%	50%	14%	40%	100%	0%	0%	50%	100%	43%	71%	59%
Pou	90%	86%	88%	38%	19%	0%	19%	43%	0%	100%	48%	50%	0%	25%	36%
Quizduell Premium	90%	100%	95%	62%	72%	27%	53%	43%	0%	0%	21%	85%	0%	43%	51%
Solitaire	90%	71%	81%	54%	19%	0%	24%	43%	0%	0%	21%	85%	14%	50%	41%
Subway Surfers	60%	86%	73%	54%	10%	50%	38%	43%	0%	0%	21%	60%	57%	59%	48%
The Amazing Spider-Man	90%	100%	95%	69%	17%	0%	29%	43%	0%	0%	21%	95%	14%	55%	47%
Wort Guru	100%	71%	86%	54%	36%	57%	49%	100%	0%	0%	50%	50%	57%	54%	56%
Wort Meister	100%	14%	57%	46%	19%	0%	22%	100%	0%	0%	50%	50%	0%	25%	32%

App	Erläuterung im App Store	Info vor Kauf	1. Im Google Play Store	Vollständigkeit	Datenschutzfreundlichkeit	Darstellung	2. Datenschutzerklärung	Zugriffsberechtigungen	Einwilligung	Nutzerkonto	3. Installation/Kauf	Sendeverhalten	Serviceorientierung in der App	4. Im Betrieb	Gesamtergebnis
Kategorie: Mail/Messenger/Social															
Askfm	100%	71%	86%	64%	37%	29%	43%	100%	80%	44%	75%	40%	57%	49%	56%
E-POST Briefe und Faxe	100%	86%	93%	31%	19%	29%	26%	100%	100%	67%	89%	65%	71%	68%	60%
Facebook	100%	71%	86%	86%	42%	57%	62%	100%	80%	56%	79%	80%	43%	61%	68%
Facebook Messenger	70%	83%	77%	86%	32%	57%	58%	100%	0%	56%	50%	100%	57%	79%	67%
Gmail	100%	86%	93%	62%	27%	29%	39%	100%	0%	22%	41%	85%	50%	68%	57%
Instagram	100%	71%	86%	85%	27%	14%	42%	100%	80%	100%	93%	100%	43%	71%	67%
Jodel	40%	100%	70%	92%	68%	57%	73%	100%	0%	0%	50%	100%	57%	79%	71%
LOVOO - Die Chat & Dating App	100%	29%	64%	71%	68%	0%	47%	100%	80%	22%	67%	50%	0%	25%	45%
Parship Partnersuche	100%	0%	50%	57%	26%	29%	37%	100%	0%	67%	56%	95%	64%	80%	57%
Pinterest	100%	71%	86%	77%	29%	57%	54%	100%	0%	44%	48%	85%	29%	57%	59%
QQ International	10%	86%	48%	71%	23%	0%	31%	43%	0%	33%	25%	95%	14%	55%	41%
Skype	100%	71%	86%	77%	68%	0%	48%	100%	80%	33%	71%	100%	0%	50%	58%
Snapchat	40%	86%	63%	92%	18%	71%	61%	100%	80%	44%	75%	100%	43%	71%	67%
Threema	100%	86%	93%	77%	40%	57%	58%	100%	0%	0%	50%	90%	43%	66%	65%
Tinder	100%	14%	57%	93%	26%	14%	44%	100%	0%	44%	48%	75%	0%	38%	44%
Twitter	10%	86%	48%	71%	58%	29%	53%	100%	80%	56%	79%	90%	29%	59%	58%
WEB.DE Mail	100%	100%	100%	62%	58%	57%	59%	100%	80%	22%	67%	80%	64%	72%	71%
WeChat	70%	14%	42%	0%	0%	0%	0%	0%	80%	33%	38%	60%	14%	37%	25%
WhatsApp Messenger	100%	100%	100%	50%	29%	47%	42%	100%	80%	0%	90%	90%	57%	74%	69%
Wire - Vertrauli-cher Messenger	100%	83%	92%	86%	29%	57%	57%	100%	80%	56%	79%	90%	43%	66%	69%

App	Erläuterung im App Store	Info vor Kauf	1. Im Google Play Store	Vollständigkeit	Datenschutzfreundlichkeit	Darstellung	2. Datenschutzerklärung	Zugriffsberechtigungen	Einwilligung	Nutzerkonto	3. Installation/Kauf	Sendeverhalten	Serviceorientierung in der App	4. Im Betrieb	Gesamtergebnis
Kategorie: Shopping															
Amazon Shopping	100%	86%	93%	77%	72%	71%	74%	43%	0%	0%	21%	70%	64%	67%	66%
ASOS	100%	100%	100%	69%	48%	29%	48%	100%	0%	0%	50%	85%	57%	71%	64%
Conrad	100%	67%	83%	54%	61%	43%	53%	43%	0%	0%	21%	95%	100%	98%	68%
eBay	100%	71%	86%	85%	39%	29%	51%	100%	0%	0%	50%	75%	43%	59%	59%
Ebay Kleinanzeigen	100%	14%	57%	69%	83%	29%	60%	100%	0%	0%	50%	65%	50%	58%	57%
Groupon	100%	83%	92%	69%	48%	43%	53%	43%	0%	0%	21%	65%	57%	61%	57%
H&M	100%	17%	58%	77%	48%	71%	65%	100%	0%	0%	50%	45%	57%	51%	57%
Hornbach	100%	67%	83%	77%	83%	57%	72%	100%	0%	0%	50%	65%	100%	83%	74%
IKEA Store	100%	83%	92%	46%	61%	57%	55%	100%	0%	0%	50%	95%	64%	80%	68%
kaufDA-	100%	83%	92%	92%	50%	57%	66%	100%	0%	0%	50%	55%	71%	63%	67%
Kleiderkreisel	100%	71%	86%	100%	53%	57%	70%	43%	0%	78%	40%	55%	50%	53%	62%
Lidl - Prospekte und Angebote	100%	100%	100%	92%	50%	71%	71%	100%	0%	0%	50%	100%	79%	89%	79%
LIEFERHELD -	100%	100%	100%	100%	61%	57%	73%	100%	0%	0%	50%	60%	79%	69%	72%
marktguru	100%	71%	86%	62%	61%	29%	50%	100%	0%	0%	50%	95%	79%	87%	68%
OTTO	100%	0%	50%	62%	72%	14%	49%	100%	0%	0%	50%	75%	79%	77%	59%
reBuy - Kaufen & Verkaufen	100%	17%	58%	77%	29%	57%	54%	43%	0%	0%	21%	60%	57%	59%	51%
Saturn Deutschland	100%	0%	50%	100%	83%	57%	80%	43%	0%	0%	21%	50%	100%	75%	65%
Shpock	100%	71%	86%	100%	57%	57%	71%	100%	0%	0%	50%	45%	86%	65%	68%
Wish	100%	83%	92%	54%	32%	0%	28%	43%	0%	78%	40%	50%	43%	46%	46%
Zalando	100%	29%	64%	92%	57%	57%	69%	100%	0%	0%	50%	65%	79%	72%	66%

App	Erläuterung im App Store	Info vor Kauf	1. Im Google Play Store	Vollständigkeit	Datenschutzfreundlichkeit	Darstellung	2. Datenschutzerklärung	Zugriffsberechtigungen	Einwilligung	Nutzerkonto	3. Installation/Kauf	Sendeverhalten	Serviceorientierung in der App	4. Im Betrieb	Gesamtergebnis
Kategorie: Musik / Streaming															
Amazon Music	70%	33%	52%	54%	63%	57%	58%	43%	0%	67%	37%	90%	57%	74%	59%
Apple Music	70%	33%	52%	46%	47%	57%	50%	43%	80%	67%	63%	75%	43%	59%	55%
ARD Mediathek	100%	17%	58%	69%	72%	71%	71%	100%	0%	0%	50%	70%	79%	74%	67%
Audible - Hörbücher	90%	17%	53%	54%	42%	71%	56%	43%	0%	0%	14%	100%	43%	71%	55%
Deezer	100%	86%	93%	54%	68%	71%	65%	43%	0%	67%	37%	65%	43%	54%	61%
JustWatch	90%	100%	95%	46%	28%	71%	48%	43%	0%	0%	21%	95%	64%	80%	62%
maxdome	100%	17%	58%	69%	100%	57%	75%	100%	0%	100%	67%	75%	71%	73%	71%
Musical.ly	60%	29%	44%	46%	9%	0%	18%	43%	0%	22%	22%	100%	14%	57%	36%
Napster	100%	100%	100%	100%	58%	57%	72%	100%	0%	56%	52%	60%	57%	59%	68%
Netflix	100%	100%	100%	69%	47%	29%	48%	43%	80%	100%	74%	100%	93%	96%	77%
ProSieben - Live TV, Mediathek	100%	71%	86%	62%	61%	57%	60%	43%	0%	0%	21%	80%	79%	79%	65%
radio.de - Der Radioplayer	100%	43%	71%	69%	72%	71%	71%	43%	0%	0%	21%	70%	64%	67%	62%
Samsung Smart View	70%	83%	77%	69%	58%	14%	47%	100%	0%	44%	48%	85%	0%	85%	65%
Shazam	90%	86%	88%	77%	38%	0%	38%	43%	0%	0%	21%	75%	29%	52%	48%
Sky go	100%	71%	86%	69%	79%	57%	68%	0%	80%	0%	27%	70%	64%	67%	64%
Spotify Music	100%	86%	93%	46%	63%	71%	60%	43%	80%	22%	48%	95%	29%	62%	64%
Tv Spielfilm	100%	29%	64%	46%	50%	57%	51%	100%	0%	0%	50%	95%	50%	73%	60%
Ultimate Guitar Tabs	100%	29%	64%	54%	50%	0%	35%	100%	0%	0%	50%	85%	0%	43%	44%
YouTube	90%	86%	88%	79%	44%	71%	65%	43%	0%	0%	21%	60%	43%	51%	57%
ZDFmediathek	100%	33%	67%	69%	83%	14%	56%	100%	0%	0%	50%	50%	57%	54%	56%

App	Erläuterung im App Store	Info vor Kauf	1. Im Google Play Store	Vollständigkeit	Datenschutzfreundlichkeit	Darstellung	2. Datenschutzerklärung	Zugriffsberechtigungen	Einwilligung	Nutzerkonto	3. Installation/Kauf	Sendeverhalten	Serviceorientierung in der App	4. Im Betrieb	Gesamtergebnis
Kategorie: Kinder															
BRIO World	90%	86%	88%	62%	29%	43%	44%	100%	0%	0%	50%	70%	64%	67%	60%
Conni lesen	100%	29%	64%	77%	50%	43%	57%	100%	0%	0%	50%	50%	0%	25%	46%
Cooking Fever	100%	86%	93%	38%	39%	0%	26%	100%	0%	0%	50%	50%	7%	29%	40%
Die Eiskönigin: Icy Shot	30%	86%	58%	77%	67%	57%	67%	100%	0%	0%	50%	75%	0%	38%	53%
DieMaus	100%	33%	67%	69%	61%	71%	67%	100%	0%	0%	50%	70%	64%	67%	65%
Disney Magic Kingdoms	100%	86%	93%	77%	17%	0%	31%	100%	80%	0%	90%	95%	64%	80%	66%
Dragon Ball Z Dokkan Battle	0%	71%	36%	77%	17%	43%	45%	100%	80%	0%	90%	95%	0%	48%	51%
Duolingo	90%	86%	88%	54%	50%	0%	35%	100%	0%	0%	50%	65%	0%	33%	44%
FIFA Mobile	70%	67%	68%	85%	28%	57%	57%	100%	80%	0%	90%	100%	64%	82%	72%
Goodgame Empire: Four Kingdoms	100%	100%	100%	100%	89%	50%	80%	100%	0%	0%	50%	90%	79%	84%	80%
Kinder Gehirn-trainer	90%	100%	95%	62%	31%	43%	45%	100%	0%	0%	50%	70%	0%	35%	50%
LEGO City My City 2	60%	33%	47%	85%	78%	29%	64%	100%	0%	0%	50%	85%	0%	43%	52%
Malen und Zeichnen für Kinder!	90%	100%	95%	58%	29%	29%	38%	100%	0%	0%	50%	70%	0%	35%	47%
Monopoly Game	70%	71%	71%	85%	28%	57%	57%	0%	0%	0%	0%	95%	57%	76%	57%
Nickelodeon Play	90%	86%	88%	85%	78%	57%	73%	100%	80%	0%	90%	75%	86%	80%	80%
PAW Patrol	90%	86%	88%	85%	78%	57%	73%	100%	0%	0%	50%	100%	57%	79%	74%
Scribblenauts Remix	0%	86%	43%	54%	17%	0%	24%	100%	0%	0%	50%	95%	0%	48%	39%
SimCity BuildIt	90%	71%	81%	85%	28%	57%	57%	100%	80%	0%	90%	95%	43%	69%	70%
Temple Run	90%	86%	88%	69%	29%	0%	33%	100%	0%	0%	50%	75%	0%	38%	45%
Toca Kitchen 2	70%	100%	85%	77%	72%	43%	64%	100%	0%	0%	50%	70%	0%	35%	55%

App	Erläuterung im App Store	Info vor Kauf	1. Im Google Play Store	Vollständigkeit	Datenschutzfreundlichkeit	Darstellung	2. Datenschutzerklärung	Zugriffsberechtigungen	Einwilligung	Nutzerkonto	3. Installation/Kauf	Sendeverhalten	Serviceorientierung in der App	4. Im Betrieb	Gesamtergebnis
Kategorie: Fitness / Gesundheit															
30 Tage Fitness Challenge	90%	100%	95%	43%	10%	0%	17%	43%	0%	0%	21%	95%	57%	76%	50%
7-Minuten-Training	90%	100%	95%	29%	10%	0%	13%	43%	0%	0%	21%	75%	57%	66%	45%
Apothekenfinder	100%	17%	58%	0%	0%	0%	0%	100%	0%	0%	50%	60%	29%	44%	33%
Jameda	100%	100%	100%	62%	56%	57%	58%	43%	0%	0%	21%	75%	86%	80%	67%
Die TK-App	100%	100%	100%	86%	79%	86%	83%	100%	100%	100%	100%	85%	Keine Bew.	85%	89%
EAT SMARTER - Rezepte	90%	29%	59%	69%	29%	29%	42%	100%	80%	0%	90%	95%	86%	90%	69%
Einzigartiges Pulsmessgerät	90%	71%	81%	29%	29%	0%	19%	100%	0%	0%	50%	75%	0%	38%	39%
Erste Hilfe0 DRK	100%	14%	57%	0%	0%	0%	0%	100%	0%	0%	50%	70%	0%	35%	28%
Fitbit	30%	83%	57%	93%	37%	57%	62%	43%	80%	11%	45%	75%	79%	77%	64%
HiPP Baby App	100%	0%	50%	0%	0%	0%	0%	43%	80%	0%	61%	60%	29%	44%	33%
MyFitnessPal	100%	86%	93%	57%	32%	33%	41%	43%	0%	0%	14%	75%	50%	63%	52%
Lifesum	90%	100%	95%	57%	29%	43%	43%	43%	0%	0%	21%	95%	0%	48%	49%
Menstruations-Kalender	90%	86%	88%	43%	10%	0%	17%	0%	0%	0%	0%	55%	7%	31%	30%
Oje, ich wachse	90%	29%	59%	29%	19%	14%	21%	43%	0%	0%	21%	40%	14%	27%	29%
Periodenka-lender	60%	0%	30%	57%	0%	14%	24%	100%	0%	0%	50%	80%	43%	61%	42%
Runtastic	100%	86%	93%	64%	84%	57%	69%	43%	0%	67%	37%	95%	7%	51%	61%
Runtastic PRO	100%	86%	93%	64%	84%	57%	69%	43%	80%	67%	63%	95%	21%	58%	68%
Sleep Cycle alarm clock	90%	100%	95%	64%	19%	43%	42%	100%	0%	0%	50%	70%	0%	35%	49%
Weight Watchers Mobile	40%	83%	62%	71%	27%	29%	42%	43%	0%	78%	40%	100%	Keine Bew.	100%	65%
Yazio	90%	100%	95%	36%	27%	27%	30%	43%	80%	33%	52%	95%	64%	80%	60%

App	Erläuterung im App Store	Info vor Kauf	1. Im Google Play Store	Vollständigkeit	Datenschutzfreundlichkeit	Darstellung	2. Datenschutzerklärung	Zugriffsberechtigungen	Einwilligung	Nutzerkonto	3. Installation/Kauf	Sendeverhalten	Serviceorientierung in der App	4. Im Betrieb	Gesamtergebnis
Kategorie: Banking / Finanzen															
aboalarm	90%	33%	62%	100%	84%	43%	76%	43%	0%	56%	33%	95%	79%	87%	71%
Bruno - Brutto Netto Rechner	100%	86%	93%	8%	0%	57%	22%	100%	0%	0%	50%	80%	64%	72%	54%
CHECK24 Vergleiche	100%	83%	92%	77%	50%	57%	61%	43%	0%	0%	21%	75%	71%	73%	64%
Clark	100%	100%	100%	93%	79%	57%	76%	43%	0%	22%	22%	90%	100%	95%	78%
Deutsche Bank Mobile	70%	33%	52%	31%	53%	20%	35%	43%	0%	56%	33%	65%	64%	65%	47%
Friendsurance	100%	100%	100%	100%	50%	57%	69%	100%	0%	33%	44%	95%	100%	98%	80%
HUK Reise	90%	100%	95%	69%	28%	29%	42%	100%	80%	0%	90%	80%	93%	86%	73%
Klarna	90%	0%	45%	69%	72%	0%	47%	100%	0%	0%	50%	85%	71%	78%	58%
LVM	100%	17%	58%	92%	77%	71%	80%	100%	0%	0%	50%	70%	79%	74%	70%
Mein Haushaltsbuch	100%	29%	64%	64%	55%	57%	58%	100%	0%	0%	50%	85%	71%	78%	65%
MeineFinanzen (7csolutions)	90%	14%	52%	46%	48%	0%	31%	100%	80%	0%	90%	60%	7%	34%	44%
Money Manager	100%	86%	93%	69%	67%	0%	45%	100%	0%	0%	29%	85%	14%	50%	55%
PAYBACK	30%	86%	58%	92%	55%	60%	69%	100%	80%	33%	57%	90%	79%	84%	73%
PayPal	70%	67%	68%	62%	27%	20%	36%	43%	80%	44%	56%	100%	64%	82%	60%
paysafecard	100%	71%	86%	54%	39%	29%	40%	100%	0%	0%	50%	90%	64%	77%	62%
Sparkasse	70%	100%	85%	69%	92%	57%	73%	100%	100%	100%	100%	65%	100%	83%	82%
Sparkasse+	70%	100%	85%	69%	92%	57%	73%	100%	100%	100%	100%	75%	86%	80%	81%
StarMoney Phone	90%	100%	95%	54%	28%	71%	51%	43%	0%	0%	21%	75%	100%	88%	66%
Währungsrechner - Finanzen100	90%	29%	59%	62%	39%	71%	57%	100%	0%	0%	50%	70%	86%	78%	64%
WebIDent	100%	100%	100%	69%	72%	53%	65%	100%	0%	0%	50%	75%	0%	75%	71%

App	Erläuterung im App Store	Info vor Kauf	1. Im Google Play Store	Vollständigkeit	Datenschutzfreundlichkeit	Darstellung	2. Datenschutzerklärung	Zugriffsberechtigungen	Einwilligung	Nutzerkonto	3. Installation/Kauf	Sendeverhalten	Serviceorientierung in der App	4. Im Betrieb	Gesamtergebnis
Kategorie: Tools / Utilities															
Adobe Acrobat Reader	100%	100%	100%	62%	39%	29%	43%	43%	0%	0%	21%	95%	57%	76%	56%
Avira Antivirus Security	100%	86%	93%	85%	39%	43%	55%	43%	0%	0%	21%	95%	0%	48%	53%
Babyphone 3G	100%	100%	100%	54%	50%	0%	35%	100%	0%	0%	50%	85%	14%	50%	50%
barcoo	100%	86%	93%	69%	10%	71%	50%	100%	0%	0%	50%	55%	79%	67%	61%
Blitzer.de Plus	100%	100%	100%	69%	19%	27%	38%	43%	0%	0%	21%	30%	21%	26%	41%
DHL Paket	100%	29%	64%	57%	39%	50%	49%	43%	80%	0%	61%	95%	79%	87%	63%
Dropbox	100%	33%	67%	85%	27%	57%	56%	43%	0%	78%	40%	55%	50%	53%	54%
facetune	90%	83%	87%	62%	19%	0%	27%	43%	0%	0%	21%	85%	14%	50%	41%
Google Chrome	100%	100%	100%	62%	29%	29%	40%	43%	0%	0%	21%	90%	64%	77%	55%
Google Übersetzer	100%	33%	67%	79%	33%	43%	52%	43%	0%	0%	21%	80%	14%	47%	48%
ImmobilienScout24	100%	71%	86%	62%	28%	57%	49%	43%	0%	0%	21%	55%	86%	70%	55%
LEO Wörterbuch	100%	14%	57%	54%	0%	53%	36%	100%	0%	0%	50%	80%	0%	40%	42%
Mein Wecker	100%	100%	100%	100%	50%	14%	55%	0%	100%	0%	50%	95%	71%	83%	68%
Samsung Smart Switch Mobile	100%	17%	58%	69%	50%	0%	40%	43%	100%	0%	71%	85%	43%	64%	54%
SD Maid Pro - Lizenzschlüssel	70%	86%	78%	54%	29%	29%	37%	100%	0%	0%	50%	75%	29%	52%	49%
Speed View GPS Pro	60%	71%	66%	23%	19%	0%	14%	43%	0%	0%	21%	70%	0%	35%	28%
Super Cleaner - Antivirus	70%	100%	85%	46%	19%	0%	22%	43%	80%	0%	61%	40%	71%	56%	46%
Taschenlampe	90%	86%	88%	38%	19%	0%	19%	43%	0%	0%	21%	60%	14%	37%	34%
VPN Master	70%	29%	49%	77%	29%	7%	38%	0%	0%	0%	0%	35%	29%	32%	32%
Wasserwaage PRO	90%	100%	95%	54%	29%	0%	27%	100%	0%	0%	50%	80%	0%	80%	55%

App	Erläuterung im App Store	Info vor Kauf	1. Im Google Play Store	Vollständigkeit	Datenschutzfreundlichkeit	Darstellung	2. Datenschutzerklärung	Zugriffsberechtigungen	Einwilligung	Nutzerkonto	3. Installation/Kauf	Sendeverhalten	Serviceorientierung in der App	4. Im Betrieb	Gesamtergebnis
Kategorie: Travel															
ADAC Camping/Stellplatz 2017	100%	71%	86%	69%	50%	29%	49%	100%	0%	0%	50%	70%	79%	74%	64%
Airbnb	90%	17%	53%	85%	32%	29%	48%	100%	0%	22%	41%	35%	29%	32%	42%
BlaBlaCar	70%	83%	77%	100%	53%	57%	70%	43%	80%	33%	52%	80%	71%	76%	70%
Booking.com	90%	83%	87%	85%	44%	57%	62%	100%	0%	0%	50%	80%	64%	72%	67%
DB Navigator	70%	83%	77%	92%	39%	57%	63%	43%	0%	0%	21%	95%	100%	98%	71%
DriveNow Carsharing	70%	83%	77%	85%	58%	29%	57%	100%	0%	22%	41%	90%	100%	95%	71%
FlixBus Fernbus App	90%	33%	62%	54%	50%	57%	54%	43%	0%	0%	21%	60%	86%	73%	57%
Google Maps	100%	29%	64%	79%	56%	43%	59%	43%	80%	0%	61%	60%	43%	51%	58%
komoot	100%	100%	100%	92%	45%	71%	70%	100%	80%	56%	79%	85%	79%	82%	80%
Lufthansa	100%	14%	57%	15%	38%	29%	27%	43%	0%	0%	21%	70%	57%	64%	44%
Miles & More	70%	100%	85%	85%	89%	57%	77%	43%	80%	56%	59%	45%	71%	58%	69%
PeakFinder Earth	100%	29%	64%	0%	19%	14%	11%	100%	0%	0%	50%	30%	21%	26%	30%
Plane Finder - Flight Tracker	40%	100%	70%	54%	19%	0%	24%	43%	0%	0%	21%	40%	29%	34%	34%
Ryanair	90%	71%	81%	77%	19%	43%	46%	43%	0%	0%	21%	70%	0%	35%	44%
Skyscanner	100%	86%	93%	54%	39%	0%	31%	100%	0%	0%	50%	65%	57%	61%	54%
TomTom GO Mobile - GPS Karten	100%	100%	100%	62%	29%	29%	40%	43%	0%	0%	21%	65%	29%	47%	48%
TripAdvisor	70%	57%	64%	77%	61%	36%	58%	43%	80%	0%	90%	45%	71%	58%	64%
trivago - Die Hotelsuche	90%	33%	62%	77%	50%	29%	52%	100%	0%	0%	50%	95%	93%	94%	68%
Uber	70%	83%	77%	92%	36%	0%	43%	43%	0%	22%	22%	75%	86%	80%	58%
Urlaubspiraten	100%	17%	58%	69%	50%	14%	45%	100%	0%	0%	50%	95%	7%	51%	50%

Tabelle 12 Operationalisierung und Gewichtung der Bewertungskriterien

Nr.	Bewertungskriterium	Operationalisierung	Gewichtung	Anmerkung
1. Dimension: Im Google Play Store				
1.1 Erläuterung der Funktion und des Zwecks der App				
1.1.1	Verständliche Funktionsbeschreibung	Die App erhält einen Punkt, wenn im App-Store eine Erläuterung über die wesentlichen Aspekte der Funktionalität und des Zwecks der App vorhanden ist.	1.5	
1.1.2	Funktionsbeschreibung auf Deutsch	Vergabe eines Punktes, wenn die Funktionsbeschreibung im App-Store auf Deutsch ist.	1.5	
1.1.3	Info über Online-/Offline-Modus	Vergabe eines Punktes, wenn in der Erläuterung im App Store eine Angabe darüber zu finden ist, ob die App einen dauerhaften Internetzugang für die Nutzung benötigt.	0.5	
1.1.4	Vorwissen über Zweck/Funktion	Vergabe eines Punktes, wenn die Funktionsbeschreibung im App-Store nur dann verständlich ist, wenn man über Vorwissen zum Dienst verfügt.	1.5	
1.2 Relevante Informationen vor dem Kauf				
1.2.1	Informationen über Nutzerprofil (fließt erst in der Kategorie „Nutzerkonto“ in die Bewertung ein)	Information darüber, ob in der App-Beschreibung im Play Store bereits auf die Notwendigkeit eines Nutzerprofils aufmerksam gemacht wird.	-	
1.2.2	Demoversion oder Version ohne Werbung vorhanden	Vergabe eines Punktes, wenn neben der kostenpflichtigen App eine kostenlose Demoversion existiert. Bei kostenlosen Apps wird ein Punkt vergeben, wenn eine Version ohne Werbung (meist kostenpflichtig oder durch In-App-Käufe) angeboten wird.	0.5	
1.2.3	Datenschutzerklärung mit Bezug auf App	Vergabe eines Punktes, wenn sich die im App Store verlinkte Datenschutzerklärung auf die App bezieht.	2.0	Auch wenn Anbieter sich in ihrer Datenschutzerklärung auf „alle Dienste“ beziehen, wurde ein Punkt vergeben.
1.2.4	Mobile Version der Datenschutzerklärung	Vergabe eines Punktes, wenn die im App-Store verlinkte Datenschutzerklärung ohne heranzoomen auf dem Smartphone lesen lässt.	0.5	

1.2.5	Anschrift	Vergabe eines Punktes, wenn im App-Store die Anschrift des App-Anbieters bzw. Entwicklers angegeben ist.	0.5	
2. Dimension: Datenschutzerklärung				
2.1 Vollständigkeit				
2.1.1	Information über personenbezogene Daten	Vergabe eines Punktes, wenn die Datenschutzerklärung Informationen über die Nutzung oder Nicht-Nutzung personenbezogener Daten enthält.	2.0	
2.1.2	Information über Zweck der Nutzung	Vergabe eines Punktes, wenn die Datenschutz-erklärung Informationen darüber enthält, für welche Zwecke die personenbezogenen Daten verwendet werden.	2.0	
2.1.3.2	Sensible Daten vorhanden (fließt nicht in die Bewertung ein)	Trifft zu, wenn die App durch ihre Funktionalitäten Anlass zur Vermutung gibt, dass sie sensible Daten ihrer Nutzer sammelt.	-	Sensible Daten werden hier nach Art.3 Abs. 9 des BDSG definiert.
2.1.3	Information über sensible Daten	Vergabe eines Punktes, wenn die Datenschutz-erklärung Informationen über die Sammlung sensibler Daten enthält.	1.0	Fließt nur in die Bewertung ein, wenn 2.1.3.2 zutrifft.
2.1.4	Information über Weitergabe an Dritte	Vergabe eines Punktes, wenn die Datenschutz-erklärung über die Weitergabe von Daten der Nutzer an Dritte aufklärt.	2.0	
2.1.5	Information über Datenübertragung ins Ausland (fließt erst bei „Sendeverhalten“ in die Bewertung ein)	Trifft zu, wenn die Datenschutzerklärung Informationen über die Übertragung von Daten ins Ausland enthält.	-	
2.1.6	Information über Löschung von personenbezogenen Daten	Vergabe eines Punktes, wenn die Datenschutz-erklärung Informationen über die Löschung personenbezogener Daten enthält.	2.0	
2.1.7	Informationen über Zugriffsberechtigungen in Datenschutzerklärung	Vergabe eines Punktes, wenn die Datenschutz-erklärung Informationen über notwendige Zugriffsberechtigungen enthält.	1.0	
2.1.8	Informationen zu Zwecken der Zugriffsberechtigungen	Vergabe eines Punktes, wenn in der Datenschutz-erklärung die Zwecke der einzelnen Zugriffsberechtigungen erläutert werden.	2.0	
2.1.9	Informationen zur Anwendung eines nationalen Rechts	Vergabe eines Punktes, wenn in der Datenschutz-erklärung die nationale Gesetzesgrundlage genannt wird, auf die sich diese bezieht.	1.0	
2.1.10	Informationen über mögliche Aktualisierungen der Datenschutzerklärung	Vergabe eines Punktes, wenn die Datenschutz-erklärung Informationen über mögliche Aktualisierungen dieser enthält.	1.0	

2.2 Datenschutzfreundlichkeit				
2.2.1	Genaue Nennung von Dritten	Vergabe eines Punktes, wenn nicht nur eine Information über Weitergabe an Dritte enthalten ist, sondern die Dritten auch namentlich genannt werden.	1.0	
2.2.2	Opt-In zur Weitergabe von Daten	Vergabe eines Punktes, wenn die App nur dann Daten an Dritte weitergibt, wenn der Nutzer explizit darin eingewilligt hat.	1.5	Punktvergabe, wenn minds. eine Opt-In-Möglichkeit, z. B. im Hinblick auf Tracking-Tools oder Werbenetzwerke gegeben wurde
2.2.3	Opt-Out zur Weitergabe von Daten	Vergabe eines Punktes, wenn der Nutzer die Möglichkeit hat, der Weitergabe der Daten an Dritte zu widersprechen.	1.5	Punktvergabe, wenn minds. eine Opt-Out-Möglichkeit, z. B. im Hinblick auf Tracking-Tools oder Werbenetzwerke gegeben wurde
2.2.4	Einbindung von Ad-Networks	Vergabe eines Punktes, wenn in der Datenschutzerklärung die Einbildung von Ad-Networks ausgeschlossen wird.	2.0	
2.2.5	Begrenzung der Speicherdauer	Vergabe eines Punktes, wenn die Speicherdauer der Nutzerdaten zeitlich begrenzt wird.	1.0	
2.2.6	Löschung der Daten nach App-Deinstallation	Vergabe eines Punktes, wenn erläutert wird, dass die Daten des Nutzers bei Deinstallation der App gelöscht werden.	1.0	
2.2.7	Hinweis in App/per Mail zur Aktualisierung der Datenschutzerklärung	Vergabe eines Punktes, wenn daraufhin gewiesen wird, dass Nutzer bei Aktualisierung der Datenschutz-erklärung einen Hinweis z. B. in der App oder per E-Mail, erhalten	1.0	
2.2.8	Erneute Einwilligung in Datenschutzerklärung nach Aktualisierung	Vergabe eines Punktes, wenn Nutzer der Datenschutzerklärung nach einer Aktualisierung aktiv zustimmen müssen, um die App weiter zu nutzen	0.5	
2.2.9	Bezug auf deutsches oder europäisches Recht	Vergabe eines Punktes, wenn sich die Datenschutzerklärung auf deutsches Recht oder auf das Recht eines anderen europäischen Staates bezieht.	2.0	
2.2.10	Information über Portabilität in Datenschutzerklärung (fließt nicht in die Bewertung ein)	Trifft zu, wenn die Datenschutzerklärung Informationen zur Portabilität von Daten enthält.	-	
2.2.11	Notwendigkeit von Portabilität gegeben	Vergabe eines Punktes, wenn aufgrund eines Nutzerkontos oder der Funktionalität der App	0.5	Diese Kriterium lehnt sich an das

		die Angabe von eigenen Daten anzunehmen ist und die Datenschutzerklärung einen Hinweis zur Portabilität enthält (siehe 2.2.10)		durch die DSGVO neu etablierte Recht auf Datenübertragung an.
2.3 Darstellung				
2.3.1	Trennung von Datenschutzerklärung und AGB	Abzug eines Punktes, wenn die Datenschutzerklärung nicht von den Allgemeinen Geschäftsbedingungen getrennt ist.	1.0	
2.3.1.2	Wenn keine Trennung, dann separater Link	Vergabe eines Punktes, wenn man durch einen separaten Link zu Beginn der AGB zur Datenschutzerklärung gelangt.	1.0	Wurde nur bewertet, wenn bei 2.3.1 ein Minuspunkt vergeben wurde
2.3.2	Datenschutzerklärung auf Deutsch	Vergabe eines Punktes, wenn die Datenschutzerklärung, die in der App zu finden ist, in deutscher Sprache verfasst wurde.	2.0	
2.3.3	Inhaltsverzeichnis	Vergabe eines Punktes, wenn die Datenschutzerklärung zur besseren Orientierung ein Inhaltsverzeichnis enthält.	0.5	
2.3.3.2	Inhaltsverzeichnis mit Direktlinks	Vergabe eines Punktes, wenn das Inhaltsverzeichnis Links zu den einzelnen Kapiteln der Datenschutzerklärung enthält.	0.5	
2.3.4	Kapitelüberschriften	Abzug eines Punktes, wenn die Datenschutzerklärung keine Kapitelüberschriften enthält.	1.0	
2.3.5	Anzahl der Wörter (fließt nicht in die Bewertung ein)	Länge der Datenschutz-erklärung (Anzahl der Wörter).	0	
2.3.6	Angemessene Länge der Datenschutzerklärung	Vergabe eines Punktes, wenn der Umfang der Datenschutzerklärung zwischen 1.000 und 1.500 Wörtern beträgt. Diese Range wird als akzeptabler zeitlicher Aufwand für den Nutzer befunden.	1.0	
2.3.7	Flesch-Lesbarkeitsindex	Der Wert des Flesch-Lesbarkeitsindex wurde im Rahmen der Studie als Messinstrument für die Lesbarkeit der Datenschutzerklärung ausgewählt. Die Punktvergabe erfolgt nach der folgenden Einteilung: Wert 0-20 = -2 Punkte Wert 21-30 = -1 Punkt Wert 31-40 = 0 Punkte Wert größer 40 = 1 Punkt.	1.0	
2.3.8	Verständlichkeit und Eindeutigkeit	Vergabe eines Punktes, wenn die Datenschutz-erklärung für den Nutzer überwiegend verständliche und klare Formulierungen enthält. Einen negativen Einfluss auf die Beurteilung haben u.a. Verallgemeinerungen wie „Grundsätzlich ist es möglich, dass…“, die	2.0	

		Benennung unklarer Größenordnungen wie „Einige ihrer Daten könnten…“, Formulierungen im Konjunktiv wie „Wir könnten…“ oder „Möglicherweise werden wir…“ sowie der übermäßige Gebrauch eingeschobener Nebensätze und Klammern.		
3. Dimension: Installation und Inbetriebnahme				
3.1 Zugriffsberechtigungen				
3.1.1	Nur notwendige Zugriffsberechtigungen	Vergabe eines Punktes, wenn ausschließlich Zugriffsberechtigungen vom App-Anbieter im Play Store benannt werden, die nachvollziehbar für die Funktionalitäten der App erforderlich sind.	2.0	
3.1.2	Starten der App ohne die nicht notwendigen Zugriffsberechtigungen	Vergabe eines Punktes, wenn die App auch dann zu öffnen war, wenn man die in 3.1.1 als nicht-notwendig eingestuften Zugriffsberechtigungen, verweigert.	1.5	Alle Apps, die laut 3.1.1 keine überflüssigen Zugriffsberechtigungen erhalten, bekommen hier ebenfalls einen Punkt.
3.2 Einwilligung				
3.2.1	Einwilligung in die Datenschutzerklärung und/oder die AGB beim ersten Öffnen der App	Vergabe eines Punktes, wenn beim ersten Öffnen der App in die Datenschutz- oder Nutzungsbestimmungen eingewilligt werden muss oder darauf hingewiesen wird, dass mit der Nutzung der App eingewilligt wird.	2.0	
3.2.2	Lesebestätigung bei Einwilligung enthalten	Vergabe eines Punktes, wenn zusätzlich eine Lesebestätigung verlangt wird, bevor die App genutzt werden kann.	0.5	
3.3 Nutzerkonto				
3.3.1	Notwendigkeit eines Nutzerprofils (fließt nicht in die Bewertung ein)	Information darüber, ob ein Nutzerprofil nur Nutzung der App notwendig ist.	0	
3.3.2	Notwendigkeit eines Nutzerprofils ohne Ankündigung	Abzug eines Punktes, wenn ein Nutzerprofil, wie in 3.3.1 erfasst, notwendig ist, der Nutzer darüber jedoch im Play Store nicht informiert wird.	2.0	Fließt nicht in die Bewertung ein wenn kein Nutzerprofil notwendig ist.
3.3.3	Anzahl Angaben Nutzerkonto (fließt nicht in die Bewertung ein)	Information darüber, wie viele Angaben zur Erstellung eines Nutzerprofils notwendig sind.	0	Fließt nicht in die Bewertung ein wenn kein Nutzerprofil notwendig ist.
3.3.4	Anzahl Pflichtangaben Nutzerkonto	Information darüber, wie viele der benötigten Angaben aus 3.3.3 Pflichtangaben sind, also	0	Fließt nicht in die Bewertung ein

	(fließt nicht in die Bewertung ein)	vom Nutzer zwingend ausgefüllt werden müssen.		wenn kein Nutzerprofil notwendig ist.
3.3.7	Überflüssige Angaben	Abzug eines Punktes, wenn die Anzahl der Pflichtangaben aus 3.3.4 größer drei ist. Mehr als drei Pflichtangaben (z. B. E-Mail, Benutzername und Passwort) werden als nicht angemessen beurteilt.	0.5	Fließt nicht in die Bewertung ein wenn kein Nutzerprofil notwendig ist.
3.3.5	Notwendigkeit eines Dritt-Anbieter-Accounts	Abzug eines Punktes, wenn man zur Nutzung der App zwingend einen Account bei einem Drittanbieter z. B. Google, Facebook oder Amazon benötigt.	1.0	Fließt nicht in die Bewertung ein wenn kein Nutzerprofil notwendig ist.
3.3.6	Anleitung zu Löschung des Accounts in Datenschutzerklärung	Abzug eines Punktes, wenn in der Datenschutzerklärung nicht erläutert wird, wie man das Nutzerprofil löschen kann.	1.0	Fließt nicht in die Bewertung ein wenn kein Nutzerprofil notwendig ist.
4. Dimension: Im Betrieb				
4.1 Sendeverhalten				
4.1.1.1	Weitergabe von Daten an Dritte (fließt nicht in die Bewertung ein)	Information darüber, ob die App Daten an Server von Dritten versendet.	0	
4.1.1	Weitergabe von Daten an Dritte ohne Angabe in Datenschutzerklärung	Abzug eines Punktes, wenn die App Daten an Dritte versendet ohne in ihrer Datenschutzerklärung darauf hinzuweisen.	1.0	
4.1.2.1	Weitergabe von Daten an Ad-Networks (fließt nicht in die Bewertung ein)	Information darüber, ob die App Daten an Server von Ad-Networks versendet.	0	
4.1.2	Weitergabe von Daten an Ad-Networks ohne Angabe in Datenschutzerklärung	Abzug eines Punktes, wenn die App Daten an Ad-Networks versendet ohne in ihrer Datenschutzerklärung darauf hinzuweisen.	1.0	
4.1.3.1	Weitergabe von Daten ins Nicht EU-Ausland (fließt nicht in die Bewertung ein)	Information darüber, ob die App Daten an Server im Nicht EU-Ausland versendet.	0	
4.1.3	Weitergabe von Daten ins Nicht EU-Ausland ohne Angabe in Datenschutzerklärung	Abzug eines Punktes, wenn die App Daten an Server im Nicht EU-Ausland versendet ohne in ihrer Datenschutzerklärung darauf hinzuweisen.	1.5	
4.1.4	Kommunikation im Ruhezustand	Abzug eines Punktes, wenn die App auch dann Daten versendet, wenn sie nicht im Betrieb ist (und notwendige Kommunikation im Ruhezustand auch aufgrund der Funktionalität nicht anzunehmen ist).	0.5	

4.1.5	Versendung Adressbuch ohne Nutzen für die App	Abzug eines Punktes, wenn die App ohne einen erkennbaren Nutzen für den Zweck der App, Daten aus dem Adressbuch des Nutzers versendet.	2.0	
4.1.6	Versendung Standort ohne Nutzen für die App	Abzug eines Punktes, wenn die App ohne einen erkennbaren Nutzen für den Zweck der App, Standortdaten des Nutzers versendet.	2.0	
4.1.7	Versendung Identifyer ohne Nutzen für die App	Abzug eines Punktes, wenn die App ohne einen erkennbaren Nutzen für den Zweck der App, Identifikationsdaten z. B. die die Smartphone-ID des Nutzers oder eine E-Mail-Adresse, versendet.	2.0	
4.3 Serviceorientierung in der App				
4.3.1	Werbeinhalte vorhanden	Vergabe eines Punktes, wenn die App laut Angabe des App-Stores keine Werbung enthält.	1.0	
4.3.2	Kosten für In-App-Käufe (fließt nicht in die Bewertung ein)	Information über den maximalen Kaufpreis für einen In-App-Kauf in dieser App.	0	
4.3.3	Datenschutzerklärung in der App verfügbar	Vergabe eines Punktes, wenn eine Datenschutzerklärung in der App verfügbar ist.	2.0	
4.3.4	Einfacher Zugang zu Datenschutzerklärung in der App	Vergabe eines Punktes, wenn die Datenschutzerklärung innerhalb der App mit zwei Klicks ab der Startseite aufzufinden ist.	1.0	
4.3.5	Datenschutzerklärung mit Bezug auf App	Vergabe eines Punktes, wenn sich die Datenschutzerklärung auf die App-Nutzung oder zumindest auf „alle Dienste“ des App-Anbieters bezieht.	1.0	
4.3.6	Einfacher Zugang zu Impressum in der App	Vergabe eines Punktes, wenn das Impressum innerhalb der App mit zwei Klicks ab der Startseite aufzufinden ist.	0.5	
4.3.7	Anzahl möglicher Kontaktkanäle	Vergabe eines Punktes, wenn in der App drei oder mehr Kontaktkanäle angegeben werden, also z. B. per E-Mail, Anschrift und Telefonnummer. Wenn es ein oder zwei Kontaktkanäle gibt, wird kein Punkt vergeben. Wenn gar keine Kontaktmöglichkeit zum Anbieter besteht, erhält die App einen Punktabzug.	1.0	
4.3.8	Expliziter Hinweis auf Support/Beschwerde-management	Vergabe eines Punktes, wenn in der App auf einen Kundensupport oder auf eine Beschwerdestelle hingewiesen wird.	0.5	