Bundeskartellamt

Sektoruntersuchung Mobile Apps

Bericht

Juli 2021

Sektoruntersuchung Mobile Apps
Bericht gemäß § 32e GWB
Az. V-35/20
Juli 2021

Kontakt
Bundeskartellamt
Beschlussabteilung Wettbewerbs- und Verbraucherschutz
Kaiser-Friedrich-Straße 16
53113 Bonn
poststelle@bundeskartellamt.bund.de
www.bundeskartellamt.de

Vorbemerkung

Die Beschlussabteilung Wettbewerbs- und Verbraucherschutz des Bundeskartellamts hat im Oktober 2020 eine verbraucherrechtliche Sektoruntersuchung nach § 32e Abs. 5 GWB[1] im Wirtschaftszweig *Mobile Apps* eingeleitet. Sektoruntersuchungen richten sich nicht gegen bestimmte Unternehmen, sondern dienen der Untersuchung eines Wirtschaftszweigs im Hinblick auf mögliche verbraucherrechtliche Verstöße.

Auf die Regelung des § 32e Abs. 6 GWB über den ausgeschlossenen Aufwendungsersatz im Falle einer Abmahnung nach § 12 Abs. 1 Satz 2 UWG[2] wird hingewiesen.

---

1 Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bek. v. 26.06.2013 (BGBl. I S. 1750, 3245), zuletzt geändert durch Gesetz vom 09.07.2021 (BGBl. I S. 2506) m. W. v. 15.07.2021 – GWB.

2 Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bek. v. 03.03.2010 (BGBl. I S. 254), zuletzt geändert durch Gesetz vom 26.11.2020 (BGBl. I S. 2568) m. W. v. 02.12.2020 – UWG.

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

A. Zusammenfassung

Bei einer App handelt es sich, so Wikipedia, um eine Anwendungssoftware, genauer um eine „Software, welche den Zweck hat, ein spezifisches Problem zu lösen“.[3] Werden Apps im Bereich mobiler Betriebssysteme eingesetzt, so spricht man von „mobilen Apps“. Im Alltag begegnen diese mobilen Apps dem Verbraucher[4] vor allem auf dem Bildschirm seines Smartphones oder Tablets. Die beiden nach App-Downloadzahlen mit weitem Abstand führenden App-Stores „Google Play“ bzw. schlicht „App Store“ (Apple) warten jeweils mit einem Angebot von mehreren Millionen Apps für alle nur erdenklichen Einsatzmöglichkeiten auf. Ebenso wie die Zahlen heruntergeladener Apps kennen auch die Umsätze der App-Stores seit Jahren nur eine Richtung: steil aufwärts. Verbraucher können in immer mehr Lebensbereichen auf die kleinen „Problemlöser“ zurückgreifen. Dass Apps unseren Alltag erobern, geht indessen auch mit dem Risiko einher, dass bereits die Nutzung spezialisierter Apps Rückschlüsse auf Verbrauchergewohnheiten, Gesundheitsdaten oder weitere intime Informationen erlaubt. In den letzten Jahren haben sich zudem immer ausgereiftere technische Möglichkeiten entwickelt, die es erlauben, das Nutzungsverhalten von Verbrauchern bei Anwendung einer App nachzuvollziehen. Dies kann einerseits auch für den Nutzer Vorteile mit sich bringen, etwa wenn hierdurch nützliche Produktweiterentwicklungen ermöglicht werden. Andererseits werden große Mengen personenbezogener Daten mit dem Ziel verarbeitet, Werbung auszuspielen, die sich an den Vorlieben und Gewohnheiten des jeweiligen Verbrauchers orientiert. Dabei stellt die Anzeige von ggf. nicht gewünschter personalisierter Werbung nicht unbedingt das maßgebliche Problem dar, sondern die womöglich langfristige Speicherung hierfür verwendeter Nutzerprofile, die den Einzelnen identifizierbar machen. Diese können, insbesondere bei Weitergabe oder Hackerangriffen, zu erheblichen Nachteilen für die betroffenen Personen führen (differenzierte Preisstellungen, Verweigerung von Vertragsschlüssen z. B. über Versicherungen, Erpressbarkeit etc.). Entscheidet das eigene Profil über die Anzeige von Meldungen und Meinungen, besteht daneben jedenfalls langfristig die Gefahr, in eine soziale Filterblase zu geraten, die einen Teil der Realität nachhaltig ausblendet.

Zahlreiche Meldungen in den Medien vermitteln derzeit den Eindruck, Verbraucher seien nicht immer in der Lage zu erkennen, bei welchen App-Nutzungen sie welche personenbezogenen Daten preisgäben und an wen. Selbst wo dies der Fall sei, könnten Verbraucher entsprechende Datenübermittlungen nicht immer effektiv stoppen, obwohl sie dies wollten.

---

[3] Wikipedia-Artikel zu Anwendungssoftware, abrufbar unter https://de.m.wikipedia.org/wiki/Anwendungssoftware.

[4] Ausschließlich zum Zweck der besseren Lesbarkeit wird im vorliegenden Bericht auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen sind geschlechtsneutral zu verstehen.

Das Bundeskartellamt hat vor diesem Hintergrund eine Sektoruntersuchung im Bereich „Mobile Apps“ in die Wege geleitet. Dabei wurden zum einen Verbraucher nach ihren konkreten Präferenzen beim Umgang mit mobilen Apps gefragt. Zum anderen wurde beleuchtet, inwiefern App-Stores, App-Publisher und in Einzelfällen auch Betriebssystembetreiber den geäußerten Verbraucherwünschen bzw. ggf. gesetzlich bestehenden Verpflichtungen nachkommen.

Die Sektoruntersuchung hat ergeben, dass im Zusammenhang mit dem Herunterladen und der Anwendung von Apps mitunter starke Transparenzmängel bestehen. So werden Verbraucher bereits nicht angemessen darüber informiert, mit wem sie beim Herunterladen einer App eigentlich einen Vertrag schließen. Die Verbraucherbefragung hat diesbezüglich ebenso wie die Analyse der Nutzungsbedingungen und App-Präsentation in den App-Stores kein eindeutiges Ergebnis geliefert. Dementsprechend klärungsbedürftig ist auch, ob nun der jeweilige App-Store-Betreiber oder App-Publisher Ansprechpartner für Gewährleistungsansprüche ist.

Verbraucher werden auch nicht hinreichend darüber aufgeklärt, wer bei der Nutzung von Apps personenbezogene Daten erhält und um welche personenbezogenen Daten es sich dabei überhaupt handelt. Weder die Beschreibungen von Apps in den App-Stores noch die Datenschutzerklärungen der App-Publisher geben hierüber hinreichend Aufschluss.

Dem in der Befragung zum Ausdruck kommenden Wunsch der Verbraucher nach mehr Kontrolle über die Verarbeitung ihrer personenbezogenen Daten wird auf Ebene der Betriebssystem-Einstellungen von *iOS* bzw. *Android* allenfalls ansatzweise entsprochen. Trotz mancher Innovationen im Datenschutzbereich (zuletzt z. B. *Apples* in diesem Jahr eingeführtes „App Tracking Transparency Framework“)[5] bleibt hier noch viel Raum für Verbesserungen. Verbraucher sind momentan noch weit entfernt von einer effektiven Kontrolle der Verarbeitungen ihrer personenbezogenen Daten, die durch Apps ausgelöst werden.

Um diesem Missstand zu begegnen, schlägt das Bundeskartellamt eine Reihe von Maßnahmen vor. So sollten zunächst die App-bezogenen Verbraucherinformationen grundlegend überarbeitet werden. Nutzer sollten über eine verbesserte Suchfunktion gezielter nach verbraucherfreundlichen Apps (z. B. Apps ohne Third-Party-Tracking) suchen können. Wesentliche Datenschutzaspekte (z. B. Verarbeitung besonders sensibler Daten, datenempfangende Unternehmen, datenschutzkritische Berechtigungen) sollten Verbraucher auf einen Blick erfassen können, ohne die ausführlichen Datenschutzklärungen der App-Publisher überhaupt lesen zu müssen. Auch muss

---

5 Das Bundeskartellamt beschäftigt sich in dieser Sektoruntersuchung nicht mit den möglichen kartellrechtlichen Auswirkungen geänderter Datentrackingbestimmungen auf das Verhältnis der führenden App-Store-Anbieter zu denjenigen App-Entwicklern, deren Geschäftsmodell (auch) im Angebot werbefinanzierter Apps liegt.

zweifelsfrei erkennbar sein, wer Anbieter einer App ist; sämtliche Nutzungs- und Gewährleistungsregeln wären dementsprechend anzupassen. Die ausführlichen Datenschutzerklärungen müssten ihrerseits so gefasst werden, dass ihnen ohne Weiteres mit hinreichender Konkretheit zu entnehmen ist, welche Daten wie und von wem verarbeitet werden. Soweit App-Stores zu Datenschutzniveau und Darstellung von Datenverarbeitungen verbindliche Vorgaben machen, sollten diese für Apps der App-Store-Betreiber ebenso gelten wie für die Apps Dritter.

Mindestens ebenso wichtig wie eine Verbraucherinformation über Apps wären effektive und einfach handhabbare Kontrollmöglichkeiten über Datenabflüsse. So könnten Nutzer über ein Datenschutz-Cockpit sämtliche datenschutzrelevanten App-Berechtigungen, insbesondere den Zugriff auf eindeutige Identifikatoren, steuern und diese ggf. auch kollektiv entziehen. Auch der Zugriff durch andere Akteure als den App-Publisher selbst sollte grundsätzlich vollständig abgestellt werden können. Soweit das Funktionieren des Betriebssystems hierdurch nicht gefährdet wird, sollten Nutzer zudem in der Lage sein, jede App zu deinstallieren oder Apps einzelne Berechtigungen zu entziehen.

Davon ausgehend, dass es sich zumindest bei manchen Datenverarbeitungen und unterlassenen Verbraucherinformationen um Rechtsverletzungen handelt, wäre schließlich auch eine verstärkte Rechtsdurchsetzung hilfreich.

TIPPS FÜR VERBRAUCHER FÜR DEN UMGANG MIT APPS:

- Informieren Sie sich vor dem Download einer App über datensparsame Alternativen (z. B. auf Seiten wie https://appcheck.mobilsicher.de/ oder https://exodus-privacy.eu.org).

- Prüfen Sie vorinstallierte Apps besonders kritisch. Brauchen Sie die betreffende App nicht, deinstallieren oder deaktivieren Sie diese. Wollen Sie die App nutzen, schauen Sie sich an, welche Zugriffsberechtigungen die App auf Gerätefunktionen hat.

- Verweigern Sie Apps nicht benötigte Berechtigungen oder entziehen Sie diese nachträglich. Falls Sie sich nicht sicher sind, ob die Berechtigung benötigt wird, können Sie diese zunächst verweigern/entziehen und im Bedarfsfall ggf. später wieder aktivieren.

- Werden Sie bei der Nutzung von Apps nach Zustimmungen gefragt, klicken Sie nicht bedenkenlos auf „Annehmen“/“Akzeptieren“ o. Ä. Lesen Sie sich genau durch, wofür Ihre Zustimmung erfragt wird und lehnen Sie im Zweifel (erst einmal) ab.

- Prüfen Sie, ob Sie eine Anwendung überhaupt als App benötigen. Nutzen Sie im Zweifelsfall lieber einen Browser mit der Möglichkeit strenger Datenschutzeinstellungen. In der Regel können Sie Links zu den Webseiten, die Sie häufig nutzen, gleich auf dem Startbildschirm ablegen.

- Stellen Sie Ihre Browser-App datenschutzfreundlich ein, achten Sie dabei insbesondere auf die Auswahl einer datenschutzfreundlichen Standardsuchmaschine (z. B. *Startpage*, den Testsieger der *Stiftung Warentest*[6]).

[6] *Stiftung Warentest*, Suchen ohne durchsucht zu werden, test 4/2019, S. 30 ff., abrufbar unter https://www.test.de/Suchmaschinen-im-Test-Eine-schlaegt-Google-5453360-5453366/.

- Falls möglich, geben Sie Apps den Vorzug, die Sie komplett offline nutzen können. Baut die App keine Datenverbindung über das Internet auf, gibt sie auch keine personenbezogenen Daten weiter.

- Vermeiden Sie es, in Apps eindeutige Identifikatoren wie z. B. Telefonnummer, Geburtsdatum oder Ihren vollen Vor- und Nachnamen anzugeben. Vermeiden Sie nach Möglichkeit Registrierungen, die solche Identifikatoren einfordern.

- Quelloffene Apps sind häufig datenschutzfreundlicher und können – außer bei Spielen – eine geeignete Alternative auch zu häufig genutzten Standard-Apps darstellen; Empfehlungen finden Sie im Internet[7]. Der Android-App-Store F-Droid (https://f-droid.org/) ist auf entsprechende Angebote spezialisiert.

- Prüfen Sie Apps nach dem Download sofort auf deren Funktionsfähigkeit und Datensendeverhalten und geben Sie diese ggf. umgehend zurück; auf diese Weise erhalten Sie jedenfalls beim Download aus den App-Stores von *Google* bzw. *Apple* Ihren Kaufpreis ohne größeren Aufwand zurück.

- Funktionieren Apps aus den App-Stores von *Google* bzw. *Apple* nicht korrekt, versuchen Sie auch nach Ablauf der von *Google*/*Apple* offiziell vorgesehenen Stornofrist eine Rückgabe über Ihr *Google*-/*Apple*-Konto. Zumindest während der Gewährleistungsfrist sollte dies häufig funktionieren.

[7] S. etwa *Wikipedia*, List of free and open iOS applications, abrufbar unter https://en.m.wikipedia.org/wiki/List_of_free_and_open-source_iOS_applications, oder Kuketz-Blog-Empfehlungsecke für Android-Apps, abrufbar unter https://www.kuketz-blog.de/empfehlungsecke/#Android.

B. Einleitung

Smartphones und Tablets sind aus dem Alltag vieler Menschen nicht mehr wegzudenken. So besaßen im Jahr 2020 bereits 86 Prozent der Bundesbürger ab 14 Jahren ein Smartphone[8], in der Gruppe der 14- bis 49-Jährigen sogar praktisch jeder.[9] Auch Tablets erfreuen sich immer größerer Beliebtheit in Deutschland. Im Jahr 2019 nutzten 57 Prozent der Einwohner ab 16 Jahren ein Tablet.[10] Bei den Kindern im Alter von sechs bis neun Jahren lag die Anzahl der Tablet-Nutzer sogar bei 79 Prozent.[11] Die Corona-Pandemie mit Home-Office und Home-Schooling dürfte dazu geführt haben, dass die betreffenden Zahlen noch weiter angestiegen sind.

Ein entscheidender Faktor der Erfolgsgeschichte von Smartphones und Tablets ist die Vielzahl und Vielgestaltigkeit hierfür erhältlicher Software-Applikationen oder kurz „Apps“. Die über Apps nutzbaren Dienste decken die unterschiedlichsten Lebensbereiche und -situationen ab. Die massenhafte Verwendung von Apps wirft indessen auch Fragen auf. So werden die meisten Apps gratis angeboten; eine Monetarisierung erfolgt (ggf. neben In-App-Käufen) häufig über das Schalten von Werbung in den Apps und/oder das Erheben und ggf. Weiterveräußern von Nutzungsdaten. Es ist zweifelhaft, ob Verbraucher diese Datenflüsse hinreichend überblicken bzw. kontrollieren können. Auch im Hinblick auf vorinstallierte Apps, die Vorab-Informationen vor einem Download, die App-Suche oder Rückabwicklungsmöglichkeiten nach dem App-Erwerb erscheint vieles ungeklärt.

Das Bundeskartellamt hat daher im Oktober 2020 eine Sektoruntersuchung „Mobile Apps“ eingeleitet. Streng genommen bezieht sich das Attribut „mobil“ natürlich nicht auf die Apps selbst (die im Grunde genommen immer „mobil“ sind), sondern auf die Endgeräte, auf denen die Apps installiert und genutzt werden. Der Begriff „mobile Apps“ für Apps, die für Smartphones und Tablets

---

8 S. *VuMA Arbeitsgemeinschaft*, Touchpoints, abrufbar unter https://touchpoints.vuma.de/#/trend/, auf der Seite müssen diverse Einstellungen vorgenommen werden, um die statistischen Ergebnisse zu erhalten; eine zusammenfassende grafische Darstellung findet sich hier: *Statista*, Anteil der Smartphone-Nutzer in Deutschland in den Jahren 2012 bis 2020, abrufbar unter https://de.statista.com/statistik/daten/studie/585883/umfrage/anteil-der-smartphone-nutzer-in-deutschland/. **Soweit nicht anderweitig angegeben, ist der Stand sämtlicher Internetquellen der 22.07.2021**.

9 Ebenda (Fn. 8).

10 S. *Bitkom*, 6 von 10 Bundesbürgern nutzen einen Tablet-Computer (Pressemeldung vom 21.01.2020), abrufbar unter https://www.bitkom.org/Presse/Presseinformation/6-10-Bundesbuergern-nutzen-Tablet-Computer. Im Gegensatz zu Smartphones werden Tablets sehr viel häufiger von mehreren Personen benutzt, so dass Statistiken in der Regel nicht auf den Besitz des Geräts, sondern auf dessen Nutzung abstellen.

11 Ebenda (Fn. 10).

konzipiert sind, hat sich indessen im allgemeinen Sprachgebrauch etabliert und wird auch in diesem Bericht entsprechend verwendet.

Mit der vorliegenden Sektoruntersuchung möchte das Bundeskartellamt mögliche verbraucherrechtliche Verstöße im Bereich Datenschutz-, Lauterkeits-, Gewährleistungs- und AGB-Recht eingehender untersuchen und auf eventuelle Rechtsverletzungen aufmerksam machen. Darüber hinaus veröffentlicht das Bundeskartellamt Empfehlungen für Verbraucher und Entscheidungsträger.

I. Branche

Einhergehend mit dem eingangs beschriebenen Smartphone-Boom hat auch die App-Branche in den letzten Jahren stark an Bedeutung gewonnen.

Statistische Angaben zu Apps klaffen mitunter zwar weit auseinander. Dennoch lässt sich ungeachtet der statistischen Quelle bei Downloadzahlen wie Umsätzen ein ungebrochener klarer Aufwärtstrend feststellen. So geht etwa der App-Analysespezialist *App Annie* von rund 175 Mrd. App-Downloads weltweit im Jahr 2017 und 218 Mrd. im Jahr 2020 aus.[12] Für denselben Zeitraum verzeichnet der Branchenverband Bitkom für Deutschland einen Anstieg von 1,8 Mrd.[13] auf 2,75 Mrd. App-Downloads[14] in den beiden größten App-Stores *Google Play* und *Apple App Store*. Dabei entfielen gut 70 Prozent der Downloads auf den *Google Play* Store, knapp 30 Prozent auf den App Store von *Apple*.[15] Die beiden genannten App-Stores boten im ersten Quartal 2021 auch die größte Anzahl an Apps an (*Google Play*: rund 3,5 Mio. Apps, *Apple App Store*: rund 2,2 Mio. Apps). Im App-Store von *Amazon* waren hingegen weniger als eine halbe Million Apps verfügbar.[16]

---

12 S. *App Annie*, Jahresrückblick 2017, S. 3 bzw. *App Annie*, The State of Mobile 2021, S. 2. Die Zahlen erscheinen indessen eher hoch gegriffen; selbst unter Einbeziehung von Zweit-Smartphones und Tablets dürfte man weltweit maximal auf 5 Mrd. Geräte kommen, was unabhängig von der Altersgruppe je Gerät eine App-Downloadzahl von rund 44 pro Jahr ergäbe.

13 S. *Bitkom*, Deutscher App-Markt knackt 1,5-Milliarden-Marke (Pressemitteilung vom 29.01.2018), abrufbar unter https://www.bitkom.org/Presse/Presseinformation/Deutscher-App-Markt-knackt-15-Milliarden-Marke.html.

14 S. *Bitkom*, App-Boom setzt sich fort (Pressemitteilung vom 31.08.2020), abrufbar unter https://www.bitkom.org/Presse/Presseinformation/App-Boom-setzt-sich-fort.

15 Ebenda (Fn. 14).

16 S. *Statista*, Number of apps available in leading app stores as of 1st quarter 2021 (Statistik beruhend auf Angaben von AppFigures), abrufbar unter https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/.

Obwohl der Download der meisten Apps kostenlos ist, wurden nach Schätzungen des Branchenverbands *Bitkom* im Jahr 2019 in Deutschland 1,61 Mrd. Euro mit mobilen Apps umgesetzt, 2020 bereits 1,99 Mrd Euro.[17] Mehr als drei Viertel der App-Umsätze gehen demnach auf sogenannte In-App-Käufe, 20 Prozent auf Werbung und nur 2 Prozent auf den Erwerb kostenpflichtiger Apps zurück.[18]

Bei der Wahl eines App Stores sind iPhone-Nutzer eingeschränkter als solche, die ein *Android*-Gerät verwenden. *iPhone*-Nutzer können ausschließlich Apps aus dem *Apple App Store* herunterladen. Demgegenüber haben *Android*-Nutzer neben *Google Play* die Möglichkeit, Apps direkt vom App-Anwender (als sog. *Android Package Kit*, APK), oder über App-Stores von anderen Anbietern wie den *Aurora*-Store oder *F-Droid* (nur Gratis-Apps, die überwiegend auf freier und offener Software basieren) zu erhalten. Zudem bieten einige Smartphone-Hersteller ihre eigenen App-Stores an, wie beispielsweise der *Galaxy Store* für *Samsung Galaxy*-Geräte oder die *Huawei AppGallery* für *Huawei*-Geräte. In der Praxis werden diese Optionen in Deutschland aber selten genutzt und dürften gegenüber den App-Downloads über *Google Play* praktisch nicht ins Gewicht fallen.

II. Hinweise auf Verbraucherschutzdefizite

Voraussetzung für eine verbraucherrechtliche Sektoruntersuchung nach § 32e Abs. 5 GWB ist der begründete Verdacht auf erhebliche, dauerhafte oder wiederholte Verstöße gegen verbraucherrechtliche Vorschriften, die nach ihrer Art oder ihrem Umfang die Interessen einer Vielzahl von Verbraucherinnen und Verbrauchern beeinträchtigen.

Für entsprechende Probleme gab es in der Vergangenheit zahlreiche Anhaltspunkte in diversen Medien, Gerichtsverfahren und Studien. So erklärte bereits im Jahr 2013 das Landgericht Frankfurt am Main mehrere Klauseln in den Allgemeinen Geschäftsbedingungen eines App-Stores für unwirksam.[19] In dem Urteil wurde u. a. kritisiert, dass Verbraucher nicht deutlich darauf hingewiesen wurden, dass der App-Hersteller Nutzerdaten erfasst und über den App-Store darauf speziell

17 S. *Bitkom*, App-Boom setzt sich fort (Fn. 14).

18 S. *Bitkom*, App-Boom setzt sich fort (Fn. 14).

19 S. LG Frankfurt, Urteil vom 06.06.2013 – 2-24 O 246/12, juris.

zugeschnittene Werbung einsetzen kann.[20] Auch die Verbraucherzentralen haben bereits mehrfach auf Unzulänglichkeiten hingewiesen und beispielsweise Datenschutzmängel und die Risiken der umfangreichen Zugriffsberechtigungen der Apps kritisiert.[21]

Bereits 2014 untersuchte der *Verbraucherzentrale Bundesverband (vzbv)* vereinzelt Apps in Bezug auf Zugriffsberechtigungen, Kontaktmöglichkeiten der App-Anbieter, Verbraucherinformationen, In-App-Käufe und Lockangebote. Im Rahmen dieser Untersuchung wurden diverse aus Verbrauchersicht bestehende Mankos aufgedeckt, etwa schwierige Kontaktaufnahme zu den App-Anbietern oder nicht erforderliche Zugriffsberechtigungen von Apps, die Nutzer nicht deaktivieren konnten. Ladungsfähige Anschriften der App-Anbieter, die für die Verfolgung und Durchsetzung rechtlicher Ansprüche notwendig sind, waren nur durch mühseliges Suchen in den Allgemeinen Geschäftsbedingungen und Datenschutzbestimmungen, die teilweise englischsprachig waren, aufzufinden.[22]

2017 warnte die *Verbraucherzentrale Nordrhein-Westfalen* vor Datenschutzmängeln bei Wearables und Fitness-Apps. Dabei fiel bei einer Untersuchung des Marktwächter-Teams vor allem auf, dass dem datenschutz- und verbraucherrechtskonformen Umgang mit den äußerst sensiblen Gesundheitsdaten, beispielsweise aufgrund fehlender Information der Nutzer, nicht genügend Rechnung getragen wurde. Auch stellten zwei Anbieter die Datenschutzbestimmungen nur in englischer Sprache für die Verbraucher zur Verfügung. Im Zuge der Untersuchung wurden neun Anbieter abgemahnt, darunter auch *Apple*.[23]

Die *Stiftung Warentest* stieß im Rahmen eines Tests von Banking-Apps auf Mängel bei Allgemeinen Geschäftsbedingungen und Datenschutzerklärungen. Parallel zu den Feststellungen bei den

---

20 S. LG Frankfurt, Urteil vom 06.06.2013 – 2-24 O 246/12, juris Rn. 64.

21 Siehe z. B. *Verbraucherzentrale Nordrhein-Westfalen e.V.*, Supermarkt-Apps: Rabatte und Risiken (Pressemitteilung vom 18.01.2019), abrufbar unter https://www.verbraucherzentrale.nrw/wissen/digitale-welt/mobilfunk-und-festnetz/supermarktapps-rabatte-und-risiken-33057 und nachstehende Beispiele.

22 S. *Verbraucherzentrale Bundesverband e.V.*, Untersuchung von Apps – Zugriffsberechtigung, Kontaktmöglichkeiten, Verbraucherinformationen und In-App-Käufe, 12.03.2014, abrufbar unter https://www.vzbv.de/sites/default/files/downloads/Apps-Untersuchungsbericht_vzbv_Surferprojekt-2014-03-12.pdf.

23 S. *Verbraucherzentrale Nordrhein-Westfalen e.V.*, Unsportlich: Datenschutz-Mängel bei Wearables und Fitness-Apps (Pressemitteilung vom 09.06.2017), abrufbar unter https://www.verbraucherzentrale.nrw/aktuelle-meldungen/digitale-welt/unsportlich-datenschutzmaengel-bei-wearables-und-fitnessapps-13659. Zu ähnlichen Ergebnisse gelangt auch eine aktuellere Studie des vzbv zu Wearables und Fitness-Apps, 12.11.2020, abrufbar unter https://www.verbraucherzentrale.de/marktbeobachtung/wearables-und-fitnessapps-40296.

Fitness-Apps und Wearables fielen Banking-Apps auf, deren Datenschutzerklärungen ebenfalls nur auf Englisch verfügbar waren. Darüber hinaus wurde bei acht *Android*- und elf *Apple*-Apps ein „kritisches Datensendeverhalten“ festgestellt. In diesen Fällen wurden etwa Informationen über den Mobilfunkanbieter oder den Gerätetyp des Smartphones an den App-Anbieter verschickt.[24]

Seit Jahren steht zudem *Facebook* in der Kritik, in großem Umfang personenbezogene Daten von Smartphone-Nutzern zu erhalten und dies auch dann, wenn der jeweilige Nutzer über gar kein *Facebook*-Konto verfügt. Die Daten werden an *Facebook* durch das *Facebook Software Development Kit* (SDK), das App-Entwickler in ihre Apps einbauen, übertragen. Die Organisation *Privacy International* stellte 2018 in einer Untersuchung fest, dass mindestens 61 Prozent der untersuchten Apps bereits beim Öffnen der App Daten an *Facebook* schickten. Teils wurden auch sensible Daten direkt an *Facebook* übermittelt, wie das Beispiel der Reise-App *Kayak* zeigte. Alle Angaben, die der Nutzer im Rahmen einer Suchanfrage angab, wurden mit *Facebook* geteilt, einschließlich durchaus als sensibel zu bewertenden Informationen wie die Ticketklasse und die mitfliegenden Kinder.[25] Aufgrund der im Mai 2019 in Kraft getretenen EU-Datenschutzgrundverordnung[26] (DSGVO) wurde laut *Privacy International* zwar bei den meisten Apps insoweit nachgebessert, als personenbezogene Daten erst an *Facebook* versendet werden, wenn der Nutzer dem zugestimmt hat.[27] Allerdings besteht weiterhin der Verdacht, dass Verbraucher nicht ausreichend über Third-Party-Tracker wie *Facebook* unterrichtet werden, wie eine Studie des norwegischen Verbraucherschutzverbands *Forbrukerrådet* zeigt.[28] Im Rahmen dieser Studie wurde bei

---

24 S. *Stiftung Warentest*, Banking-Apps im Test – 38 Apps fürs Banking mit dem Handy (18.05.2020), abrufbar unter https://www.test.de/Banking-Apps-Die-besten-Apps-fuers-Smartphone-Banking-4849502-0/.

25 S. *Privacy International*, How Apps on *Android* Share Data with Facebook – Report (29.12.2019), abrufbar unter https://privacyinternational.org/report/2647/how-apps-*Android*-share-data-facebook-report; zum Teil hier auf Deutsch zusammengefasst: *Kleinz*, Kein Entkommen – *Android*-Apps schicken Nutzerdaten ungefragt an Facebook (c’t 3/2019, S. 18), abrufbar unter https://www.heise.de/select/ct/2019/3/1549009783045427.

26 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. EU L 119 vom 04.05.2016, S. 1.

27 S. *Privacy International*, Guess what? Facebook still tracks you on *Android* apps (even if you don’t have a Facebook account) (05.03.2020, aktualisiert am 07.10.2020), abrufbar unter https://privacyinternational.org/blog/2758/appdata-update.

28 S. *Forbrukerrådet*, Out of control – how consumers are exploited by the online advertising industry (14.01.2020), abrufbar unter https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf.

zehn untersuchten Apps festgestellt, dass Nutzerdaten an mindestens 135 verschiedene Dritte weitergegeben wurden, worüber die Nutzer meist nicht oder nicht ausreichend informiert wurden.[29] Zieht man die App-Tracker-Statistik von *Exodus Privacy* für mehr als 100.000 untersuchte *Android*-Apps heran, so wird deutlich, dass *Google* ebenfalls in großem Umfang App-Daten erhält, so dass sich hier das Problem in ähnlicher Weise stellen könnte wie bei *Facebook*.[30]

Auch die *New York Times* wies auf die Gefahren der ständigen Überwachung durch Apps hin und demonstrierte, wie einfach es ist, mit den durch Apps erlangten GPS-Informationen weitere Informationen über den App-Nutzer, beispielsweise über seine Tagesabläufe, seine Wohnadresse, Treffen mit anderen Menschen etc., zu erhalten.[31] Die von der *New York Times* durchgeführte Untersuchung einer Datenbank ergab, dass durch die von Apps generierten Daten nahezu metergenaue Bewegungsprofile erstellt werden konnten und diese Daten in manchen Fällen sogar mehr als 14.000 Mal am Tag aktualisiert wurden.[32]

Im August 2019 machte der *vzbv* auf das im Internet häufig diskutierte und kritisierte[33] Phänomen der vorinstallierten Apps auf Smartphones aufmerksam. Diese werden von den Nutzern häufig nicht verwendet, sind aber trotzdem nicht löschbar. Die Mehrheit der befragten Verbraucher gab an, selbst bestimmen zu wollen, welche Apps auf ihrem Smartphone installiert sind.[34]

---

29 Ebenda (Fn. 28), S. 5, 177 ff.

30 Abrufbar unter https://reports.exodus-privacy.eu.org/de/trackers/stats/.

31 S. *Valentino-DeVries/Singer/ Keller/Krolik*, Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret, The New York Times (10.12.2018), abrufbar unter https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

32 Ebenda (Fn. 31).

33 S. etwa *Fischer*, Seit Jahren frustrierend: Zu viele *Android*-Smartphones haben Apps doppelt vorinstalliert und lassen sie nicht löschen (smartdroid.de, 25.09.2020), abrufbar unter https://www.smartdroid.de/seit-jahren-frustrierend-zu-viele-*Android*-smartphones-haben-apps-doppelt-vorinstalliert-und-lassen-sie-nicht-loeschen/.

34 S. *Verbraucherzentrale Bundesverband e.V.*, Vorinstallierte Apps auf Smartphones: Kaum genutzt und schwer loszuwerden (Pressemitteilung vom 27.08.2019), abrufbar unter https://www.vzbv.de/pressemitteilungen/vorinstallierte-apps-auf-smartphones-kaum-genutzt-und-schwer-loszuwerden, s. dazu auch Abbildung 15 auf S. 31.

Darüber hinaus zeigte der im Januar 2019 vom Bundesministerium der Justiz und für Verbraucherschutz (BMJV) veröffentlichte Abschlussbericht zu der Untersuchung „Verbraucherinformationen bei Apps – Empirie“[35] erhebliche daten- und verbraucherschutzrechtliche Mängel bei den meisten der 200 getesteten Apps auf. Die Untersuchung ergab unter anderem, dass die Datenschutzerklärungen der getesteten Apps auch nach Inkrafttreten der DSGVO noch erheblich verbesserungsbedürftig waren, insbesondere fehlten „konkrete Erklärungen zur genauen Umsetzung der Datenverarbeitung und den möglichen Folgen für die Nutzer“[36].

Auch während der vorliegenden Sektoruntersuchung ergaben sich weitere Hinweise auf mögliche Verbraucherrechtsverstöße. So veröffentlichte das Verbraucherschutzportal *mobilsicher.de* im März 2021 eine Untersuchung, der zufolge sieben von 20 getesteten E-Mail-Apps den Inhalt von E-Mails auslasen und an Dritte weitergaben, worüber die Nutzer nicht informiert wurden.[37] Ebenfalls im März 2021 warnte der Blogger Mike Kuketz vor den datenschutzrechtlichen Problemen durch die Verwendung von Trackern in Apps, insbesondere aufgrund der Möglichkeit, einen Personenbezug zu Identifikatoren (wie *Google Advertising ID*) herzustellen.[38]

In Anbetracht der oben dargestellten weiten Verbreitung mobiler Endgeräte und hohen Downloadzahlen liegt auf der Hand, dass die genannten Probleme im Zusammenhang mit Apps in der Regel eine große Zahl an Verbrauchern betreffen. Verbraucherrechtsverstöße in diesem Bereich haben mithin eine extrem hohe Reichweite. Darüber hinaus können bei der Benutzung einer App hochsensible personenbezogene Daten an Dritte weitergegeben werden. Das Recht auf informationelle Selbstbestimmung kann hierdurch schwerwiegend und nachhaltig verletzt werden.

---

35 *Projektträger Bundesanstalt für Landwirtschaft und Ernährung (ptble) für das Bundesministerium der Justiz und für Verbraucherschutz*, Abschlussbericht, Verbraucherinformationen bei Apps – Empirie (22.10.2018), abrufbar unter https://www.bmjv.de/SharedDocs/Downloads/DE/Service/StudienUntersuchungenFachbuecher/Verbraucherin-fos_Apps.pdf;jsessionid=8349799B9F553F7A9ADEA6F7C1E9ED5C.1_cid324?__blob=publicationFile&v=1.

36 S. Fn. 35, S. 102.

37 S. *Mobilsicher*, Apps gecheckt: Vorsicht, diese 7 Mail-Apps lesen Ihre E-Mails mit (*Android*) (13.03.2021, aktualisiert am 17.03.2021), abrufbar unter https://mobilsicher.de/ratgeber/apps-gecheckt-diese-7-e-mail-apps-lesen-mit.

38 S. *Kuketz*, Wie Tracking in Apps die Sicherheit und den Datenschutz unnötig gefährdet (03.03.2021), abrufbar unter https://www.kuketz-blog.de/wie-tracking-in-apps-die-sicherheit-und-den-datenschutz-unnoetig-gefaehrdet/.

III. Untersuchungsgegenstand

Apps für mobile Endgeräte waren schon des Öfteren Gegenstand wissenschaftlichen oder auch aufsichtsbehördlichen Interesses. Sehr häufig geht es bei entsprechenden Untersuchungen um die Rolle des App-Stores gegenüber App-Publishern, Zugangsvoraussetzungen zum App-Store, Vorgaben für die App-Programmierung, Preisdiskriminierungen oder die Angemessenheit der Beteiligung der App-Store-Betreiber an den Erlösen, die durch Apps erzielt werden. Mitunter wird auch das Betriebssystem als solches, welches ggf. mit manchen Apps eng verzahnt ist, unter die Lupe genommen.

Im vorliegenden Bericht hingegen soll die Perspektive des Verbrauchers eingenommen werden und wie dieser mit mobilen Apps in Berührung kommt. Dies geschieht zunächst bei der Erstinbetriebnahme eines Smartphones oder Tablets und dem Download weiterer Apps. Dabei sind Besitzer von *Apple*-Geräten auf *Apples* App-Store beschränkt, Alternativen stehen ihnen nicht zur Verfügung. Bei *Android*-Geräten kommt auch eine Installation aus Quellen außerhalb des von *Google* angebotenen App-Stores *Google Play* zwar grundsätzlich infrage. Die Praxis zeigt jedoch, dass alternative App-Stores den Nutzern weitestgehend unbekannt sind und Downloads nahezu ausschließlich über *Google Play* erfolgen.[39] Geräte mit anderen Betriebssystemen als *Apple iOS* oder *Google Android* haben in der Praxis keine nennenswerte Bedeutung.[40] Der vorliegende Bericht konzentriert sich daher im Wesentlichen auf die beiden App-Stores von *Google* bzw. *Apple*. Dabei wird im Schwerpunkt untersucht, ob der Verbraucher alle für seine Download-Entscheidung nötigen Informationen erhält und inwieweit er Datenverarbeitungen effektiv kontrollieren oder auch nur hinreichend überblicken kann. Daneben werden auch verbrauchervertragsrechtliche Fragen erörtert.

Das Ermittlungsinstrumentarium unterscheidet sich bei dieser Sektoruntersuchung von demjenigen, welches normalerweise zum Einsatz kommt. So wurde insbesondere von einer Unternehmensbefragung abgesehen und mittels einer Verbraucherbefragung der Fokus auf die Abnehmerseite und deren Wünsche und Vorstellungen gerichtet. Die Untersuchung stützt sich des Weiteren auf eine App-Analyse speziell zur Verwendung von Third-Party-Trackern und der transparenten Verbraucherinformation hierüber. Daneben wurden die Darstellung und Vermarktung von

---

39 S. dazu unten S.16.

40 Die Betriebssysteme Windows und Blackberry werden kaum noch genutzt; Amazons Fire OS kommt (mobil) nur auf den firmeneigenen Fire-Tablets zum Einsatz, mobile Geräte mit Huaweis Betriebssystem HarmonyOS befinden sich noch in der frühen Phase der Markteinführung.

Apps an mehreren *iOS*- und *Android*-Geräten unterschiedlicher Preisklassen getestet. Schließlich wurden weitere öffentlich zugänglich Informationen herangezogen, wie etwa die Nutzungs- und sonstigen Bedingungen der App Store-Anbieter.

C. Verbraucherbefragung

Im Rahmen der vorliegenden Sektoruntersuchung sollte insbesondere aufgeklärt werden, welche Erfahrungen Verbraucher beim Herunterladen und Nutzen von Apps machen. Dabei sollte punktuell beleuchtet werden, inwieweit App-Store-Betreiber bzw. App-Publisher den Wünschen der Verbraucher entgegenkommen – unabhängig davon, ob sie hierzu gesetzlich verpflichtet sind oder nicht – und inwieweit Verbraucher hier Verbesserungsbedarf sehen. Zu den zahlreichen Fragen, die sich in diesem Zusammenhang stellen, gibt es nach Kenntnis des Bundeskartellamtes keine aktuellen, Deutschland betreffenden Verbraucherbefragungen. Dabei ist die Haltung der Verbraucher nicht nur von rein wissenschaftlichem Interesse. Die Einschätzung bzw. Erwartung der Verbraucher kann etwa auch für die Prüfung Relevanz entfalten, ob die geschäftliche Handlung eines Unternehmens als unlauter im Sinne des Gesetzes gegen unlauteren Wettbewerb (UWG) einzustufen ist oder nicht. Das Bundeskartellamt hat daher entschieden, eine eigene Verbraucherbefragung durchzuführen bzw. zu beauftragen.

I. Konzeption

Themen der Verbraucherbefragung sollten nach der Vorstellung des Bundeskartellamtes insbesondere allgemeine Angaben zur Nutzung von Apps, die Möglichkeiten der Sortierung/Filterung von Suchergebnissen im App-Store, die Frage der Vertragspartner und Erstattungsmöglichkeiten beim Herunterladen einer App, die Datenzugriffsberechtigungen der Apps, die Ausgaben für Apps sowie die Einstellung der Verbraucher zu Werbung in Apps sein. Das Bundeskartellamt hat zu diesen Themen einen Fragenkatalog entwickelt, der die Grundlage für den späteren Verbraucher-Fragebogen bildete.

Um hinreichend valide Aussagen für die gesamte Online-Bevölkerung zu erhalten und gleichzeitig Unterschiede im Hinblick auf die beiden wesentlichen Nutzergruppen erkennen zu können, sollten mindestens 1.300 Interviews durchgeführt werden, davon mindestens 1.000 mit Nutzern

von *Android*-Smartphones und 300 mit Nutzern von *iPhones*.[41] Die Formulierungen und Screenshots des Fragebogens sollten bei den verschiedenen Nutzergruppen jeweils leicht angepasst sein.

Im November und Dezember 2020 forderte das Bundeskartellamt insgesamt vier Unternehmen zur Abgabe eines Angebots für die Durchführung der Verbraucherbefragung auf. Aufgrund der drei eingegangenen Angebote wurde der Auftrag im Dezember 2020 an die *Infas Institut für angewandte Sozialwissenschaft GmbH (Infas)* erteilt. Im Januar 2021 erfolgte sodann mit Infas die inhaltliche und formale Abstimmung der seitens des Bundeskartellamts entworfenen Fragen und die Finalisierung des Fragebogens.

II. Durchführung

Die Teilnehmer der Befragung stammten aus einem Online-Access-Panel und standen repräsentativ für die Online-Bevölkerung in Deutschland hinsichtlich der Merkmale Alter, Geschlecht, sozialer Status, Einkommen und Wohnort. Die Befragung erfolgte ausschließlich online, d. h. die Teilnehmer füllten den digitalen Fragebogen auf ihrem PC, Tablet oder Smartphone aus und sendeten ihn anschließend ab. Insgesamt umfasste der Fragebogen 39 (*iOS*) bzw. 38 (*Android*) Fragen inklusive zahlreicher offener Fragen.

Die Befragung wurde zwischen dem 8. und 11. Februar 2021 durchgeführt. Von den 1.389 vollständig erfassten Interviews entfielen 1.055 Interviews auf *Android*-Nutzer und 334 Interviews auf *iOS*-Nutzer.

Im Anschluss an die Befragung wurden die erhobenen Daten zudem nach den Merkmalen Alter, Geschlecht und Bundesland gewichtet, um die prozentuale Verteilung dieser Merkmale an die Verteilung in der Grundgesamtheit (Bevölkerung Deutschlands mit Internetzugang) herzustellen. Die erhobenen und geprüften Daten wurden dem Bundeskartellamt in Form einer Excel-Datei zur Verfügung gestellt. Die Auswertung der Daten führte das Bundeskartellamt – wie im Auftrag vorgesehen – selbst durch.

---

41 Diese Verteilung (ca. 77 Prozent zu 23 Prozent) entspricht in etwa der Verbreitung von *iPhones* und *Android*-Smartphones in Deutschland in jüngerer Vergangenheit. Die tatsächliche *iPhones*-Quote der Befragung lag dann bei 24 Prozent.

III. Grundlegende Erkenntnisse

Obwohl *Android*-Smartphone-Nutzer die Möglichkeit haben, neben dem *Google Play Store* auch andere App-Stores zu nutzen, gaben in der Befragung des Bundeskartellamts nur rund 16 Prozent der befragten Nutzer mit *Android*-Smartphones an, dass ihnen andere App-Stores überhaupt bekannt seien. Lediglich rund 1,5 Prozent hatten ihren letzten Download von einem anderen App-Store als *Google Play* oder direkt vom App-Publisher bezogen. Dies zeigt nachdrücklich die überragend wichtige Rolle von *Google Play* für die Verbreitung von *Android*-Apps und rechtfertigt die Konzentration der Verbraucherbefragung ebenso wie der Sektoruntersuchung insgesamt auf die beiden Hauptanbieter *Apple* und *Google* mit ihren jeweiligen App-Stores.

Wichtige Ergebnisse der Verbraucherbefragung waren u. a., dass 90 Prozent der Befragten den Schutz ihrer persönlichen Daten bei der Nutzung von Apps als „sehr wichtig“ oder „wichtig“ einstuften. Demensprechend würde ein Großteil der Befragten auch verbesserte Möglichkeiten zum Datenschutz bei Apps begrüßen. So gaben jeweils über 90 Prozent der Befragten an, sie fänden es eher oder sehr hilfreich,

- über eine App oder Funktion zu verfügen, mit der sie zentral die Zugriffsrechte von Apps steuern könnten;
- für das Funktionieren einer App erforderliche Zugriffsberechtigungen für Werbezwecke sperren zu können;
- für bestimmte Apps einen Internetzugriff vollständig ausschließen zu können.

Die Teilnehmer wurden aber auch danach befragt, ob sie beim Erwerb einer App zum Preis von drei Euro bereit wären, gegen einen (selbst zu beziffernden) Rabatt personenbezogene Daten preiszugeben[42]. Dies verneinten rund 62 Prozent der Befragten, während rund 38 Prozent der Befragten Bereitschaft zeigten, ihre Daten gegen einen Preisnachlass zu tauschen.

---

42 Hier wurde bewusst nicht der Ansatz des Preisaufschlags für mehr Datenschutz gewählt, sondern der Ansatz des Preisnachlasses bei bewusster Datenpreisgabe. Dies trägt zum einen dem Grundsatz datenschutzfreundlicher Voreinstellungen („privacy by default“) besser Rechnung. Zum anderen bedeutet die datenschutzfreundlichere (Standard-)Variante keinen Mehraufwand für den Nutzer durch einen andernfalls nicht notwendigen Zahlvorgang.

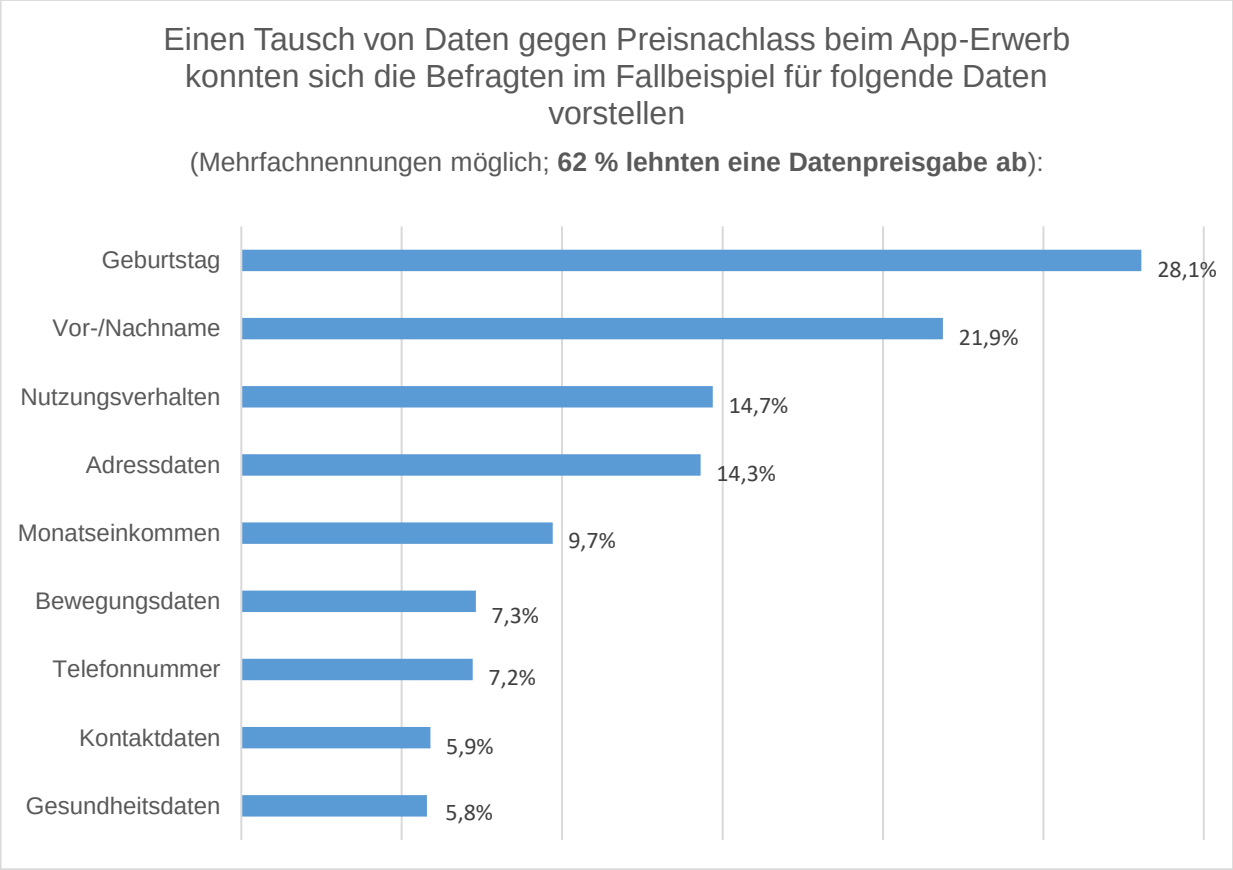


Abbildung 1: Bereitschaft zur Datenpreisgabe gegen Preisnachlass beim App-Erwerb

Vor dem Hintergrund, dass App-Publisher in der Regel mit ihren Apps auch Geld verdienen wollen, befragte das Bundeskartellamt die Teilnehmer nach ihrer Haltung zu Werbung. Hierbei zeigte sich, dass Verbraucher überwiegend Verständnis dafür haben, dass Werbung notwendig sein kann, um die Monetarisierung einer Gratis-App zu ermöglichen. Gleichzeitig zeigten sie sich jedoch skeptisch gegenüber Werbung, die auf einer Erhebung eigener personenbezogener Daten basiert:

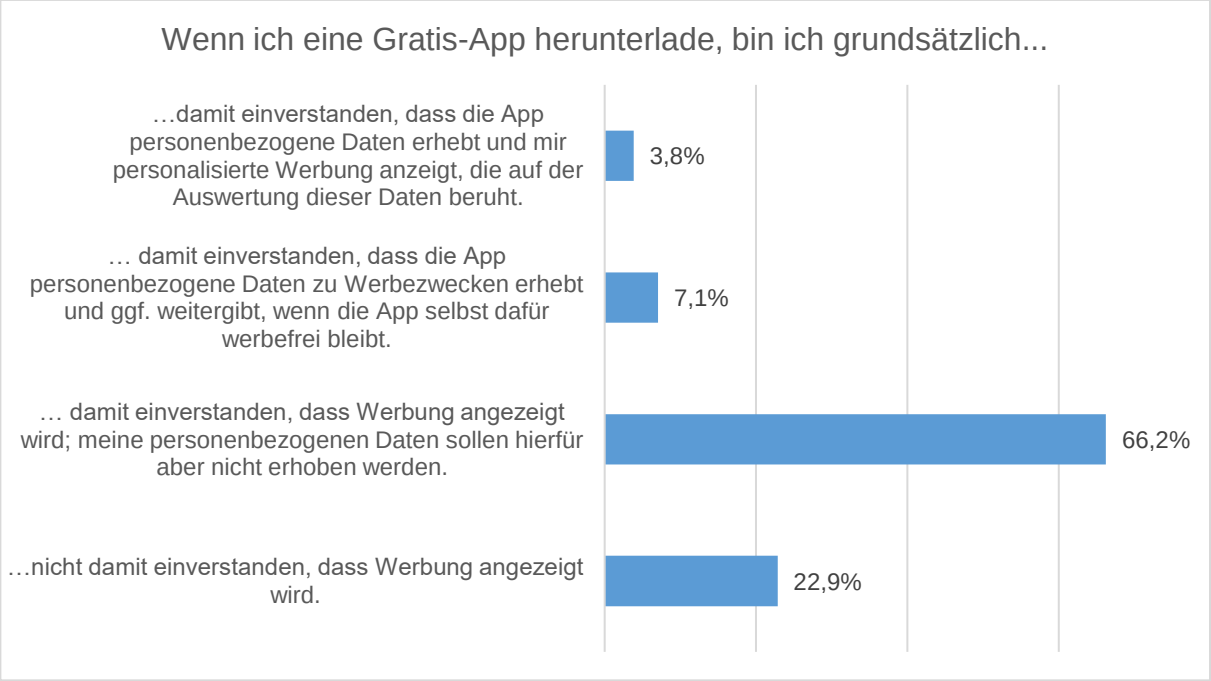


Abbildung 2: Haltung der Verbraucher zu Werbung bei Gratis-Apps

Bezahlen Verbraucher hingegen Geld für eine App, so sind sie ganz überwiegend nicht bereit, Werbung in der App zu akzeptieren:

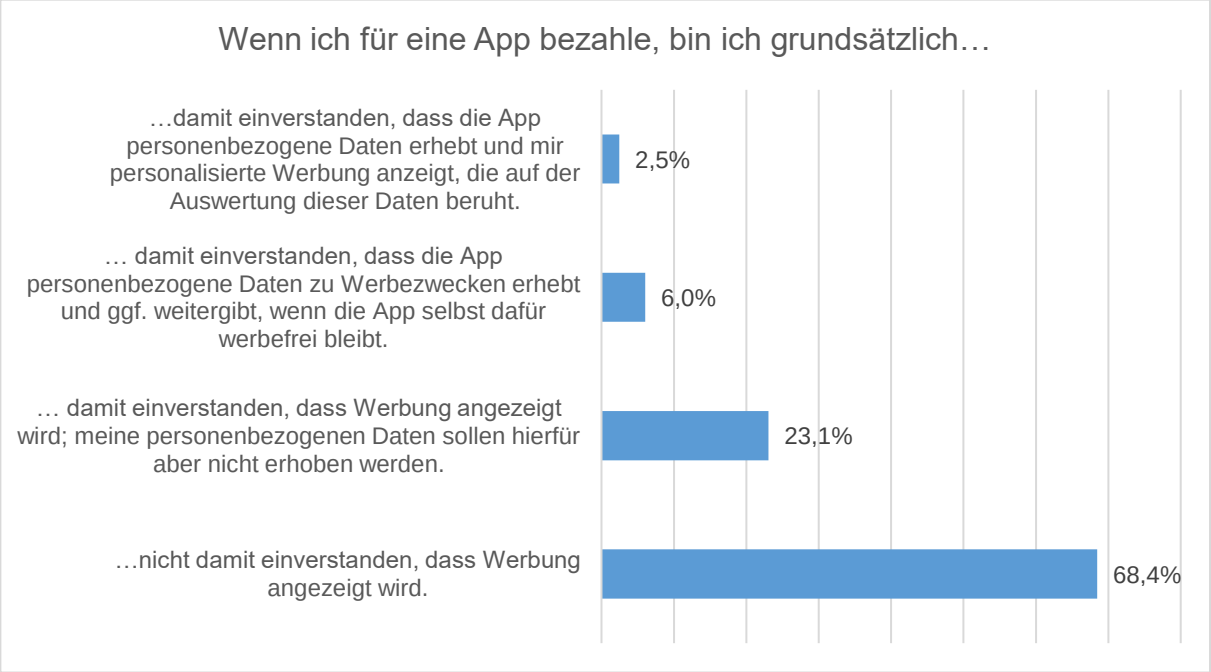


Abbildung 3: Haltung der Verbraucher zu Werbung bei Bezahl-Apps

Weitere Erkenntnisse aus der Verbraucherbefragung betreffen etwa das Ranking sowie die Sortierung und Filterung von Suchergebnissen, die Frage, wen Verbraucher beim App-Download eigentlich als Vertragspartner ansehen oder welche bislang nicht verfügbaren Informationen sie

sich wünschen. Im Einzelnen werden die Ergebnisse der Verbraucherbefragung im vorliegenden Bericht an den Stellen dargestellt und diskutiert, wo sie virulent werden.

D. Vertragsverhältnisse beim App-Download

Im Zusammenhang mit Downloads von Apps stellen sich eine Reihe komplexer rechtlicher Fragen, die bislang weder in der Literatur noch in der Rechtsprechung einer klaren Lösung zugeführt wurden. Ungeklärt ist etwa, welche Rechtsnatur der Vertrag hat, der – unabhängig vom Rahmenvertrag zur Nutzung des betreffenden App-Stores – im Zuge des Downloads[43] einer App eingegangen wird.

Anders als etwa das US-amerikanische Recht kennt das deutsche Recht keinen Lizenzvertrag. Dessen ungeachtet stellen jedoch die von *Google* bzw. *Apple* für den deutschen Markt verwendeten Allgemeinen Geschäftsbedingungen zumindest in Teilen ganz maßgeblich auf die Figur des Lizenzvertrags ab. Dies geht mitunter einher mit zweifelhaften und rechtlich nicht passgenauen Übersetzungen, die zu Verwirrung auf Verbraucherseite führen können und womöglich zu Rechtsfolgen, die von den App-Store-Betreibern selbst ursprünglich nicht beabsichtigt waren. Nach deutschem Recht können je nachdem, ob die betreffende App gratis angeboten wird, kostenpflichtig ist oder ggf. ein Abo-Modell enthält, verschiedene Vertragstypen und insbesondere auch typengemischte Verträge vorliegen.

Wesentlich häufiger als in der nicht-virtuellen Welt kann auch die Bestimmung des Vertragspartners des App-Nutzers schwierig sein. Dem Kunden, der eine App aus einem App-Store herunterlädt, stehen als mögliche Vertragspartner der App-Publisher[44] und der App-Store-Betreiber gegenüber. In der Verbraucherbefragung des Bundeskartellamts wurden den Befragten Screenshots des jeweiligen App-Stores sowie Auszüge aus den Nutzungsbedingungen von *Apple* bzw.

---

43 Streng genommen müsste man auf die Betätigung des Download- bzw. Kaufen-Buttons (und den Erhalt des entsprechenden Signals durch den anderen Vertragsteil) abstellen. Der Download selbst kann auch zu einem späteren Zeitpunkt erfolgen. So ist insbesondere denkbar, dass der Nutzer einen Download abbricht und diesen auf einen Zeitpunkt verschiebt, zu dem ihm wieder mehr Bandbreite zur Verfügung steht. Im vorliegenden Bericht ist der besseren Lesbarkeit halber jeweils vom Download die Rede.

44 In diesem Bericht wird der Begriff *App-Publisher* verwendet und meint die juristische oder natürliche Person, die eine App unter ihrem Namen (in der Regel indirekt) vertreibt. „App-Anbieter“ impliziert hingegen, dass dieser auch das Angebot zum „Verkauf“ einer App abgibt, was aber keinesfalls als gesichert gelten kann. Der Begriff des „App-Entwicklers“ ist seinerseits missverständlich, da ein Entwickler seine App auch an ein anderes Unternehmen verkaufen kann und dieses die App anschließend vermarktet.

Google angezeigt. Das Ergebnis spiegelt wider, dass für die Nutzer nicht klar ist, mit wem sie einen Vertrag abschließen, wenn sie eine App herunterladen:

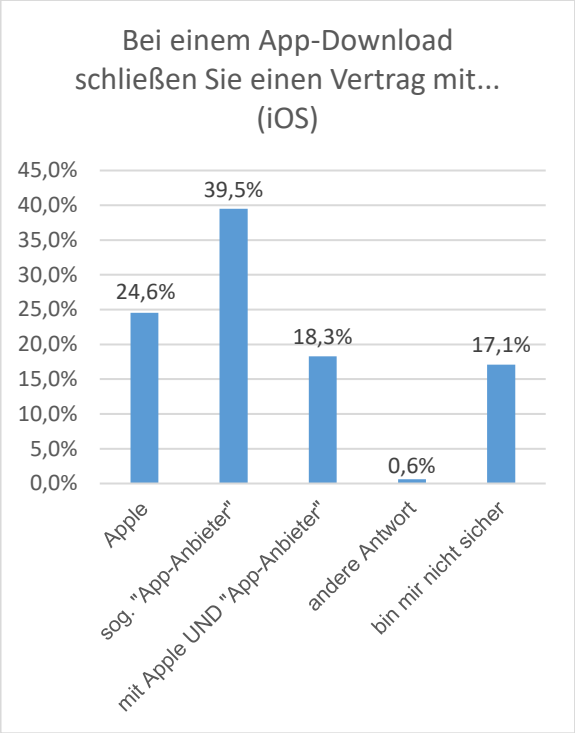


Abbildung 4: Vertragspartner aus Nutzersicht (*iOS*)[45]

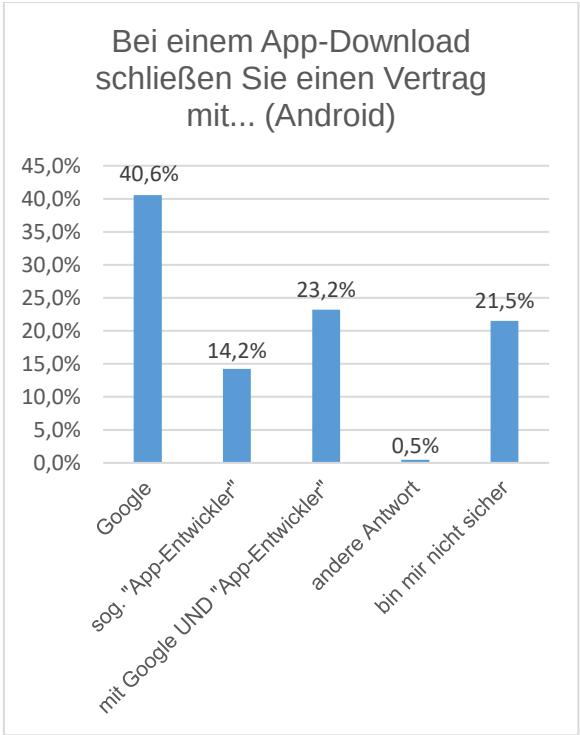


Abbildung 5: Vertragspartner aus Nutzersicht (*Android*)

Dies gibt Anlass, die Situation des Verbrauchers beim App-Download[46] genauer zu untersuchen.

I. Google Play

Zur Beurteilung der Situation beim App-Download auf *Google Play* wurden zum einen die vertraglichen Vereinbarungen zwischen *Google* und App-Publishern bzw. App-Store-Nutzern und zum anderen die Nutzeroberfläche des App-Stores untersucht.

---

45 Die Anzahl der befragten *iOS*-Nutzer ist zu gering, um eine Repräsentativität für die Gruppe aller *iOS*-Nutzer im statistischen Sinne zu gewährleisten.

46 Hier wird absichtlich nicht von einem App-Kauf gesprochen, da das Herunterladen einer App zwar durchaus einen Kauf (nach hier vertretener Auffassung jedenfalls bei dauerhaft offline nutzbaren Apps) darstellen, je nach den Umständen aber auch eine Schenkung oder ein Dauerschuldverhältnis vorliegen kann.

1. Ermittlungen

Zwar ist der Verbraucher keine Partei des vertraglichen Verhältnisses *zwischen Google und dem App-Publisher*. Dennoch können sich aus *Googles* „Vertriebsvereinbarung für Entwickler“[47] auch Anhaltspunkte für das an den App-Download anknüpfende Vertragsverhältnis ergeben. Die Vereinbarung gilt gemäß Ziff. 3.2 sowohl für entgeltliche als auch für unentgeltliche Angebote. In Ziff. 3.1 beschreibt *Google* sich selbst als „Vertreter oder Marktplatz-Dienstanbieter, um Produkte auf *Google Play* verfügbar zu machen“. Ziff. 3.4 lautet auszugsweise:

> „Während Sie als Auftraggeber fungieren, tritt *Google* als Ihr Vertreter auf und ist der Merchant of Record (Vertragspartner) für Produkte, die in den hier [Verlinkung, unter der u. a. alle Länder des EWR aufgeführt sind] beschriebenen Gebieten und Ländern verkauft oder für sie bereitgestellt werden. Sie sind der Merchant of Record (Vertragspartner) für Produkte, die Sie über *Google Play* an andere Nutzer verkaufen oder für sie bereitstellen. […]“

Auf weiteren Webseiten von *Google* finden sich hierzu Erläuterungen. So heißt es an einer Stelle:

> „Merchant of Record (Vertragspartner)
> Im Rahmen der Vertriebsvereinbarung für Entwickler ist Google der zuständige Merchant of Record (Vertragspartner) für Produkte, die Nutzern in den folgenden Ländern [hierunter alle Länder des EWR] oder Gebieten verkauft oder zur Verfügung gestellt werden. Google tritt hierbei als Ihr Vertreter auf, während Sie der Auftraggeber sind.“ [48]

Und an anderer Stelle:

> **„Kommerzielle Beziehung zwischen Ihnen und Google.** Sie setzen Google Commerce Limited als Ihren Vertreter ein, um Ihre Produkte bei Google Play für Nutzer in den folgenden Ländern [u. a. alle Länder des EWR genannt] zur Verfügung zu stellen. Da Google als Vertreter und Sie als Auftraggeber fungieren, erkennen Sie an, dass der Kauf und Verkauf Ihrer Produkte durch einen direkten Kaufvertrag zwischen Ihnen und den Nutzern geregelt wird. Eine Ausnahme besteht dann, wenn Google als Ihr Vertreter der Merchant of Record (Vertragspartner) für Produkte ist, die in den hier aufgelisteten Ländern/Gebieten [wiederum u. a. alle Länder des

---

47 *Google Play* – Vertriebsvereinbarung für Entwickler mit Wirkung zum 17. November 2020, abrufbar unter https://play.google.com/intl/ALL_de/about/developer-distribution-agreement.html.

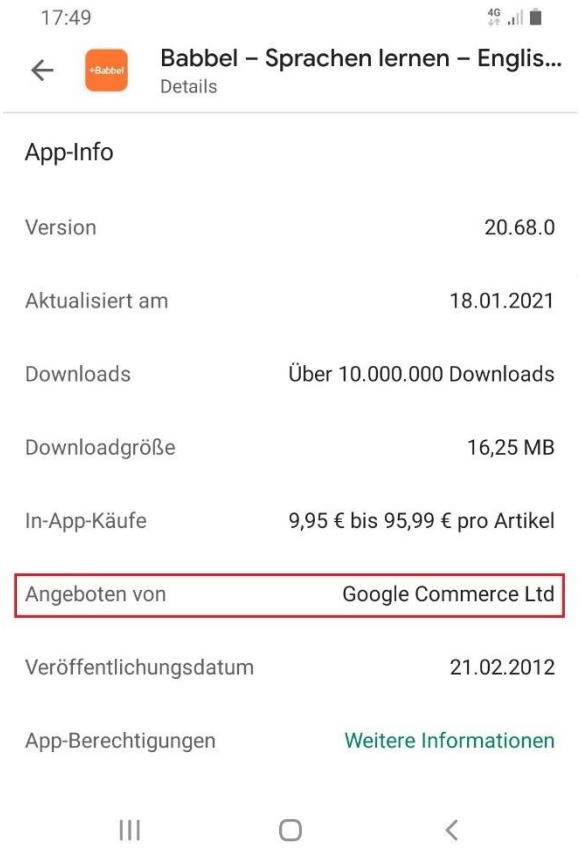
48 Siehe https://support.google.com/googleplay/Android-developer/answer/7645364?hl=de.

> EWR genannt] verkauft oder für Nutzer zur Verfügung gestellt werden. […].“[49]

Im *Verhältnis zum Endverbraucher* finden sich hingegen deutlich abweichende Formulierungen. In den *Google Play*-Nutzungsbedingungen[50] bezeichnet sich *Google* selbst als App-Anbieter:

> „3. Erwerb und Zahlung
>
> Die Inhalte bei Google Play werden von Google Commerce Limited angeboten und wenn Sie Inhalte bei oder über Google Play herunterladen, ansehen, verwenden oder erwerben, gehen Sie damit einen separaten Vertrag gemäß diesen Nutzungsbedingungen (soweit anwendbar) mit Google Commerce Limited ein.“

Auch die zentrale App-Informationsseite in *Google Play* weist *Google* als Anbieter aus:



---

49 Siehe https://support.google.com/googleplay/Android-developer/answer/10532353?hl=de.

50 *Google Play*-Nutzungsbedingungen vom 04.08.2020, abrufbar unter https://play.google.com/intl/de_de/about/play-terms/index.html.

Abbildung 6: Screenshot der Info zur „Babbel“-App im App-Store *Google Play*[51]

Daten zum App-Publisher finden sich in *Google Play* im Abschnitt „Kontaktdaten des Entwicklers“:

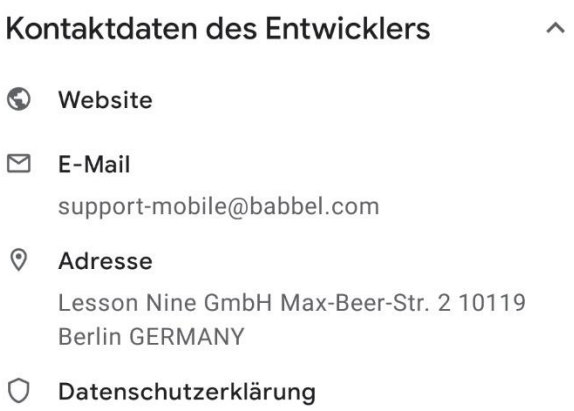


Abbildung 7: Screenshot des Abschnitts *Kontaktdaten des Entwicklers* zur „Babbel“-App im App-Store *Google Play*, bearbeitet

Nach dem Einkauf wird dem Kunden bestätigt, „bei *Google* Commerce Limited auf *Google Play*“ eingekauft zu haben:

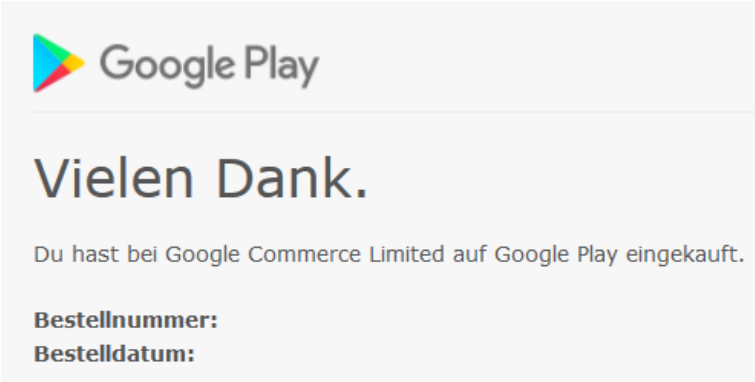


Abbildung 8: Screenshot aus Kaufbestätigungs-E-Mail, bearbeitet

Bei In-App-Käufen wird die Bezahlung zwar aus der App heraus initiiert, aber ebenfalls über *Google Play* abgewickelt:

51 Hervorhebung hinzugefügt.

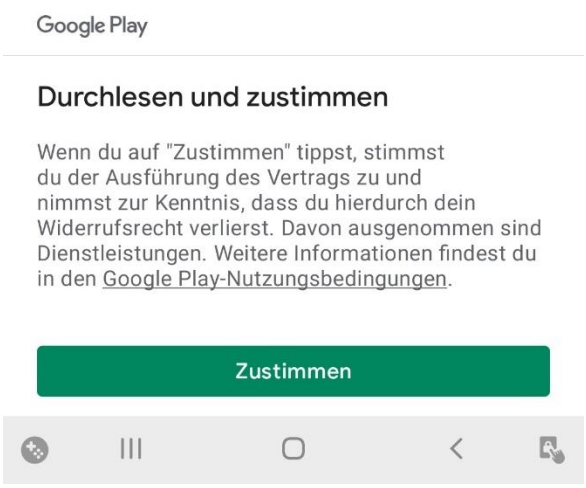


Abbildung 9: Screenshot In-App-Kauf (*Android*) – Zustimmung zu Nutzungsbedingungen[52]

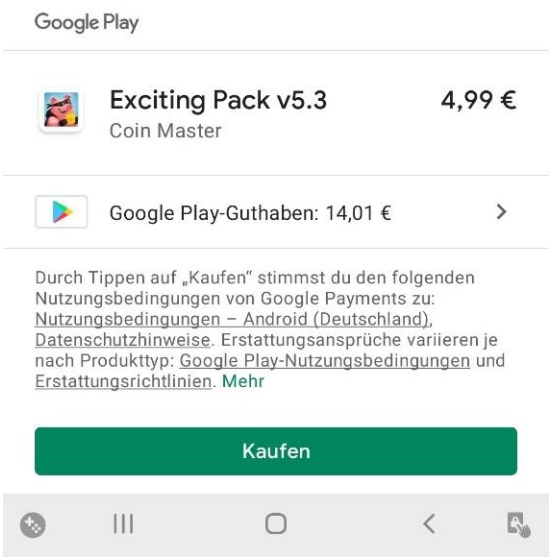


Abbildung 10: Screenshot In-App-Kauf (*Android*) - Kauf

2. Würdigung

In seiner Vertriebsvereinbarung für Entwickler erweckt *Google* den Eindruck, nur vertretungsweise für die App-Publisher zu handeln[53]. Dem steht auch nicht entgegen, dass *Google* gemäß dieser Vereinbarung als „Merchant of Record" auftritt. Beim sog. Merchant of Record handelt es sich um eine Einrichtung, die autorisiert ist, Zahlungen von Verbrauchern für ein Unternehmen zu verarbeiten. Der Merchant of Record übernimmt die gesamte Verantwortung für die Zahlungsabwicklung, einschließlich der Einhaltung von Steuergesetzen und der Ergreifung von Maßnahmen zu Betrugsbekämpfung. Allein aus der Bezeichnung „Merchant of Record" lässt sich somit nicht der Schluss ziehen, das betreffende Unternehmen wolle selbst notwendigerweise Vertragspartner des Endabnehmers werden. Freilich ist in diesem Zusammenhang verwirrend, dass *Google* dem Begriff „Merchant of Record" stets den Klammerzusatz „Vertragspartner" hinzufügt. Mutmaßlich handelt es sich hierbei schlicht um eine unpräzise Übersetzung von „Merchant of Record"; aus dem Kontext könnte die Formulierung aber durchaus so verstanden werden, dass *Google* jedenfalls im EWR Vertragspartner des Endabnehmers werden soll.

Es ist aber ohnehin sehr zweifelhaft, ob und inwieweit die in der Vertriebsvereinbarung für Entwickler geregelte Vertretungsregelung die rechtliche Beziehung zwischen *Google* und dem Endverbraucher bestimmen kann. Bei den für einen Vertragsschluss erforderlichen Willenserklärun-

---

52 Die Anzahl der befragten *iOS*-Nutzer ist zu gering, um eine Repräsentativität für die Gruppe aller *iOS*-Nutzer im statistischen Sinne zu gewährleisten.

53 Siehe oben, S. 21 f.

gen handelt es sich um empfangsbedürftige Erklärungen, so dass bei der erforderlichen Auslegung neben dem tatsächlichen Willen der Parteien auch zu berücksichtigen ist, wie sie der Empfänger nach Treu und Glauben unter Berücksichtigung der Verkehrssitte verstehen musste, § § 133, 157 BGB[54]. Zu berücksichtigen sind dabei alle Umstände, insbesondere früheres Verhalten, Zeit und Ort der Erklärung, die berufliche Stellung der Parteien, Art und Inhalt ihrer Werbung und die erkennbare Interessenlage.[55] Die Frage, wer Vertragspartner wird, kann also nicht einseitig festgelegt werden. Insbesondere können Vertragsbedingungen, die ein Vertragsteil mit einem Dritten vereinbart und die dem anderen weder bekannt sind noch ihm zur Kenntnis gegeben werden, allenfalls eine äußerst schwache Indizwirkung entfalten. Man mag einwenden, dass der App-Store *Google Play* beim Betrachter den Anschein eines „Marktplatzes“ erwecken könnte, auf dem – ähnlich wie bei eBay – lediglich Dritt-Apps im Namen anderer Anbieter verkauft werden. Wie oben dargestellt[56], bezeichnet sich jedoch *Google* gegenüber dem Play-Store-Nutzer konsequent als Anbieter der auf *Google Play* herunterladbaren Apps. Es ist somit für den Nutzer nicht ersichtlich, dass *Google* nicht in eigenem, sondern in fremdem Namen handeln will. § 164 Abs. 2 BGB sieht zudem vor, dass selbst der fahrlässig verursachte Anschein, ein Eigengeschäft abschließen zu wollen, unbeachtlich ist. Auch eine Ausnahme vom Offenkundigkeitsprinzip kann beim Herunterladen einer App auf *Google Play* nicht angenommen werden. Eine solche Ausnahme könnte etwa angenommen werden, wenn es an einem Interesse des Geschäftsgegners an der Identität des Vertretenen fehlt (sog. Geschäft für den, den es angeht). Da an die Vertragspartnerstellung jedoch durchaus relevante gewährleistungs- und haftungsrechtliche Fragen anknüpfen und eine Abwicklung von Ansprüchen mit dem App-Store-Betreiber grundsätzlich einfacher abzuwickeln sein dürfte, kann nicht davon ausgegangen werden, dem Nutzer sei die Identität des Vertretenen gleichgültig.

Google ist demnach als Vertragspartner des Endverbrauchers anzusehen, der eine App aus dem App-Store herunterlädt. Dies gilt gleichermaßen für kostenfreie wie kostenpflichtige Apps. Auch

---

54 Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 02.01.2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Artikel 1 des Gesetzes vom 09.06.2021 (BGBl. I S. 1666). Die Anwendbarkeit deutschen Rechts gegenüber Verbrauchern ergibt sich bereits aus den *Google*-Nutzungsbedingungen, die auch der Nutzung von *Google Play* zu Grunde liegen (Abschnitt "Streitbeilegung, geltendes Recht und Gerichte“).

55 S. *Ellenberger* in Palandt [Hrsg.], Bürgerliches Gesetzbuch: BGB, 80. Aufl. 2021, § 164 Rn. 4.

56 Siehe hierzu die Ausführungen und Abbildungen auf S. 22 f.

bei In-App-Käufen tritt *Google* als Verkäufer auf.[57] Hierbei handelt es sich indessen um eine zivilrechtliche Einschätzung des Verhältnisses zwischen App-Store-Betreiber und App-Nachfrager. Es ist zum einen durchaus vorstellbar, dass das Vertragsverhältnis zwischen App-Publisher und *Google Play* aufgrund der dort vorherrschenden Vertragsverhältnisse entgegengesetzt zu beurteilen ist. Es ist zum anderen nicht auszuschließen, dass die Rolle des App-Store-Betreibers in anderem Zusammenhang, z. B. im Rahmen der Anwendung europäischer Rechtsakte, abweichend zu definieren ist.

II. Apples App-Store

Auch für den App-Store von *Apple* wurden Nutzeroberfläche und die Vertragstexte im Verhältnis von *Apple* zu App-Publishern bzw. App-Store-Nutzern untersucht.

1. Ermittlungen

Bei *Apple* wird das Verhältnis zwischen Store-Betreiber und App-Publisher durch das *Apple Developer Program Licence Agreement* (ADPLA) geregelt, welches lediglich in englischer Sprache erhältlich ist und eine Anmeldung im kostenpflichtigen „Developer Program“ voraussetzt.

Die Ausgestaltung des App-Vertriebs ist für kostenlose Apps in Schedule 1, für kostenpflichtige Apps in Schedule 2 des ADPLA geregelt. Dort wird *Apple* für den Vertrieb an Nutzer, die in Deutschland ansässig sind, jeweils zum „commissionaire for the marketing and delivery of the Licensed Applications to end-users“. Der Begriff des „commissionaire“ (Französisch „commissionnaire“) ist dabei ausweislich Exhibit A Ziff 2. des ADPLA im Sinne des Art. 91 des Luxemburgischen Code du Commerce zu verstehen und in etwa gleichbedeutend mit dem Kommissionär im deutschen Recht.[58]

---

57 Bei Abo-Modellen hingegen (Netflix, Spotify) schließt der Abnehmer erkennbar mit dem Inhalteanbieter einen Vertrag ab. Derzeit ist noch nicht absehbar, wie sich *Googles* Ankündigung, ab Oktober 2021 auch solche Abomodelle über *Google Play* abzurechnen, auf die konkrete Interaktion zwischen Kunden und Inhalteanbieter auswirken wird, vgl. *Samat*, Listening to Developer Feedback to Improve *Google Play* (*Android* Developers Blog, 28.09.2020), abrufbar unter https://android-developers.googleblog.com/2020/09/listening-to-developer-feedback-to.html.

58 S. dazu auch *Engelhardt* in: Solmecke/Taeger/Feldmann [Hrsg.], Mobile Apps, 2013, S. 76.

In den Bedingungen der *Apple Media Services*[59] findet sich eine Passage, in der *Apple* als Vertreter bezeichnet wird:

> „App-Lizenzen werden Ihnen von Apple oder einem Drittentwickler („App-Provider“) zur Verfügung gestellt. Eine von Apple lizenzierte App ist eine „Apple-App“; eine von einem App-Provider lizenzierte App ist eine „Dritt-App“. Indem Apple den App Store zur Verfügung stellt, handelt Apple als Vertreter für App-Provider und ist keine Partei des Kaufvertrages oder der Benutzervereinbarung zwischen Ihnen und dem App-Provider.“

Allerdings wird diese Aussage sofort wieder eingeschränkt durch den Zusatz

> „Falls Sie jedoch Kunde von Apple Distribution International Ltd. sind, ist Apple Distribution International Ltd. der Vertragspartner, was bedeutet, dass Sie die App von Apple Distribution International Ltd. erwerben, aber die App von dem App-Provider lizenziert wird.“

Um herauszufinden, bei welcher *Apple*-Gesellschaft man Kunde ist, muss man zunächst einen Blick auf die einleitenden Worte der Bedingungen der *Apple* Media Services werfen („Diese Bedingungen begründen einen Vertrag zwischen Ihnen und *Apple*“) und sodann Abschnitt L. der Bedingungen zu Rate ziehen, in dem sich folgende Definition von „*Apple*” findet:

> „Abhängig von Ihrem Heimatland bedeutet „Apple“:
>
> [Regelungen für USA, Kanada, Mexiko, Mittel- oder Südamerika, karibische Länder oder Territorien, Japan, Australien und Neuseeland]
>
> …Apple Distribution International Ltd., mit Sitz in Hollyhill Industrial Estate, Hollyhill, Cork, Republic of Ireland, für alle anderen Benutzer.“

Die App-Titelseite in *Apples* App-Store weist dasselbe Unternehmen zunächst als „Entwickler“, bei den detaillierten App- Informationen aber als „Anbieter“ aus:

---

59 S. Bedingungen der *Apple* Media Services (Stand: 16.09.2020), Abschnitt G. Zusätzliche Bedingungen für den App Store … – Lizenz für App Store-Inhalte, abrufbar unter https://www.apple.com/legal/internet-services/itunes/de/terms.html.

Abbildung 11: Screenshot der Info zur „komoot“-App im App-Store von *Apple*[60]

Zur besseren Erkennbarkeit nachfolgend eine auszugsweise vergrößerte Darstellung:

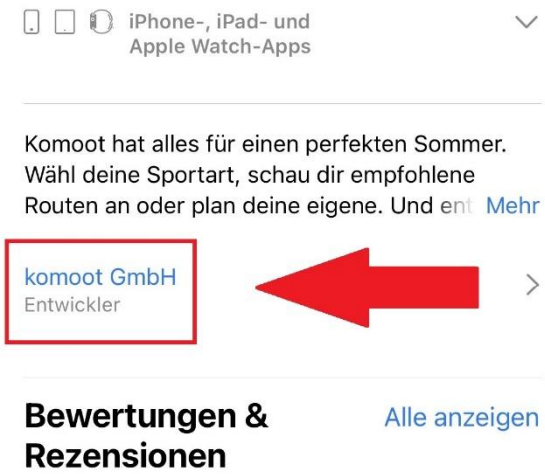


Abbildung 12: Screenshot *komoot* als „Entwickler“ bezeichnet

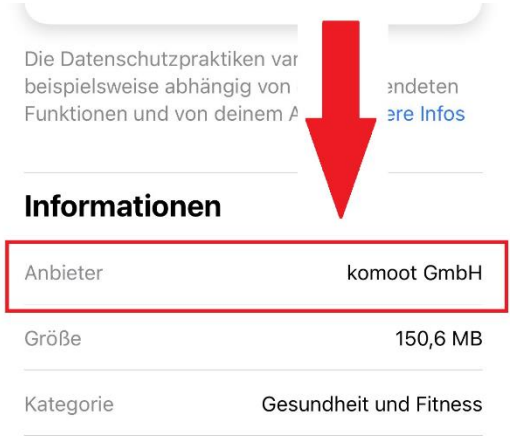


Abbildung 13: Screenshot *komoot* als „Anbieter“ bezeichnet

60 Hervorhebungen hinzugefügt.

Die von *Apple* versandte Rechnung enthält zwar das *Apple*-Logo, lässt aber ansonsten keine direkten Rückschlüsse darauf zu, von wem die App gekauft wurde:

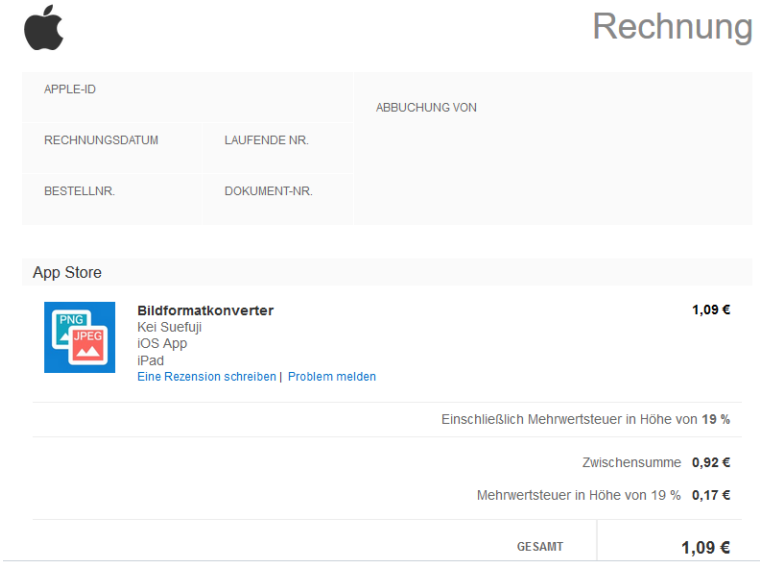


Abbildung 14: Screenshot aus Kaufbestätigungs-E-Mail, bearbeitet

2. Würdigung

Bei *Apple* stellt sich die Situation etwas komplexer dar als bei *Google*. Hier definiert das ADPLA die Rolle *Apples* als die eines Kommissionärs[61]. Bei Kommissionsgeschäften wird der Kommissionär selbst Vertragspartner des Endabnehmers. Abgesehen von der ohnehin schwachen Indizwirkung von vertraglichen Vereinbarungen *Apples* mit App-Publishern im Hinblick auf das Verhältnis zum Endabnehmer gilt es hier zu beachten, dass das ADPLA ohne kostenpflichtiges Entwicklerkonto nicht frei zugänglich und für den durchschnittlichen Endabnehmer somit nicht einsehbar ist. Eine nennenswerte Ausstrahlungswirkung auf das Rechtsverhältnis zwischen *Apple* und Endabnehmer wird man daher grundsätzlich nicht annehmen können.

Auf der jeweiligen App-Seite in *Apples* App-Store wird der App-Publisher zunächst als „Entwickler“ genannt, in den zentralen App-Informationen[62] hingegen als Anbieter. Obwohl die Rolle als App-Entwickler zuerst genannt wird, dürfte die Bezeichnung als Anbieter in den zentralen App-Informationen schwerer wiegen, da es aus Sicht des App-Interessenten durchaus möglich sein kann, dass ein Unternehmen als Entwickler und Anbieter auftreten kann. Im Ergebnis spräche dies für die Annahme einer (Handels-)Vertreterposition *Apples*. Dies steht wiederum im Widerspruch zu den Bedingungen für die *Apple Media Services*. Diese sehen vor, dass *Apple* selbst

61 Siehe oben, S. 26.

62 Siehe dazu oben Abbildung 11 auf S. 28.

Vertragspartner wird, jedenfalls u. a. für die europäischen Kunden von *Apple* Distribution International Ltd.[63] – als Ausnahme von einer ansonsten für Kundenbeziehungen in anderen Ländern einschlägigen Vertreterstellung. Die vom Bundeskartellamt durchgeführte Verbraucherbefragung legt nahe, dass Nutzer eher der Auffassung sind, beim App-Download mit dem „App-Anbieter" einen Vertrag zu schließen als mit *Apple* selbst[64]. Dennoch trifft mit rund 40 Prozent nur eine Minderheit der Befragten die Aussage, der „App-Anbieter" sei alleiniger Vertragspartner. Man mag nun einwenden, dass Verbraucher im Alltag – im Gegensatz zur Verbraucherbefragung, bei der den Testteilnehmern relevante Auszüge aus den Nutzungsbedingungen vorgelegt wurden – solche Texte ganz überwiegend nicht oder nur flüchtig lesen.[65] Demnach lässt sich vermuten, dass womöglich eine Mehrheit von *Apples* App-Store-Nutzern den jeweiligen „App-Anbieter" als Vertragspartner betrachtet. Eine Restunsicherheit bleibt jedoch. Auch in der Literatur wird *Apple* mitunter als Vertragspartner angesehen.[66] Dessen ungeachtet stellt sich die Frage, ob *Apple* im Rahmen des Gewährleistungsrechts auch dann als Vertragspartner Betracht kommt, wenn *Apple* nicht oder nicht mit Sicherheit als solcher identifiziert werden kann (dazu unten, S. 99).

E. Verbraucherrechtliche Problemfelder

Nachfolgend wird dargestellt, mit welchen Problemen Verbraucher in Berührung kommen, wenn sie mit mobilen Apps zu tun haben. Dies beginnt mit den Apps, die Verbraucher auf neu gekauften Mobilgeräten vorfinden (dazu unten I.). Anschließend wird die Suche nach Apps in den App-Stores von *Google* und *Apple* eingehender betrachtet (dazu unten II.). Einen zentralen Punkt der Untersuchung bildet die Frage, ob der Verbraucher vor dem App-Download im App-Store ausreichende Informationen erhält (dazu unten III.). Der mit dem Download einhergehende Vertragsschluss sowie Gewährleistungsfragen (dazu unten IV.) werden sodann ebenso erörtert wie die Frage der Einstellungen der Datenzugriffsberechtigungen von Apps (dazu unten V.).

---

63 S. dazu oben S. 27 f.

64 S. Abbildung 4 auf S. 20.

65 S. etwa *Institut für Demoskopie Allensbach*, Freiwillige und informierte Einwilligung? - Die Nutzerperspektive, (Allensbacher Archiv, IfD-Umfrage 8201, September 2019), S. 6 der Darstellung unter https://www.ifd-allensbach.de/fileadmin/IfD/sonstige_pdfs/FOCUS_deutsch.pdf; Verbraucherzentrale Bundesverband e. V., Was wissen Verbraucher über ihre Daten? – Ergebnisse einer Umfrage (22.01.2020, nicht repräsentativ), abrufbar unter https://www.verbraucherzentrale.de/umfrage-betroffenenrechte-dsgvo; *Rudolph/Feth/Polst*, Why Users Ignore Privacy Policies – A Survey and Intention Model for Explaining User Privacy Behavior, in: Kurosu [Hrsg.], Human-Computer Interaction. Theories, Methods, and Human Issues 2018, 587, 589, abrufbar unter https://link.springer.com/content/pdf/10.1007%2F978-3-319-91238-7_45.pdf.

66 *Ewald* in: Baumgartner/Ewald [Hrsg.], Apps und Recht, 2. Aufl. 2016, Rn. 54d; Auer-Reinsdorff/Conrad IT-R-HdB, 3. Aufl. 2019, § 36 Datenschutz im Internet, Rn. 255.

I. Vorinstallation von Apps

Smartphones und Tablets werden mit bereits vom Hersteller vorinstallierten Apps ausgeliefert, wobei in der Regel für den Käufer nicht vorab ersichtlich ist, um welche Apps es sich handelt. Es kann daher durchaus vorkommen, dass Nutzer vorinstallierte Apps nicht als Bereicherung, sondern als Ärgernis wahrnehmen.

Die Verbraucher wünschen in ihrer großen Mehrheit keine oder nur eine geringe Zahl von App-Vorinstallationen, wie eine Untersuchung der Marktwächter Digitale Welt aus dem Jahr 2019 zeigt:

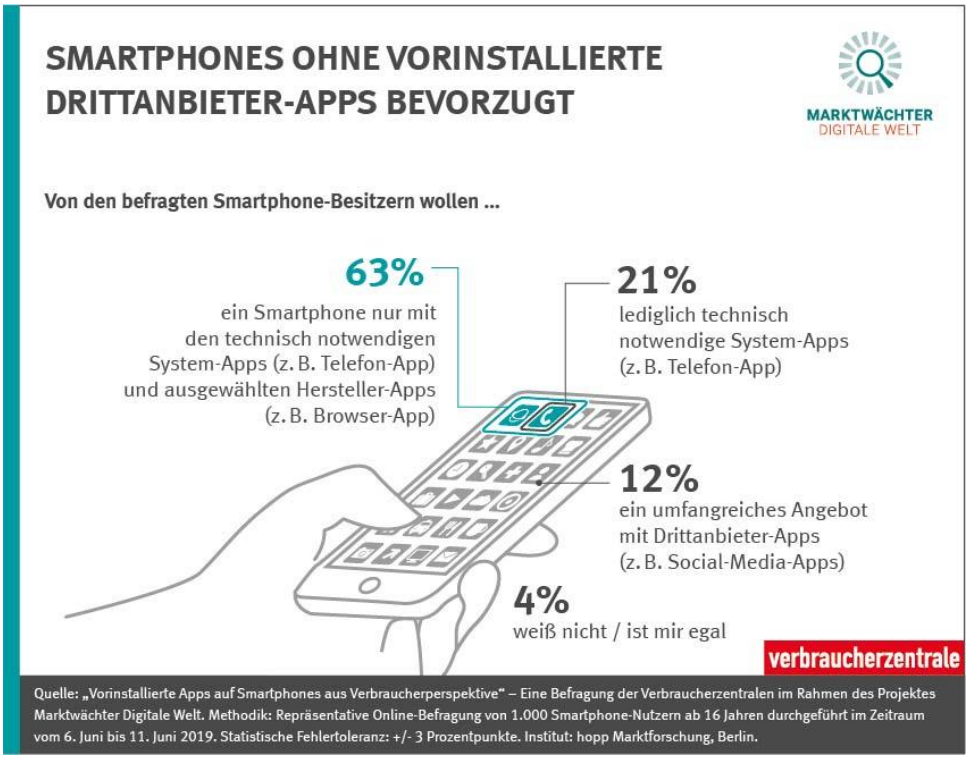


Abbildung 15: Ergebnisse der Marktwächter-Verbraucherbefragung zu vorinstallierten Apps (Abdruck mit freundlicher Genehmigung des Verbraucherzentrale Bundesverband (vzbv))

1. Ermittlungen

Bei *Apple*-Geräten stammen die vorinstallierten Apps allesamt von *Apple* selbst. Dabei erlaubt *Apples* Betriebssystem *iOS* überwiegend ein Löschen der vorinstallierten Apps; eine Grundausstattung von Apps (z. B. App-Store, Kamera-App, Internet-Browser) kann hingegen nicht entfernt werden. Die nachfolgenden Abbildungen zeigen links den Startbildschirm eines *iPads* mit allen vorinstallierten Apps sowie rechts den gleichen Startbildschirm nach Löschung aller deinstallierbaren Apps:

Abbildung 16: iPad-Homescreen – Auslieferungszustand mit vorinstallierten Apps

Abbildung 17: iPad-Homescreen nach Löschung aller deinstallierbaren Apps

Nach einem Zurücksetzen auf Werkseinstellungen sind sämtliche Apps wieder vorhanden oder werden automatisch aus dem Internet heruntergeladen (sofern der Downloadvorgang nicht unterbrochen wird). Dies zeigt die folgende Abbildung:

Abbildung 18: iPad-Homescreen nach Zurücksetzen auf Werkseinstellungen[67]

Bei *Android*-Geräten sind hingegen im Regelfall neben diversen *Google*-Apps sowohl Apps des Herstellers als auch Drittanbieter-Apps vorinstalliert. Es kommt dabei häufig vor, dass Apps für die gleiche Funktion doppelt vorinstalliert sind (z. B. Browser, Fotogalerien, Cloud-Speicher).

67 Vier Apps werden noch geladen bzw. befinden sich in der Warteschleife.

Die Anzahl vorinstallierter Apps auf *Android*-Geräten kann erheblich variieren, wobei tendenziell auf preisgünstigeren Smartphones und Tablets mehr Apps anzutreffen sind als bei teureren Geräten.[68] Einige dieser Apps können gelöscht werden, andere lediglich deaktiviert[69]. Es gibt auch Apps, die weder gelöscht noch deaktiviert werden können. Während System-Apps in der Regel weder deinstalliert noch deaktiviert werden können, ergibt sich bei den *Google*-, Smartphone-Hersteller- und Dritt-Apps kein einheitliches Bild. So können die gleichen Apps auf unterschiedlichen Geräten (nicht) deaktivierbar/deinstallierbar ausgestaltet sein, wie die folgende Gegenüberstellung veranschaulicht:

Smartphone / Vorinstallierte App	**Samsung Note10 Lite**	**Poco M3 (Xiaomi)**
Facebook	deaktivierbar	deinstallierbar
Google Chrome	deaktivierbar	nicht deaktivierbar
Gmail	deaktivierbar	nicht deaktivierbar
Google Maps	deaktivierbar	nicht deaktivierbar
Netflix	deaktivierbar	deinstallierbar
YouTube	deaktivierbar	deinstallierbar

Tabelle 1: Deaktivierbarkeit/Deinstallierbarkeit von Apps auf zwei *Android*-Smartphones

Es kann durchaus vorkommen, dass Apps ohne jegliche Systemrelevanz weder deinstallierbar noch deaktivierbar ausgestaltet, also ggf. stets im Hintergrund aktiv sind. So waren etwa bei einem vom Bundeskartellamt untersuchten Wifi-Tablet ohne Mobilfunkmodul sowohl eine Telefon- als auch eine SMS-App vorinstalliert, die sich weder deinstallieren noch deaktivieren ließen. Siehe hierzu auch die folgende Abbildung zweier vorinstallierter Wetter-Apps, bei denen jeweils kein Deinstallations-Button vorhanden und die Deaktivierungsschaltfläche ausgegraut (nicht klickbar) ist:

---

68 S. dazu unten Tabelle 2 auf S. 35, die nur die *deinstallierbaren* vorinstallierten Apps aufführt.

69 Während bei einer Deinstallation die betreffende App (ggf. mit Ausnahme von Installationsdateien, die für den Nutzer nicht sichtbar sind) komplett vom Gerät „verschwindet“, sind deaktivierte Apps lediglich „eingefroren“ und nach wie vor auf dem Gerät vorhanden und werden z. B. in den Einstellungen bei der Auflistung aller Apps angezeigt. Deaktivierte Apps belegen jedoch nach wie vor Speicherplatz und können jederzeit mit einem Klick wieder aktiviert werden. Im Gegensatz zu *Android* gibt es bei *iOS* keine Deaktivierungsmöglichkeit.

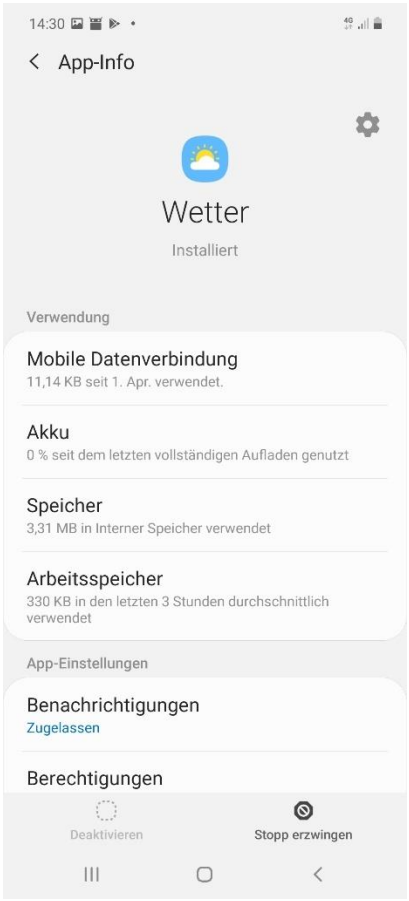


Abbildung 19: Wetter-App, vorinstalliert auf dem *Samsung Note10 Lite*

Abbildung 20: Wetter-App, vorinstalliert auf dem *Poco M3* (Hersteller: *Xiaomi*)

Werden Apps deinstalliert, so können diese nach einem Werksreset (Zurücksetzen auf den Auslieferungszustand) wieder vorhanden sein. So waren die von einem iPad gelöschten Apps[70] nach dem Zurücksetzen des Tablets entweder wieder vorhanden oder sie wurden – ohne Zutun des Nutzers – unmittelbar bei erstmaliger Anzeige des Homescreens per Download nachinstalliert. Bei *Android*-Geräten variiert die Endgültigkeit von Löschungen je nach Smartphone- oder Tabletmodell. Im folgenden Beispiel etwa wurde ein Teil der deinstallierten Apps wiederhergestellt:

70 Siehe Abbildung 16 und Abbildung 17 auf S. 32.

Deinstallierbare Apps im Auslieferungszustand	Kurzbeschreibung der App	Wieder vorhanden nach Werksreset?
Agoda	Online-Hotelbuchungsportal	**Ja**
AliExpress	Online-Shop	Nein
Amazon Shopping	Online-Shop	**Ja**
Block Puzzle Guardian	Spiel	Nein
Bubble Shooter	Spiel	Nein
Bubble Story	Spiel	Nein
Crazy Juicer	Spiel	Nein
Dust Settle	Spiel	Nein
eBay	Online-Auktionsplattform	**Ja**
Facebook	Soziales Netzwerk	**Ja**
Fotos	Foto-Galerie	Nein
Google Drive	Cloud-Speicher	Nein
Google Duo	Videoanrufe-App	Nein
Google News	Nachrichtenportal	Nein
Google Play Filme & Serien	Streamingportal für Filme	Nein
Google Podcasts	Portal für Podcasts	Nein
LinkedIn	Soziales Netzwerk f. Geschäftskontakte	**Ja**
Lords Mobile	Spiel	**Ja**
Mi Dokumente-Viewer	App zum Betrachten von Dokumenten	**Ja**
Mi Fernbedienung	IR-Fernbedingungs-App	**Ja**
Mi Store	Online-Shop für Xiaomi-Produkte	Nein
Netflix	Streamingportal für Filme	**Ja**
Opera	Internetbrowser	Nein
TikTok	Social-Media-App	**Ja**
Tile Fun	Spiel	Nein
WPS Office	Office-Paket	Nein
YouTube Music	Streamingportal für Musik	Nein

Tabelle 2: Manche Apps „überleben“ die Deinstallation (*Xiaomi Poco M3*)

2. Würdigung

Die Problematik nicht löschbarer vorinstallierter Apps wurde bereits in der Sektoruntersuchung Smart-TVs des Bundeskartellamts geprüft. Im Ergebnis stellt die Vorinstallation nicht benötigter Apps (sog. „Bloatware“) jedenfalls nach aktueller Gesetzeslage und Rechtsprechung im Regelfall

keinen Verstoß der Gerätehersteller oder Händler gegen Verbraucherrecht dar.[71] Eine zivilrechtliche Haftung erscheint aber auch nicht völlig ausgeschlossen, wenn vorinstallierte nicht-deinstallierbare/-deaktivierbare (Dritt[72]-)Apps erkennbar rechtswidrige Verarbeitungen personenbezogener Daten vornehmen. Eine solche Vorinstallation würde eine Gefahrenquelle im Hinblick auf mögliche Verletzungen des Rechts des Nutzers auf informationelle Selbstbestimmung eröffnen, was es rechtfertigen würde, dem Gerätehersteller eine eigenständige Prüfpflicht auch im Hinblick auf Datenschutzverletzungen durch vorinstallierte Apps aufzuerlegen.[73] Ungeachtet dessen empfinden Verbraucher die Vorinstallation etlicher Apps, die sie nicht benötigen, jedenfalls als lästig, wie die obige Abbildung 15 auf Seite 31 zeigt.

Mit Ausnahme wirklich systemrelevanter Apps gibt es für eine Sperrung der Deinstallationsmöglichkeit keine erkennbaren technischen Gründe. Mutmaßlich hängt es maßgeblich von der jeweiligen Gegenleistung der betreffenden App-Publisher ab, ob eine App deinstallierbar, nur deaktivierbar oder weder deinstallierbar noch deaktivierbar ausgestaltet ist. Gegen eine Deinstallierbarkeit lässt sich auch nicht einwenden, die App müsse bei einem Zurücksetzen auf Werkseinstellungen wieder vorhanden sein; dies lässt sich durch entsprechende Gestaltung der Geräteeinrichtung auch anderweitig erreichen und wird bei vielen vorinstallierten Apps auch bereits so praktiziert.[74] Eine grundsätzliche Deinstallierbarkeit von Apps wäre das einfachste Mittel, um die Interessen von Kunden (nur wenige Apps) und Hersteller (Gestaltungs- und Finanzierungsmöglichkeiten bei der Vermarktung der Geräte) unter einen Hut zu bringen.

---

71 Siehe hierzu den Abschlussbericht der Sektoruntersuchung Smart-TVs des Bundeskartellamts auf S. 207 ff., abrufbar unter https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_SmartTVs_Bericht.pdf?__blob=publicationFile&v=5. Eine kartellrechtliche Einschätzung kann hier ggf. zu anderen Ergebnissen gelangen, insbesondere wenn das Verhalten von marktmächtigen Betriebssystem-Betreibern bzw. generell Unternehmen mit überragender marktübergreifender Bedeutung i. S. v. § 19a GWB in Frage steht.

72 Bei der Haftung für Rechtsverletzungen durch eigene Apps ergeben sich keine Besonderheiten; in diesem Zusammenhang können sich gerade bei marktbeherrschenden Unternehmen darüber hinaus auch kartellrechtliche Fragen stellen. So hatte die Europäische Kommission im Verfahren *Google Android* u. a. bemängelt, dass *Google* Smartphone-Hersteller durch illegale Kopplungspraktiken faktisch zur Vorinstallation der Google-Such-App sowie des Chrome-Browsers gezwungen habe, s. dazu Europäische Kommission, Entscheidung vom 18.07.2018, Az. AT 40099, insb. Rn. 754 ff., abrufbar (in Englisch) unter https://ec.europa.eu/competition/antitrust/cases/dec_docs/40099/40099_9993_3.pdf - *Google Android*.

73 Vgl. dazu *Specht-Riemenschneider*, Herstellerhaftung für nicht-datenschutzkonform nutzbare Produkte – Und er haftet doch!, MMR 2020, 73, 75.

74 Es wäre auch denkbar, für alle nicht systemrelevanten Apps lediglich einen Download-Link auf der Nutzeroberfläche des Mobilgeräts zu platzieren.

Die Notwendigkeit einer grundsätzlichen Deinstallationsmöglichkeit sieht auch der Entwurf für einen sog. „Digital Markets Act“[75] der Europäischen Kommission für dessen Normadressaten vor. Art. 6 Abs. 1 des Entwurfs lautet auszugsweise:

> „Der Gatekeeper muss in Bezug auf jeden seiner zentralen Plattformdienste im Sinne des Artikels 3 Absatz 7
>
> […]
>
> b) Endnutzern die Möglichkeit geben, Software-Anwendungen, die auf seinem zentralen Plattformdienst vorinstalliert sind, zu deinstallieren; dies gilt unbeschadet der Möglichkeit eines Gatekeepers, die Deinstallation von Software-Anwendungen zu beschränken, die für das Funktionieren des Betriebssystems oder des Geräts unabdingbar sind und die aus technischen Gründen nicht von Dritten eigenständig angeboten werden können […]“

Als zentrale Plattformdienste gelten gem. Art. 2 Nr. 1 und Nr. 2 lit. f) des Entwurfs auch Betriebssysteme (wie *Apple iOS* und *Google Android*). Allerdings verlangt die „Gatekeeper“-Eigenschaft gem. Art. 3 Abs. 1 lit. b) des Entwurfs u. a. den Betrieb eines zentralen Plattformdienstes, der gewerblichen Nutzern als wichtiges Zugangstor zu Endnutzern dient. Dieses Kriterium ist nach Art. 3 Abs. 2 lit. b) des Entwurfs in der Regel erfüllt, wenn der Plattformdienst im vergangenen Geschäftsjahr mehr als 45 Millionen in der Union niedergelassene oder sich dort aufhaltende monatlich aktive Endnutzer und mehr als 10.000 in der Union niedergelassene jährlich aktive gewerbliche Nutzer hatte. Für das mobile Betriebssystem *Apple iOS* erscheint dies ebenso wie für *Googles Android* nicht fernliegend. Bei *Android* besteht indessen die Schwierigkeit, dass das Betriebssystem von den Geräteherstellern zumeist modifiziert und mit einer eigenen Bedienoberfläche versehen wird; mitunter wird in diesem Zusammenhang sogar von eigenständigen Betriebssystemen gesprochen[76]. Auch sind es die Gerätehersteller, die – ggf. mit Ausnahme einiger *Google*-Apps – über die Löschbarkeit vorinstallierbarer Apps entscheiden. Nach der eher weiten Definition des Betriebssystems in Art. 2 Nr. 10 des Entwurfs („eine Systemsoftware, die die Grundfunktionen der Hardware oder Software steuert und die Ausführung von Software-Anwendungen ermöglicht“) ließe es sich vertreten, neben *Google*[77] auch die Gerätehersteller, die das

---

75 Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte) vom 15.12.2020, COM(2020) 842 final, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0842.

76 Siehe hierzu etwa den Wikipedia-Eintrag zu Xiaomis MIUI, abrufbar unter https://de.wikipedia.org/wiki/MIUI.

77 Soweit der Endabnehmer für die Nutzung seines Smartphones bzw. Tablets die *Google*-Nutzungsbedingungen akzeptieren muss, ist davon auszugehen, dass *Google* auch als Betriebssystem-Betreiber zu qualifizieren ist.

„nackte“ von *Google* bereitgestellte *Android*-Betriebssystem mehr als nur völlig unerheblich auf die Besonderheiten des eigenen Geräts zuschneiden und an die eigenen Bedürfnisse anpassen, ebenfalls als Betreiber eines (zweischichtigen) Betriebssystems anzusehen. Dies wird man jedenfalls wohl dann annehmen können, wenn der Gerätehersteller eigene Nutzungsbedingungen für die Nutzung des Betriebssystems vorsieht. Ob die Hersteller von Smartphones und/oder Tablets jedoch die in Art. 3 Abs. 1 des Entwurfs für den „Gatekeeper“-Status grundsätzlich vorgesehenen Voraussetzungen bzw. die in Art. 3 Abs. 2 vorgesehenen Nutzerzahlen- und Umsatz- bzw. Marktkapitalisierungsschwellen erreichen würden, kann jedoch – ggf. mit Ausnahme von *Samsung* – nicht als gesichert gelten.[78]

Derzeit ist noch nicht absehbar, wann und in welcher Form dieses Gesetz über digitale Märkte letztlich in Kraft treten wird. Aus Verbrauchersicht wäre es jedenfalls zu begrüßen, wenn sämtliche Betriebssystem-Betreiber, Mobilgerätehersteller oder ggf. auch Händler, die Vorinstallationen vornehmen, eine Deinstallation nicht systemrelevanter vorinstallierter Apps ermöglichen würden – sei es freiwillig oder aufgrund einer gesetzlichen Verpflichtung.

II. Suche nach Apps

Den meisten Nutzern reicht die App-Ausstattung ihres Smartphones im Auslieferungszustand nicht aus.[79] Soweit die gewünschten Apps bereits namentlich bekannt sind, lassen diese sich über *Google Play* oder *Apples* App Store leicht auffinden und nachinstallieren. Schwieriger ist es hingegen für die Nutzer, wenn eine App für eine bestimmte Funktion gesucht wird (z. B. ein Kompass, eine Poker-App, eine App zum Abspielen von Hörbüchern), ohne dass die Wahl bereits vorab auf eine ganz bestimmte App gefallen wäre, und die Suchfunktion im App-Store dazu genutzt wird, um unter mehreren in Frage kommenden Apps eine App auszuwählen, die den eigenen Bedürfnissen am besten gerecht wird. Die Verbraucherbefragung des Bundeskartellamts hat nämlich ergeben, dass die Nutzer von App-Stores in der Reihung der Suchergebnisse ganz überwiegend keine Logik erkennen können:

---

78 Im Rahmen von Art. 3 Abs. 1 DMA-E binden die Schwellenwerte des Art. 3 Abs. 2 die Kommission bei der Benennung von Gatekeepern nicht, dürften faktisch aber eine starke Indizwirkung besitzen, weshalb eine Benennung von Unternehmen mit wesentlich geringeren Werten eher unwahrscheinlich sein dürfte.

79 S. dazu oben Fn. 12.

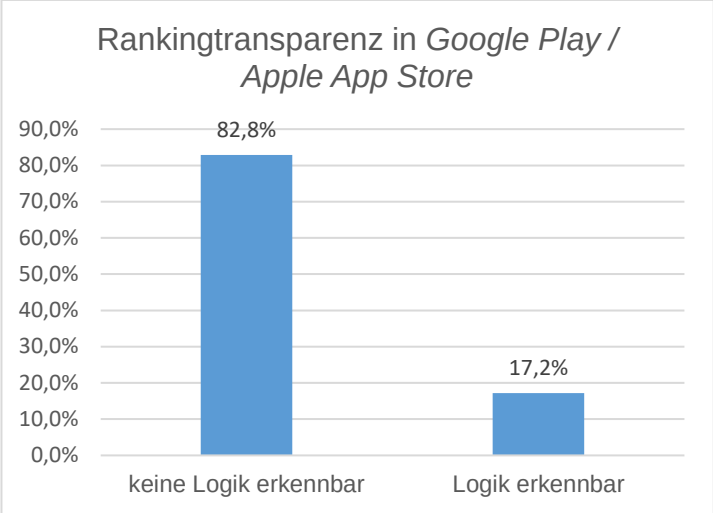


Abbildung 21: Erkennbarkeit der Logik der Suchergebnisreihung in den App-Stores von *Google* und *Apple*

Die Befragten, die eine Logik zu erkennen glaubten, gaben zudem überwiegend Ranking-Kriterien an, die ganz offensichtlich nicht zutrafen.

In der Befragung des Bundeskartellamts bewerteten außerdem jeweils mehr als 80 Prozent der Befragten die folgenden (bislang nicht existierenden) Sortierkriterien als sehr hilfreich oder eher hilfreich für eine Suche nach Apps:

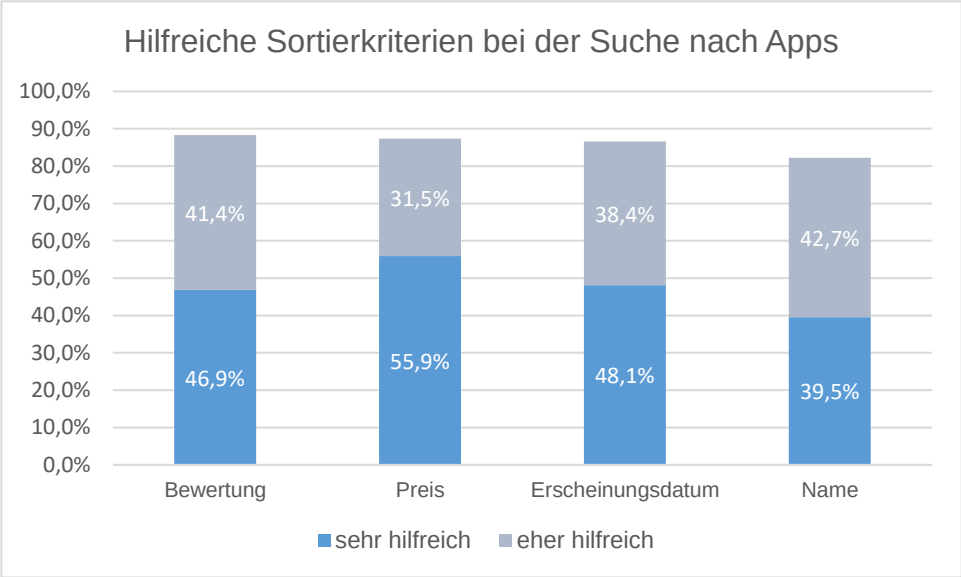


Abbildung 22: Sortierkriterien, die über 80 % der Verbraucher als sehr/eher hilfreich bewerteten

Auch eine Filterung von Suchergebnissen, die bislang nicht oder allenfalls sehr eingeschränkt möglich ist, stößt auf positive Resonanz. So bewerteten jeweils mehr als 80 Prozent der Befragten die folgenden Filterkriterien als sehr hilfreich oder eher hilfreich:

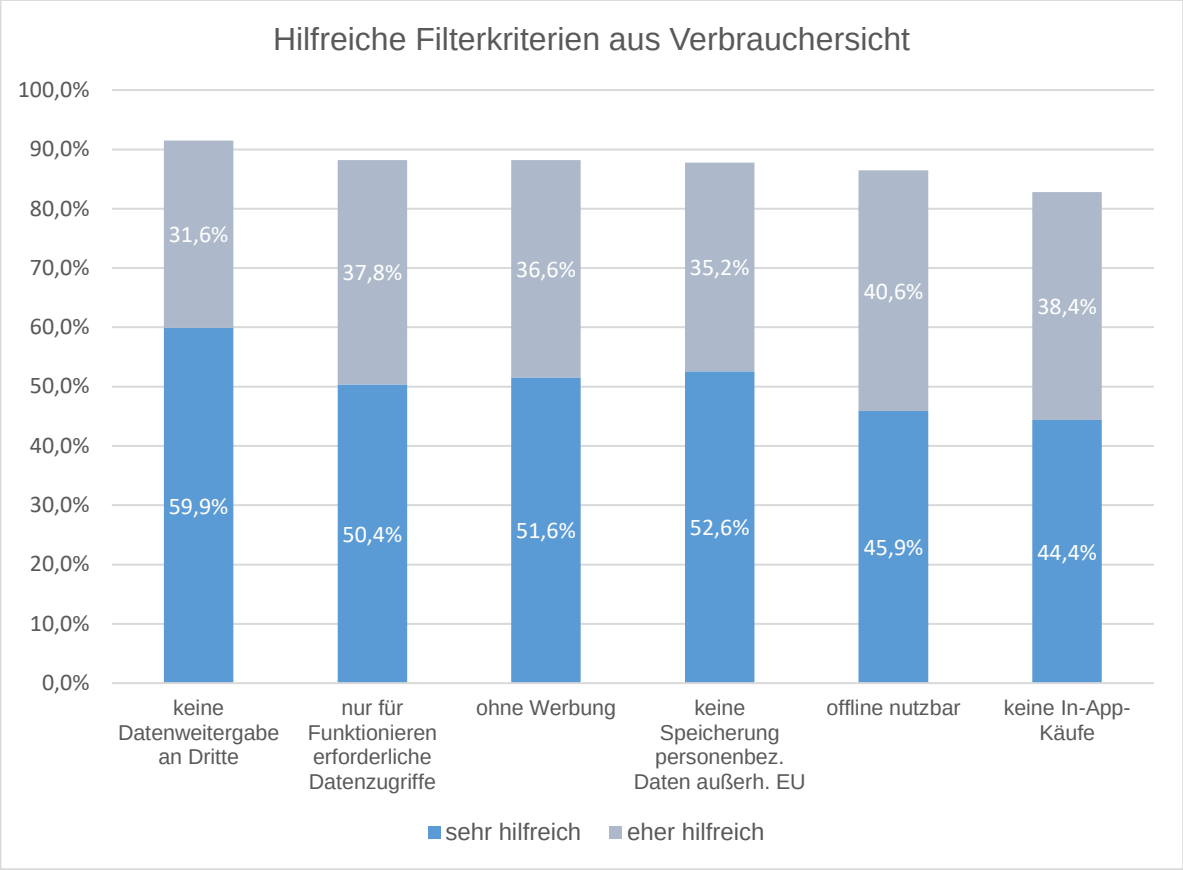


Abbildung 23: Filterkriterien, die über 80 % der Verbraucher als sehr/eher hilfreich bewerteten

1. Ermittlungen

Suchen Smartphone-Nutzer nach einer bestimmten populären App (z. B. *TikTok*) und geben sie den entsprechenden Suchbegriff im App-Store ein, so finden sie die App in aller Regel unter den ersten Treffern. Komplizierter gestaltet sich hingegen die Suche, wenn der Nutzer noch keine bestimmte App im Auge hat, sondern diese anhand verschiedener Kriterien auswählen möchte.

a) Google Play

Gibt man im Suchfeld von *Googles* App-Store *Google Play* ein Stichwort ein (z. B. *Browser*), so erhält man eine lange vertikale Ergebnisliste von Apps, wobei je nach Größe des Smartphone-Bildschirms im Regelfall sechs bis acht Apps (bei Tablets neun bis zwölf) je Seite angezeigt werden. Die Ergebnisliste enthält zu Beginn zumeist ein oder zwei Werbeanzeigen, die erkennbar als „Anzeige“ oder „Werbeanzeige“ gekennzeichnet sind. Mutmaßlich in Abhängigkeit von dem hierfür entrichteten Entgelt sind diese an erster oder zweiter Stelle der Ergebnisliste platziert und können etwas mehr Raum einnehmen als die Darstellung der sonstigen aufgelisteten Apps. Die Ergebnisliste wird unterbrochen durch horizontale Reihen von Apps, die mit „Werbeanzeigen – Passend zu deiner Suche“ oder „Empfehlungen für Dich“ überschrieben sind. Die Ergebnisliste

wird ferner unterbrochen durch einen Block „Ähnliche Suchanfragen“. Je nach eingegebenem Suchwort kann die Ergebnisliste sehr lang ausfallen. Hier ein Beispiel für „Sudoku“:

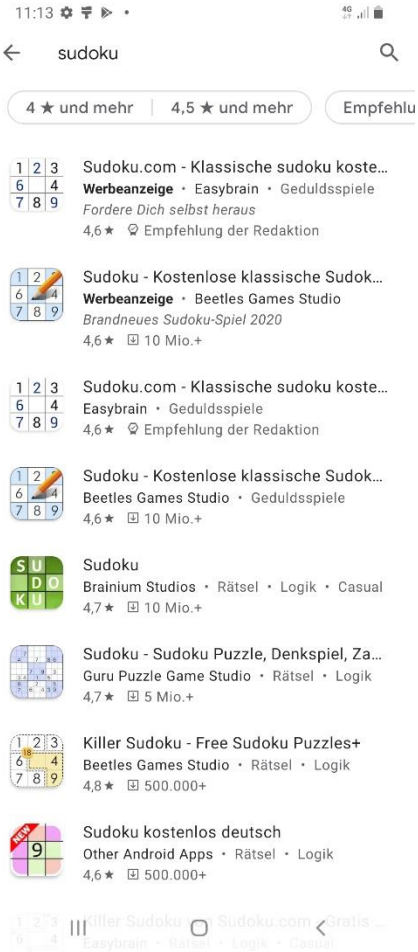


Abbildung 24: Screenshot der ersten Suchergebnisseite für das Stichwort *Sudoku* in *Google Play*

Eine vollständige Darstellung der Suchergebnisliste findet sich in Anhang 1.

Eine Sortiermöglichkeit (etwa alphabetische Reihenfolge, auf-/absteigender Preis o. Ä.) wird auf *Google Play* nicht angeboten. Als Filtermöglichkeiten stehen in der Regel die Optionen

- „4,5 Sterne und mehr“,
- „4 Sterne und mehr“,
- „Premium“ (kostenpflichtige Apps),
- „Neu“ und
- „Play Pass“

zur Verfügung. Während daneben häufig die Filteroption „Empfehlungen“ angeboten wird, ist die „Offline“-Filtermöglichkeit eher selten anzutreffen.[80]

b) App Store (Apple)

Auch beim App-Store von *Apple* erhält man bei Eingabe eines Suchbegriffs eine lange vertikal aufgebaute Ergebnisliste, an deren Anfang zumeist eine mit „Ad“ (englisch für „Werbung“) gekennzeichnete App vor blauem Hintergrund präsentiert wird. Im Gegensatz zur Darstellung bei *Google Play* werden auf den Ergebnisseiten je nach Bildschirmgröße des iPhones nur zwei bis drei Apps angezeigt (auf einem iPad in der Regel sechs). Die entsprechenden Darstellungen enthalten dafür bis zu drei Screenshots, die auch animiert sein können. Mitunter wird die Ergebnisliste unterbrochen durch eine mit großem Bild versehene sog. „Story“, bei deren Anklicken eine App zumeist unter Verwendung weiterer Bilder oder Videosequenzen ausführlich dargestellt und zum Download angeboten wird. Mitunter werden diese Apps dann als „App des Tages“ oder „Spiel des Tages“ bezeichnet.[81] In die Ergebnisliste sind zudem „Sammlungen“ eingebettet. Hierbei handelt es sich um themenverwandte App-Listen, die in der Ergebnisliste zunächst auszugsweise und bei Anklicken vollumfänglich angezeigt werden.

---

80 Zwar ist es auch möglich, dem Suchbegriff das Stichwort „offline“ hinzuzufügen, die entsprechende Suchergebnisliste kann je nach Suchbegriff dennoch überwiegend Apps enthalten, die nicht offline nutzbar sind. Teilweise sind auch mit dem Tag „Offline“ versehene Apps tatsächlich nicht offline nutzbar.

81 Diverse Internetquellen weisen darauf hin, dass eine Listung als „App des Tages” gerade für weniger bekannte Apps einen enormen Zuwachs an Downloads mit sich bringen kann, s. etwa *Blacker*, What Getting Featured in The New App Store Could Mean For You (Apptopia, 24.10.2017), abrufbar unter https://blog.apptopia.com/new-app-stores-app-of-the-day-gets-an-average-download-boost-of-1747.

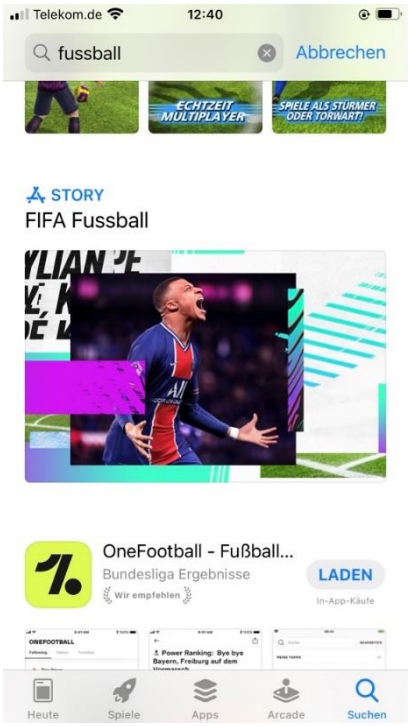


Abbildung 25: Anzeige „Story“ in der App-Suchergebnisliste (*iOS*)

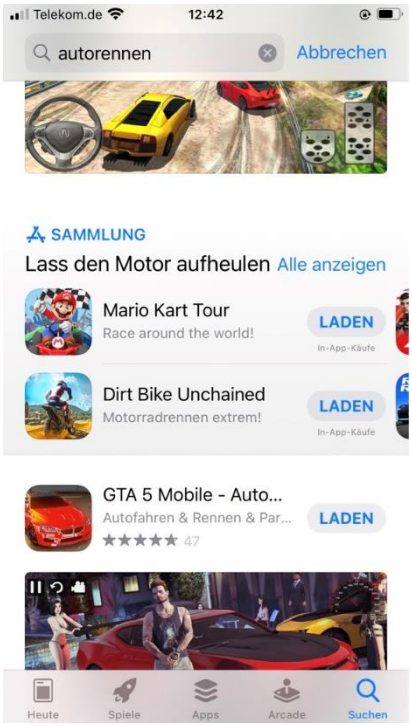


Abbildung 26: Anzeige „Sammlung“ in der App-Suchergebnisliste (*iOS*)

Zur Veranschaulichung wurde auch hier eine Suche mit dem Stichwort „Sudoku“ durchgeführt:

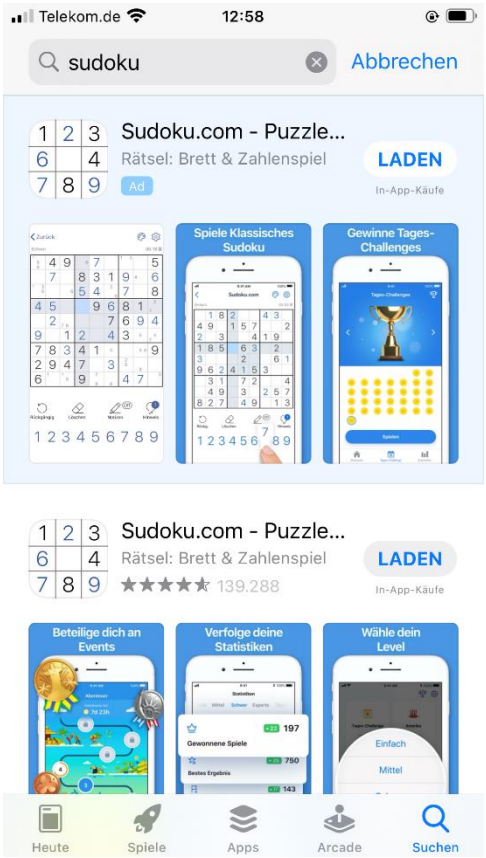


Abbildung 27: Screenshot der ersten Suchergebnisseite für das Stichwort *Sudoku* im App-Store von *Apple*

Eine vollständige Darstellung der Suchergebnisliste findet sich in Anhang 2.

Im Gegensatz zu *Google Play* besteht beim App-Store von *Apple* weder eine Sortiermöglichkeit noch eine Möglichkeit, die ausgegebenen Suchergebnisse zu filtern.

2. Würdigung

Weder *Google* noch *Apple* erklären in ihren App-Stores, nach welchen Kriterien Suchergebnisse gelistet werden. Eine eigene Sortierung von Ergebnislisten durch den Nutzer wird nicht angeboten. Filter werden von *Apple* gar nicht und von *Google* nur in geringem Umfang angeboten. Während für die Reihung von Suchergebnissen mittlerweile unterschiedliche rechtliche Anforderungen formuliert wurden, ist die Zurverfügungstellung von Suchfiltern bislang nicht speziell reglementiert.

a) Darstellung von Suchergebnislisten

Es gibt verschiedene gesetzliche Regelungen, die eine größere Transparenz von Suchalgorithmen bzw. bei der Darstellung von Suchergebnissen bewirken sollen.

aa) Anforderungen der P2B-Verordnung von 2019

Rechtliche Vorgaben zu Auswahl und Offenlegung von Rankingparametern ergeben sich zunächst aus der sog. „Platform to Business"- oder kurz „P2B"-Verordnung.[82] Diese gilt seit dem 12. Juli 2020 und soll sicherstellen, dass für gewerbliche Nutzer[83] von Online-Vermittlungsdiensten und Nutzer mit Unternehmenswebsite eine angemessene Transparenz, Fairness und wirksame Abhilfemöglichkeiten geschaffen werden. In diesem Zusammenhang stellen sich eine Reihe von Fragen, wie etwa nach der generellen Anwendbarkeit der P2B-Verordnung auf die

82 Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten, ABl. EU vom 11.07.2021, S. 57, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R1150 (im Folgenden „P2B-Verordnung").

83 In diesem Zusammenhang ist ausschließlich derjenige gemeint, dessen Produkte oder Dienstleistungen über die Plattform angeboten werden, hier also der App-Publisher. Nicht erfasst ist hingegen der gewerbliche Endabnehmer, also hier der gewerbliche App-Nutzer.

App-Stores von *Google* und *Apple*[84] oder danach, ob die Rankingkriterien für Entwickler auch vor Vertragsschluss hinreichend verfügbar[85] sind. Die P2B-Verordnung schützt aber in erster Linie nicht die Verbraucher, sondern die gewerblichen Nutzer, die ihre Waren und Dienstleistungen bei den genannten Vermittlungsdiensten anbieten wollen. Diesen gegenüber muss der Anbieter von Online-Vermittlungsdiensten in seinen Allgemeinen Geschäftsbedingungen die das Ranking bestimmenden Hauptparameter und die Gründe für die relative Gewichtung dieser Hauptparameter gegenüber anderen Parametern darstellen (Art. 5 Abs. 1 P2B-VO). Setzte der Online-Vermittlungsdiensteanbieter diese Vorgaben nicht nur in AGB um, sondern darüber hinaus, wie dies Art. 5 Abs. 2 P2B-VO vorsieht (klare und verständlich formulierte Erläuterungen, die öffentlich und leicht verfügbar sind), so könnten hiervon natürlich auch die Nutzer auf der Abnehmerseite profitieren. Die genannte Vorschrift gilt allerdings nur für allgemeine Online-Suchmaschinen, darüber hinaus besteht gerade keine entsprechende Verpflichtung zur Anzeige von Sortierkriterien im Zusammenhang mit der Darstellung anderweitiger Suchergebnislisten, die dem Verbraucher angezeigt werden. Auf die einzelnen Anforderungen der P2B-Verordnung wird daher an dieser Stelle nicht weiter eingegangen.

---

84 Ginge man davon aus, dass die App-Stores von *Google* bzw. *Apple* im Hinblick auf die Zurverfügungstellung von Apps zum Download selbst Vertragspartner der Endabnehmer sind, läge streng genommen insoweit kein Vermittlungsverhältnis für direkte Transaktionen zwischen Endabnehmer und einem nicht zum Plattformbetreiber gehörenden Unternehmen vor, wie es Art. 2 Nr. 2 lit. b) der P2B-Verordnung explizit als Voraussetzung für das Vorliegen eines Online-Vermittlungsdienstes fordert. Nach Sinn und Zweck der P2B-Verordnung sollen indessen Dreiparteien-Konstellationen erfasst werden, in denen die das Angebot präsentierende Partei wesentlichen Einfluss auf dessen Absatzchancen ausübt. Dies legt eine Anwendung auf die App-Stores von *Google* und *Apple* zumindest nahe. Auch geht Erwägungsgrund 11 der P2B-Verordnung explizit davon aus, dass Vertriebsplattformen für Softwareanwendungen (in der englischen Fassung „application stores“) unter die P2B-Verordnung fallen sollen. Ferner enthalten die hierzu ergangenen Leitlinien der Kommission (Leitlinien zur Transparenz des Rankings gemäß der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates (2020/C424/01), ABl. EU C424 vom 08.12.2020, S. 1, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020XC1208(01)&from=EN) zahlreiche Beispiele zur Veranschaulichung, von denen einige auch die Darstellung in App-Stores enthalten. Für *Google* könnte in diesem Zusammenhang bei der Einordnung als Online-Vermittlungsdienst (zumindest gegenüber App-Publishern) auch eine Rolle spielen, dass sich das Unternehmen gerade in seiner Vertriebsvereinbarung für Entwickler im Hinblick auf das Vertragsverhältnis zum Endkunden als bloßer Vertreter bezeichnet.

85 Soweit ersichtlich stellt *Apple* betreffende Informationen nicht frei zugänglich zur Verfügung, so dass die Anforderung des Artikels 3 Absatz 1 lit. b) der P2B-Verordnung nicht erfüllt wäre. *Google* stellt zumindest auf Supportseiten einschlägige Informationen bereit, s. https://support.google.com/google-play/Android-developer/answer/9958766?hl=de, https://support.google.com/googleplay/Android-developer/answer/4448378?hl=de.

bb) Anforderungen der Omnibus-Richtlinie von 2019

Im Verhältnis zum Verbraucher, hier also dem App-Nutzer, werden Anforderungen an die Rankingtransparenz in der sog. Omnibus-Richtlinie[86] geregelt. Die Vorgaben dieser Richtlinie sind bis zum 28. November 2021 in nationales Recht umzusetzen und müssen ab dem 28. Mai 2022 in den Mitgliedstaaten verbindlich gelten. Der deutsche Gesetzgeber ist dem mit dem Gesetz zur Stärkung des Verbraucherschutzes im Wettbewerbs- und Gewerberecht nachgekommen, welches zum 28. Mai 2022 in Kraft treten wird.[87]

Die Richtlinie modifiziert eine Vielzahl verbraucherschützender Richtlinien, darunter die Richtlinien über Preisangaben (98/6/EG[88]), unlautere Geschäftspraktiken (2005/29/EG – UGP-Richtlinie[89]) und über die Rechte der Verbraucher (2011/83/EU – Verbraucherrechte-Richtlinie[90]). Die Omnibus-Richtlinie sieht in Artikel 3 Nr. 4b) folgende (klarstellende) Ergänzung der Irreführungstatbestände der UGP-Richtlinie vor (umgesetzt in § 5b Abs. 2 UWG n. F.):

---

86 Richtlinie (EU) 2019/2161 des Europäischen Parlaments und des Rates vom 27. November 2019 zur Änderung der Richtlinie 93/13/EWG des Rates und der Richtlinien 98/6/EG, 2005/29/EG und 2011/83/EU des Europäischen Parlaments und des Rates zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union, ABl. EU L328 vom 18.12.2019, S. 7, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L2161 (im Folgenden „Omnibus-Richtlinie“).

87 Zum Redaktionsschluss des vorliegenden Berichts war das Gesetz noch nicht im Bundesgesetzblatt veröffentlicht.

88 Richtlinie 98/6/EG des Europäischen Parlaments und des Rates vom 16. Februar 1998 über den Schutz der Verbraucher bei der Angabe der Preise der ihnen angebotenen Erzeugnisse, ABl. EU L80 vom 18.03.1998, S. 27, abrufbar unter https://eur-lex.europa.eu/resource.html?uri=cellar:b8fd669f-e013-4f8a-a9e1-2ff0dfee7de6.0004.02/DOC_1&format=PDF.

89 Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates vom 11. Mai 2005 über unlautere Geschäftspraktiken im binnenmarktinternen Geschäftsverkehr zwischen Unternehmen und Verbrauchern und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken), ABl. EU L149 vom 11.06.2005, S. 22, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32005L0029&from=DE (im Folgenden „UGP-Richtlinie“).

90 Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates, ABl. EU L304 vom 22.11.2011, S. 64, abrufbar unter https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:304:0064:0088:de:PDF (im Folgenden: „Verbraucherrechte-Richtlinie“). Das Gesetz zur Umsetzung der Verbraucherrechte-Richtlinie und zur Änderung des Gesetzes zur Wohnungsvermittlung ist am 13.06.2014 in Deutschland in Kraft getreten.

> „Wenn Verbrauchern die Möglichkeit geboten wird, mithilfe eines Stichworts, einer Wortgruppe oder einer anderen Eingabe nach Produkten zu suchen, die von verschiedenen Gewerbetreibenden oder von Verbrauchern angeboten werden, gelten, unabhängig davon, wo Rechtsgeschäfte letztendlich abgeschlossen werden, allgemeine Informationen, die die Hauptparameter für die Festlegung des Rankings der dem Verbraucher im Ergebnis der Suche vorgeschlagenen Produkte, sowie die relative Gewichtung dieser Parameter im Vergleich zu anderen Parametern, betreffen und die in einem bestimmten Bereich der Online-Benutzeroberfläche zur Verfügung gestellt werden, der von der Seite, auf der die Suchergebnisse angezeigt werden, unmittelbar und leicht zugänglich ist, als wesentlich."

Die Einstufung als „wesentliche Informationen" führt dazu, dass bereits nach dem Gesetzeswortlaut eine wettbewerbswidrige irreführende Unterlassung anzunehmen ist, wenn die betreffenden Informationen zu Rankings nicht angegeben werden.

Zudem wurde ein neuer Artikel 6a in die Verbraucherrechte-Richtlinie eingefügt, durch den die Betreiber von Online-Marktplätzen insbesondere verpflichtet werden, Verbrauchern vor dem Abschluss eines Fernabsatzvertrags allgemeine Informationen zu den Hauptparametern zur Festlegung eines Rankings sowie der relativen Gewichtung von Rankingkriterien zur Verfügung zu stellen. Ebenso wie die P2B-Verordnung geht die Omnibus-Richtlinie von der Prämisse aus, dass die Anbieter nicht verpflichtet sein sollen, die Funktionsweise ihrer Ranking-Systeme, einschließlich der Algorithmen, im Detail offen zu legen. Eine allgemeine Erläuterung der Parameter und ihrer Gewichtung wird als ausreichend angesehen.[91] Umgesetzt wird der neue Artikel 6a der Verbraucherrichtlinie in Art. 246d § 1 des EGBGB n. F.[92]

Rankingparameter zeigen derzeit weder *Google* noch *Apple* bei ihren Suchergebnislisten an. Dies müsste sich bis zum 28. Mai 2022, dem Datum des Inkrafttretens des novellierten UWG, ändern. Erst ab diesem Zeitpunkt wäre eine fehlende Angabe von Rankingparametern als Rechtsverstoß zu qualifizieren. Vorab wäre indessen auch hier abschließend zu klären, ob die App-Stores von *Google* bzw. *Apple* als Online-Marktplätze zu qualifizieren sind (Art. 246d § 1

---

91 Vgl. Erwägungsgründe 22 f. der Omnibus-Richtlinie (Fn. 86).

92 S. dazu Art. 2 des Gesetzes zur Änderung des Bürgerlichen Gesetzbuchs und des Einführungsgesetzes zum Bürgerlichen Gesetzbuche in Umsetzung der EU-Richtlinie zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union und zur Aufhebung der Verordnung zur Übertragung der Zuständigkeit für die Durchführung der Verordnung (EG) Nr. 2006/2004 auf das Bundesministerium der Justiz und für Verbraucherschutz, das ebenfalls zum 28.05.2022 in Kraft treten soll. Zum Redaktionsschluss des vorliegenden Berichts war das Gesetz noch nicht im Bundesgesetzblatt veröffentlicht.

EGBGB n. F.)[93] bzw. ein Unternehmer Verbrauchern die Möglichkeit einräumt, nach Waren oder Dienstleistungen zu suchen, die von verschiedenen Unternehmern oder von Verbrauchern angeboten werden (§ 5b Abs. 2 UWG n. F.).

Die Richtlinie enthält insbesondere auch Vorgaben dazu, dass Verbraucher in kurzer, einfach zugänglicher und verständlicher Weise darüber informiert werden, wenn ein Gewerbetreibender den Anbieter einer Online-Suchfunktion unmittelbar oder mittelbar dafür bezahlt hat, dass ein Produkt im Rahmen der Suchergebnisse ein höheres Ranking erhält.[94] Zu diesem Zweck wird gemäß Artikel 3 Nr. 7a) der Omnibus-Richtlinie der Anhang I der UGP-Richtlinie, in dem Geschäftspraktiken aufgelistet sind, „die unter allen Umständen als unlauter gelten", um folgende Nr. 11a ergänzt[95]:

> „Anzeige von Suchergebnissen aufgrund der Online-Suchanfrage eines Verbrauchers, ohne dass etwaige bezahlte Werbung oder spezielle Zahlungen, die dazu dienen, ein höheres Ranking der jeweiligen Produkte im Rahmen der Suchergebnisse zu erreichen, eindeutig offengelegt werden."

Im Unterschied zur P2B-Verordnung müssen die Angaben zu Rankings nicht lediglich in den Allgemeinen Geschäftsbedingungen zu finden, sondern direkt auf der Nutzeroberfläche platziert sein. So heißt es in der Richtlinie, dass die Informationen „knapp gehalten und leicht, an gut sichtbarer Stelle und unmittelbar verfügbar" sein sollen.[96]

Die rechtliche Vorgabe, bezahlte Werbeeinblendungen als solche zu kennzeichnen, ist bei *Google Play* ebenso umgesetzt wie im *Apple App Store*. *Googles* fettgedruckte Angabe „Werbeanzeige" ist dabei eher geeignet, Verbrauchern den Werbecharakter der Einblendung zu verdeutlichen als *Apples* „Ad"-Kennzeichnung. Es stellt sich auch die Frage, ob die Kennzeichnung mit dem englischen „Ad" für alle deutschen Nutzer verständlich ist.[97] Man mag auch die Einblendung

---

93 Ähnlich wie beim Merkmal des Online-Vermittlungsdiensts im Rahmen der P2B-Verordnung (s. dazu oben, Fn. 84) soll ein Online-Marktplatz nur dann vorliegen, wenn dieser es ermöglicht, Fernabsatzverträge mit anderen Gewerbetreibenden (als dem Plattformbetreiber) oder Verbrauchern abzuschließen (Art. 3 Nr. 1 lit. b) Omnibus-Richtlinie, umgesetzt in § 2 Abs. 1 Nr. 6 UWG n. F.).

94 Vgl. Erwägungsgrund 20 der Omnibus-Richtlinie (Fn. 86).

95 Umgesetzt als neue Nr. 11a im Anhang zu § 3 Abs. 3 UWG (Inkrafttreten 28.05.2022).

96 Vgl. Erwägungsgrund 22 der Omnibus-Richtlinie.

97 So genügte der Hashtag #ad im Zusammenhang mit einem Influenzer-Beitrag auf Instagram dem OLG Celle nicht, um Werbung als solche zu kennzeichnen, s. OLG Celle, Urt. v. 08.06.2017, Az. 13 U 53/17 – juris.

der „Story“ und der „Sammlung“[98] für problematisch halten; je mehr hier jedoch eine klare optische Abgrenzung zur Suchergebnisliste erfolgt, desto weniger dürften die betreffenden Einschübe von Verbrauchern als Teil des Rankings wahrgenommen werden.[99]

cc) Anforderungen aus der bisherigen Rechtsprechung

Auch die Gerichte haben sich bereits mit den Anforderungen an die Rankingtransparenz beschäftigt. Diese Rechtsprechung betrifft dabei in erster Linie Vergleichs- und Bewertungsportale, kann aber – da letztlich auch dort die Präsentation von Suchergebnissen in Fokus steht – auch für App-Stores Bedeutung entfalten.[100] So entschied etwa der Bundesgerichtshof (BGH) im Jahr 2017 in einem Grundsatzurteil, Vergleichsportale seien nach dem UWG dazu verpflichtet, transparent offenzulegen, ob sie nur Anbieter listeten, von denen sie eine Provision erhielten.[101] In seinem *Yelp*-Urteil[102] lehnte der BGH eine deliktsrechtliche Haftung der Vergleichsplattform ab und billigte die Praxis *Yelps*, bestimmte Bewertungen eines Unternehmens besonders hervorzuheben und andere gar nicht in die Bewertung mit einzubeziehen. Die von einem Bewertungsalgorithmus vorgenommene Kategorisierung nach „empfohlenen“ und „nicht empfohlenen“ Bewertungen (wobei nur empfohlene Bewertungen in eine Gesamtbewertung einflossen) sei auch ohne eine Offenlegung der Funktionsweise des Algorithmus für den Nutzer hinreichend transparent. Erwähnenswert ist schließlich ein Urteil des LG Hamburg aus dem Jahr 2020.[103] Der *vzbv* hatte gegen den Reisevermittler *Opodo Ltd.* geklagt. Hier bemängelte das Gericht unter lauterkeitsrechtlichen Gesichtspunkten, dass Rankingparameter zwar genannt, jedoch keinerlei Hinweise darauf zu finden waren, wie diese Parameter in die Gesamtbewertung eingingen.[104] Auch lasse *Opodos* Liste

98 S. dazu Abbildung 25 und Abbildung 26 auf S. 43.

99 Soweit ersichtlich, wählt *Apple* Apps des Tages sowie in speziellen Sammlungen enthaltene Apps redaktionell aus und erhält hierfür kein Entgelt, sodass insoweit keine ggf. verbotene versteckte Werbung vorliegt.

100 Im *jameda*-Urteil (BGH, Urteil vom 20.02.2018, Az. VI ZR 30/17, juris) entschied der BGH, dass das Ärztebewertungsportal jameda.de zwar grundsätzlich eine von der Rechtsordnung gebilligte und gesellschaftlich erwünschte Funktion wahrnehme, das Unternehmen aber seine Stellung als neutraler Informationsmittler nicht verlassen dürfe, ohne dies dem Internetnutzer hinreichend offenzulegen. In diesem Verfahren waren jedoch im Kern grundrechtliche Fragen (insbesondere der informationellen Selbstbestimmung) betroffen, so dass die Entscheidung im Hinblick auf die Darstellung ausschließlich kommerzieller Informationen nur einen sehr beschränkten Leitbildcharakter aufweist.

101 BGH, Urteil vom 27.04.2017, Az. I ZR 55/16, juris.

102 BGH, Urteil vom 14.01.2020, Az. VI ZR 495/18, juris.

103 LG Hamburg, Urteil vom 23.04.2020, Az. 324 O 234/19, juris; vorgehend LG Hamburg, (Versäumnis-)Urteil vom 07.11.2019, Az. 327 O 234/19, juris.

104 LG Hamburg, Urteil vom 23.04.2020, Az. 324 O 234/19, juris Rn. 29.

mit sog. „Top-Tipps“, die in einer Reihe mit anderen Auflistungsrubriken gestanden habe, eine Kennzeichnung als Werbung vermissen.[105]

Soweit ersichtlich gibt es bislang keine Entscheidung zur kommentarlosen Anzeige von Suchergebnissen. Man kann auf der Grundlage der dargestellten Rechtsprechung jedoch davon ausgehen, dass bereits jetzt – noch vor Inkrafttreten der entsprechenden neuen „schwarzen Klausel“ in Nr. 11a im Anhang zu § 3 Abs. 3 UWG zum 28. Mai 2022 – jedenfalls dann von einer für Verbraucher wesentlichen Information auszugehen ist, wenn die Darstellung von Suchergebnissen von Provisionszahlungen beeinflusst wird. Dies gilt für die allgemeine Darstellung von Suchergebnislisten ebenso wie – wie im Fall *Opodo* – für eine gefilterte Darstellung („Top Tipps“). Sollten demnach Provisionszahlungen beim Ranking eine Rolle spielen, sei es bei der allgemeinen App-Suchergebnisliste oder bei der Auflistung von „Empfehlungen“, so wäre in der unterbliebenen Kennzeichnung ein Verstoß gegen § 3 Abs. 1 i. V. m. § 5a Abs. 2 UWG zu sehen.

b) Individuelle Anpassbarkeit von Suchergebnislisten

Soweit ersichtlich, gibt es derzeit keine spezifischen rechtlichen Vorgaben dahingehend, inwieweit Suchergebnislisten individuell anpassbar sein müssen. Es steht jedoch außer Frage, dass Verbraucher eine individuelle Anpassbarkeit von Suchergebnislisten wünschen, wie auch die Befragung des Bundeskartellamts ergeben hat (siehe oben[106]).

In Anbetracht der Tatsache, dass auch gesetzgeberische Vorgaben – schon aus Gründen des Schutzes von Geschäftsgeheimnissen und zur Vermeidung der Manipulation von Suchergebnislisten – niemals zu einer vollständigen Transparenz der Sortierkriterien führen werden, kommt deren individueller Anpassbarkeit eine große Bedeutung zu. Entsprechende Möglichkeiten der Verbraucher zur Filterung bzw. Sortierung der Suchergebnisse nach bestimmten Kriterien gehören bei klassischen Vergleichsportalen – beispielsweise für die Suche nach einem Hotel, einer Versicherung oder einem Stromanbieter – heute zum Standard.

III. Informationen vor dem App-Download

Verbraucherrechtliche Probleme können sich insbesondere daraus ergeben, dass App-Nutzer Informationen nicht oder nicht in einer Form erhalten, die leicht verständlich ist und eine zügige Kenntnisnahme ermöglicht. Dieses Problem betrifft nicht nur die ggf. umfangreiche Vorinstallation von Apps und die Suche nach einer App, sondern vor allem die Situation vor dem Download einer App.

---

105 LG Hamburg, Urteil vom 23.04.2020, Az. 324 O 234/19, juris Rn. 30.

106 S. Abbildung 22 auf S. 39 und Abbildung 23 auf S. 40.

1. Datenschutzbestimmungen und Nutzungsbedingungen der App-Stores

Will der Nutzer den App-Store von *Apple* bzw. *Google* benutzen, muss er zuvor deren Nutzungsbedingungen akzeptieren und Datenschutzerklärungen zur Kenntnis nehmen.[107] Eine Nutzung von *Google Play* setzt die Akzeptanz der *Google*-Play- sowie der allgemeinen *Google*-Nutzungsbedingungen sowie der allgemeinen Datenschutzerklärung von *Google* voraus. Für eine Nutzung des *Apple App Store* sind die Bedingungen der *Apple Media Services* einschließlich des Abschnitts „G. Zusätzliche Bedingungen für den App Store (mit Ausnahme von *Apple* Arcade-Apps)" sowie die Datenschutzerklärungen „App Store & Datenschutz" und die allgemeine *Apple*-Datenschutzrichtlinie einschlägig. Eine tiefergehende Prüfung der Nutzungs- und Datenschutzbestimmungen von *Google* bzw. *Apple* würde den Rahmen dieses Berichts sprengen. Allerdings ist im Rahmen der Sektoruntersuchung zutage getreten, dass Vorgaben des Kammergerichts Berlin aus gerichtlichen Auseinandersetzungen der Vergangenheit um die betreffenden Texte nicht vollständig umgesetzt worden sind. So stellte im Jahr 2013 das Landgericht Berlin in gleich zwei Urteilen die Unwirksamkeit verschiedener Klauseln in den Nutzungsbedingungen, der Datenschutzerklärung und der „Vereinbarungen über die Nutzung eines Marktplatzes" von *Google* sowie der Datenschutzrichtlinie von *Apple* fest.[108] Das Kammergericht Berlin bestätigte (in Bezug auf *Apple* zumindest teilweise) 2018[109] bzw. 2019[110] die in den erstinstanzlichen Urteilen festgestellte Unwirksamkeit der Klauseln.[111] Die Gerichte hielten insgesamt 25 Klauseln in *Googles* Bestimmungen und sieben Klauseln in *Apples* Datenschutzrichtlinie wegen Verstoßes gegen das AGB-Recht für unwirksam. Die Unwirksamkeit der Klauseln in den Datenschutzerklärungen ergab sich dabei vorwiegend aus einer unangemessenen Benachteiligung der Nutzer, da die Klauseln mit wesentlichen Grundgedanken der DSGVO nicht zu vereinbaren waren (§ 307 Abs. 1 S. 1, Abs. 2 Nr. 1 BGB).

Obgleich sowohl *Google* als auch *Apple* mittlerweile Änderungen an den entsprechenden Klauseln vornahmen, bleiben einige dieser geänderten Klauseln aus Sicht des Bundeskartellamts

---

107 Da bei der Ersteinrichtung von *Google Android* ebenso wie bei der Erstnutzung von *Google Play* die Schaltfläche „Akzeptieren" bzw. „Ich stimme zu" jeweils unterhalb der des Hinweises, wie *Google* mit Nutzerdaten umgeht, platziert ist, spricht sogar einiges dafür, dass der Nutzer um eine ausdrückliche Zustimmung zur Datenschutzerklärung ersucht wird.

108 LG Berlin, Urteil vom 30.04.2013, Az. 15 O 92/12 (*Apple*), juris; LG Berlin, Urteil vom 19.11.2013, Az. 15 O 402/15 (*Google*), juris.

109 KG Berlin, Urteil vom 27.12.2018, Az. 23 U 196/13 (*Apple*), juris.

110 KG Berlin, Urteil vom 21.03.2019, Az. 23 U 268/13 (*Google*), juris.

111 Das KG Berlin stellte in seinen Urteilen jeweils auf die Rechtslage im Entscheidungszeitpunkt ab und zog die bereits geltende und anwendbare DSGVO zur Bewertung der unangemessenen Benachteiligung der Verbraucher heran. Die Vorinstanz hatte noch das BDSG angewendet.

weiterhin verbesserungsbedürftig. Beispielsweise stellte das Kammergericht die Unwirksamkeit einer Klausel in *Googles* Datenschutzerklärung fest, die die Weitergabe personenbezogener Daten an außerhalb von *Google* stehende Dritte dann erlaubt, wenn *Google* „nach Treu und Glauben davon ausgehen" darf, dass der Zugriff auf diese Daten oder ihre Nutzung, Aufbewahrung oder Weitergabe vernünftigerweise notwendig ist, um z. B. Betrug, Sicherheitsmängel oder technische Probleme aufzudecken, zu verhindern oder zu bekämpfen. Das Kammergericht monierte bei dieser Klausel zum einen, dass sie an *Googles* subjektive Einschätzung, nicht aber an objektive Voraussetzungen anknüpfe.[112] Zum anderen fiele das oben genannte Beispiel der Aufdeckung, Verhinderung oder Bekämpfung von Betrug, Sicherheitsmängeln oder technischen Problemen nicht generell und ohne Berücksichtigung entgegenstehender Interessen des Betroffenen unter den Erlaubnistatbestand des Art. 6 Abs. 1 S. 1 lit. f)[113] DSGVO. Vielmehr sei stets eine Einzelfallentscheidung vorzunehmen, sodass die von *Google* verwendete Klausel unwirksam sei.[114] *Google* nahm mittlerweile zwar Anpassungen an dieser Klausel vor, änderte jedoch die Anknüpfung an die subjektive Einschätzung „nach Treu und Glauben" nicht. Zudem wurde das Erfordernis einer Entscheidung im Einzelfall unter Berücksichtigung der Interessen des Betroffenen nicht in die Klausel eingefügt.[115] Darüber hinaus fallen in *Googles* Datenschutzbestimmungen weitere Klauseln auf, die die durch das Kammergericht festgestellten Verstöße nicht beseitigen, sondern den Wortlaut der beanstandeten Klauseln im Wesentlichen übernehmen.[116]

Ähnlich stellt sich die Situation im Hinblick auf einige aktualisierte Bestimmungen in *Apples* Datenschutzrichtlinie dar. Das Kammergericht hielt unter anderem eine Klausel für unwirksam, nach der *Apple* und seine verbundenen Unternehmen personenbezogene Daten untereinander austauschen und sie mit anderen Informationen zur Produktverbesserung und zu Werbezwecken verbinden durften. Die dort bestimmte Datenverarbeitung finde ohne Einwilligung des Nutzers statt und sei zudem nicht für die Erfüllung des Vertrags erforderlich (Art. 6 Abs. 1 S. 1 lit. b) DSGVO). Die Tatbestände des Art. 6 Abs. 1 S. 1 lit. c) bis f) DSGVO kämen von vornherein schon

---

112 KG Berlin (Fn. 110), juris Rn. 136, 139.

113 Im Urteil des KG Berlin (Fn. 110), juris Rn. 139, wird Art. 6 Abs. 1 S. 1 lit. c) DSGVO genannt, wobei es sich aber offensichtlich um einen Tippfehler handelt.

114 KG Berlin (Fn. 110), juris Rn. 139 f.

115 S. *Google*-Datenschutzerklärung mit Wirksamkeit ab 04.02.2021, abrufbar unter https://www.gstatic.com/policies/privacy/pdf/20210204/3jla0xz1/*Google*_privacy_policy_de_eu.pdf, unter dem Punkt „Datenweitergabe durch *Google* aus rechtlichen Gründen".

116 Z. B. Klausel zur Weitergabe von Daten bei Unternehmenszusammenschluss, -erwerb oder Verkauf von Vermögensgegenständen, s. *Google*-Datenschutzerklärung (Fn. 115) unter dem Punkt „Datenweitergabe durch *Google* aus rechtlichen Gründen", letzter Abschnitt; Klausel zur einseitigen Änderung der Datenschutzbestimmungen, s. *Google*-Datenschutzerklärung (Fn. 115), „Änderungen an dieser Datenschutzerklärung".

nicht in Betracht.[117] Es liege somit ein Verstoß gegen Art. 6 DSGVO vor, der zu einer unangemessenen Benachteiligung des Nutzers nach § 307 Abs. 1 S. 1, Abs. 2 Nr. 1 BGB führe.[118] Dieser Kritikpunkt wird auch durch eine von *Apple* durchgeführte Änderung der betreffenden Klausel nicht beseitigt. Zwar wird zu Beginn des Abschnitts „Verwendung personenbezogener Daten durch *Apple*“ erwähnt, dass *Apple* nur personenbezogene Daten verwende, wenn eine gültige rechtliche Grundlage bestehe. Allerdings räumt sich *Apple* im Folgenden das Recht ein, personenbezogene Daten zu erheben, die zur Bereitstellung seiner Dienste erforderlich sind.[119] Als Beispiele werden unter anderem Daten zur Produktverbesserung und Angebotspersonalisierung genannt. Auffällig ist dabei die Orientierung am Wortlaut des Art. 6 Abs. 1 S. 1 lit. b) DSGVO („zur Bereitstellung unserer Dienste erforderlich“), die suggeriert, dass *Apple* trotz gegenteiliger Ansicht des Kammergerichts weiterhin daran festhält, eine solche Datenverarbeitung sei auch ohne Einwilligung des Nutzers auf Grundlage des Art. 6 Abs. 1 S. 1 lit. b) DSGVO zulässig. Jedenfalls aber macht *Apple* nicht deutlich, dass eine solche Datenverarbeitung nur auf Grundlage einer vorherigen Einwilligung des Nutzers zulässig ist.

Als weiteres Beispiel für eine nicht erfolgte Umsetzung des Urteils ist die Klausel zur Weitergabe personenbezogener Daten durch *Apple* zu nennen. Das Kammergericht hat bei dieser Klausel ebenfalls ein Vorliegen der Erlaubnistatbestände des Art. 6 Abs. 1 S. 1 lit. b) bis f) DSGVO verneint.[120] In der aktuellen Version dieser Klausel ist aber nicht ersichtlich, auf welche Rechtsgrundlage sich *Apple* für die Datenweitergabe stattdessen stützt, insbesondere wird nicht auf die Einholung einer Einwilligung eingegangen.[121] Diese nur kursorische Analyse der aktualisierten Datenschutzbestimmungen zeigt, dass weiterhin Verbesserungsbedarf bei *Google* und *Apple* besteht, um den Anforderungen der DSGVO und – jedenfalls nach Auffassung des Kammergerichts – auch des AGB-Rechts gerecht zu werden.

---

117 KG Berlin (Fn. 109), juris Rn. 41 ff.

118 KG Berlin (Fn. 109), juris Rn. 39.

119 S. *Apple*-Datenschutzrichtlinie (Stand 01.06.2021), abrufbar unter https://www.apple.com/legal/privacy/pdfs/apple-privacy-policy-de-ww.pdf, unter dem Punkt „Verwendung personenbezogener Daten durch *Apple* – Bereitstellung unserer Dienste“.

120 KG Berlin (Fn. 109), juris Rn. 41 ff.

121 S. *Apple*-Datenschutzrichtlinie (Fn. 119), unter dem Punkt „Weitergabe personenbezogener Daten durch *Apple* – Dienstanbieter“.

Generell ist es sehr fraglich, ob die Datenschutztexte beider Unternehmen grundlegenden Transparenzerfordernissen entsprechen.[122] Die betreffenden Texte weisen die gleichen Schwächen auf wie eine große Anzahl aktuell verwendeter Datenschutzerklärungen von Unternehmen, bei denen Datenverarbeitungen einen wesentlichen Teil ihrer Geschäftstätigkeit ausmachen. So fehlt es insbesondere an aussagekräftigen Angaben dazu, welche konkreten Daten

- bei welchem Nutzungsszenario verarbeitet werden[123];
- für welchen Zweck aufgrund welchen Rechtfertigungsgrunds (und ggf. welcher berechtigten Interessen) verwendet werden;
- an welche konkreten Dritten weitergegeben werden;
- in welche Drittstaaten übermittelt werden;
- wie lange gespeichert werden.

Diese völlige Pauschalität und Unverbindlichkeit in den jeweiligen Datenschutzerklärungen lässt sich insbesondere mit den Transparenzerfordernissen der DSGVO kaum in Einklang bringen.[124]

2. Anbieterinformationen nach dem Telemediengesetz

Nach dem Inkrafttreten der DSGVO hat das Telemediengesetz (TMG)[125] aufgrund der Vorrangigkeit der Verordnung nur noch einen beschränkten Anwendungsbereich, insbesondere für nicht-

122 S. auch Seite 85 f., insb. Abbildung 60. Das Problem der mangelnden Transparenz verdeutlicht auch eine von der *Australian Competition & Consumer Commission (ACCC)* durchgeführte Verbraucherbefragung zu App Marketplaces, in der 70 Prozent der befragten Nutzer angaben, sie seien mit den Informationen über die Datensammlung und -weitergabe nicht zufrieden. Als Grund wurde von einem Teil der Befragten die Masse an Informationen angegeben. Demgegenüber verwies ein anderer Teil auf fehlende Informationen. Fast alle Befragten gaben an, sie seien unsicher, wer Zugriff auf ihre Daten habe und zu welchen Zwecken die Daten genutzt werden können, s. *ACCC*, App marketplaces report – Consumer questionnaire responses (27.11.2020), abrufbar unter https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025/march-2021-interim-report.

123 *Apple* gibt in seiner Datenschutzrichtlinie (Fn. 119) auf S. 4 zwar an, der Nutzer sei nicht verpflichtet, die von *Apple* angeforderten personenbezogenen Daten anzugeben; ob hieraus folgt, dass der Nutzer vor jeder Datenpreisgabe unter Nennung der konkret betroffenen Daten gesondert um eine Einwilligung ersucht wird, kann hier nicht nachvollzogen werden.

124 S. dazu ausführlich *Bundeskartellamt*, Sektoruntersuchung Smart-TVs (Fn. 71), S. 56 ff. Bei *Google* besteht zudem das Problem, dass sämtliche (höchst unterschiedlichen) *Google*-Dienste in einer Datenschutzerklärung erfasst werden.

125 Telemediengesetz vom 26.02.2007 (BGBl. I S. 179, 251), zuletzt geändert durch Artikel 2 des Gesetzes vom 03.06.2021 (BGBl. I S. 1436).

öffentliche Stellen.[126] Die Datenschutzregelungen der §§ 11 ff. TMG sind insoweit grundsätzlich nicht mehr anwendbar.[127] Im Zusammenhang mit Apps ist daher in erster Linie die allgemeine Informationspflicht nach § 5 TMG noch relevant.[128]

Apps mit journalistisch-redaktionell gestalteten Angeboten[129], in denen insbesondere vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild wiedergegeben werden, müssen zusätzlich gemäß § 18 Abs. 2 Medienstaatsvertrag (MStV)[130] einen Verantwortlichen unter Angabe von Name und Anschrift benennen.[131]

a) Ermittlungen

Unter dem Abschnitt „Kontaktdaten des Entwicklers“ enthält der *Google Play Store* Angaben zum Namen, der Rechtsform, Adresse und E-Mail-Adresse des App-Publishers. Darüber hinaus sind dort die Website und die Datenschutzerklärung verlinkt. [132]

Im *Apple App Store* werden unter der Überschrift „Informationen“ u. a. der Anbieter einschließlich der Rechtsform, Urheberrechtsangaben sowie Links zur Entwicklerwebsite und zu den Datenschutzbestimmungen aufgeführt.

---

126 S. Positionsbestimmung der unabhängigen Datenschutzbehörden des Bundes und der Länder, Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018 (26.04.2018), abrufbar unter https://datenschutzkonferenz-online.de/media/ah/201804_ah_positionsbestimmung_tmg.pdf. S. aber unten S. 79 zu § 15 Abs. 3 TMG.

127 Ebenda (Fn. 126). Aufgrund der Verdrängung datenschutzrechtlicher TMG- und TKG-Bestimmungen durch die DSGVO hat der Bundestag – mit Zustimmung des Bundesrats – das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) beschlossen, welches am 01.12.2021 in Kraft treten wird (BGBl. I vom 28.06.2021, S. 1982). Das TTDSG dient der Anpassung der Datenschutzbestimmungen des TKG und TMG an die DSGVO und die ePrivacy-Richtlinie (S. 1 des Gesetzesentwurfes, BT-Drucks. 19/27441).

128 Darüber hinaus bestehen bei Apps in Fällen kommerzieller Kommunikation im Sinne des § 2 Nr. 5 TMG die besonderen Pflichten des § 6 TMG, die sich insbesondere auf die klare Kennzeichnung als Werbung beziehen. Diese Pflicht ist aber für App-Publisher vor dem App-Download im Regelfall noch nicht relevant.

129 Z. B. die Spiegel-App (vgl. *Ewald* in: Taeger/Pohle [Hrsg.], ComputerR-HdB, 36. EL Februar 2021, 32.7 Erstellung und Vertrieb von Mobile Apps, Rn. 75).

130 Staatsvertrag zur Modernisierung der Medienordnung in Deutschland (Medienstaatsvertrag) vom 14. – 28.04.2020, in Kraft getreten am 07.11.2020.

131 S. *Sesing* in: BeckOK IT-Recht, TMG § 5 Rn. 111.

132 S. Abbildung 7 auf S. 23.

Das Impressum des *Google Play Stores* selbst ist bei Aufrufen der eigenen Profilübersicht am Seitenende unter „Über Google Play“ einsehbar. Durch Klicken auf diesen Button wird der Nutzer zu dem Abschnitt „Impressum“ auf *Googles* Website weitergeleitet, auf der sich die Adress- und Kontaktdaten der Google Ireland Limited, Dublin, befinden.

Ein Impressum oder eine Verlinkung zu einem solchen ist im *Apple App Store*, soweit ersichtlich, nicht vorhanden.

b) Würdigung

Nach wohl herrschender Literaturmeinung sind App-Store-Betreiber stets[133] sowie Publisher kommerzieller Apps unter bestimmten Umständen[134] als Anbieter von Telemedien anzusehen und müssen daher die Transparenzpflichten des Telemediengesetzes einhalten. Nach § 5 Abs. 1 Nr. 1 bzw. 2 TMG sind u. a. Name und Niederlassungsanschrift, bei juristischen Personen Rechtsform, Vertretungsberechtigte sowie Angaben zur schnellen elektronischen Kontaktaufnahme einschließlich E-Mail-Adresse leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten.

Soweit ersichtlich enthalten die meisten App-Darstellungen in den App-Stores diese Angaben allenfalls teilweise. Während bei *Google Play* im Abschnitt „Kontaktdaten des Entwicklers“[135] zumindest ein Teil der erforderlichen Angaben enthalten ist (Name einschließlich Rechtsform, Anschrift und E-Mail-Adresse), werden im *Apple App Store* unter dem Punkt „Informationen“[136] nur Name und Rechtsform angezeigt. Sofern einschlägige Informationen über einen Link zu Nutzungsbedingungen, Datenschutzbestimmungen oder Unternehmenswebsites zugänglich sind, fehlt es in der Regel an einer leichten Erkennbarkeit, da die relevanten Angaben in der Regel unvollständig oder jedenfalls nicht zusammenhängend und ohne weiteres Scrollen visuell erfassbar sind.

---

133 Siehe hierzu *Ewald* in: Baumgartner/Ewald [Hrsg.], Apps und Recht, 2. Aufl. 2016, Rn. 154; *Feldmann*, DSRI-Tagungsband 2011, 47, 61; *Kremer* in: Auer-Reinsdorff/Conrad IT-R-HdB, 3. Aufl. 2019, § 28 Apps und Social Media Rn. 21; *Mankowski* in: Fezer/Büscher/Obergfell [Hrsg.], Lauterkeitsrecht: UWG, Zweiter Teil Wettbewerbsrecht des Internets (S. 12), Rn. 298h.

134 Beispielsweise sind Apps, die lediglich lokale Funktionen anbieten und nicht online kommunizieren, keine Telemedien im Sinne des § 1 Abs. 1 S. 1 TMG, siehe hierzu *Ewald* in: Baumgartner/Ewald [Hrsg.], Apps und Recht, 2. Aufl. 2016, Rn. 148 ff.; *Feldmann*, DSRI-Tagungsband 2011, 47, 61. Zur Anwendbarkeit des TMG auch auf Anbieter aus anderen Mitgliedstaaten der Europäischen Union siehe *Ewald* in: Taeger/Pohle [Hrsg.], ComputerR-HdB, 36. EL Februar 2021, 32.7 Erstellung und Vertrieb von Mobile Apps, Rn. 73.

135 Siehe dazu oben Abbildung 7 auf S. 23.

136 Siehe dazu oben Abbildung 13 auf S. 28.

Was *Google Play* selbst betrifft, so kann der Nutzer zwar nach Aufrufen seiner Profilübersicht und dort durch Klicken auf „Über *Google Play*“ das Impressum auf einer externen *Google*-Webseite aufrufen, die die nach § 5 Abs. 1 TMG erforderlichen Angaben enthält. Fraglich ist hier aber, ob die relevanten Informationen „unmittelbar verfügbar“ sind. Für weiterführende Links zu den nach § 5 Abs. 1 TMG relevanten Informationen müssen Bezeichnungen gewählt werden, die verständlich sind und sich dem Nutzer ohne weiteres erschließen.[137] Der BGH hat es bei einer Internetseite hinsichtlich der Voraussetzungen der leichten Erkennbarkeit und unmittelbaren Erreichbarkeit für ausreichend angesehen, wenn das Impressum durch zwei Klicks (wie hier) aufgerufen werden kann.[138] Auch hat das OLG München einen Link mit der Bezeichnung „Wir über uns“ grundsätzlich als hinreichend aussagekräftig erachtet.[139] Folgte man dieser Auffassung, wäre auch „Über Google Play“ als Bezeichnung nicht zu beanstanden. Allerdings ist jedenfalls die Verortung dieses Links im Profilbereich von *Google Play* kritisch zu sehen. Bei einem lediglich verlinkten Impressum stellt sich ferner die Frage, ob dieses „ständig verfügbar“ ist. Zwar ergibt sich aus einem kurzfristigen Ausfall der verlinkten Website von nur wenigen Minuten noch kein Verstoß gegen § 5 Abs. 1 TMG.[140] Allerdings besteht stets das Risiko einer längeren Unerreichbarkeit der Website, was zu einem Verstoß gegen § 5 Abs. 1 TMG führen kann. Ferner ist umstritten und bisweilen ungeklärt, ob die Voraussetzung der ständigen Verfügbarkeit gewahrt ist, wenn das Impressum, wie beispielsweise im *Google Play* Store, nur abrufbar ist, solange eine Internetverbindung besteht.[141]

3. Informationen über Drittempfänger personenbezogener Daten

Die Untersuchung ist auch dem tatsächlichen Datensendeverhalten mobiler Apps sowie der diesbezüglichen Transparenz gegenüber dem Verbraucher nachgegangen. Apps können mit verschiedenen Diensten kommunizieren, etwa mit den Web-Servern des App-Publishers, soweit dies nötig ist, um ihre Funktion gegenüber dem App-Nutzer zu erbringen. Aus diesem Grund können sie auch externe Dienste einbinden, wenn der App-Publisher diesen Dienst nicht selbst bereithält (z. B. zur Nutzung eines Kartendienstes in der App). Weitere Gründe für die Kommunikation mit den Diensten Dritter sind Analysen des Nutzungsverhaltens und das Sammeln personenbezogener Daten zum Ausspielen interessenbasierter Werbung. Bei der Kommunikation mit

---

137 S. BGH, Urteil vom 20.07.2006, Az. I ZR 228/03, juris Rn. 19; *Müller-Broich*, Telemediengesetz, 2012, § 5 Rn. 18.

138 BGH, Urteil vom 20.07.2006, Az. I ZR 228/03, juris.

139 OLG München, Urteil vom 12.02.2004, Az. 29 U 4564/03, juris Rn. 32.

140 OLG Düsseldorf, Urteil vom 04.11.2008, Az. I-20 U 125/08, juris.

141 *Ewald* in: Taeger/Pohle [Hrsg.], ComputerR-HdB, 36. EL Februar 2021, 32.7 Erstellung und Vertrieb von Mobile Apps, Rn. 79.

Dritten kommen häufig sog. Anwendungsprogrammierschnittstellen (engl. Application programming interface, kurz: API) von den Anbietern dieser Dienste zum Einsatz, die in den Code der App eingebettet werden und Daten, die bei der App-Nutzung entstehen, an diese Dienste senden. Bei der Sammlung von Daten zur Nutzungsanalyse und zum Ausspielen interessenbasierter Werbung werden in der Regel eindeutige Identifikatoren, etwa in Form einer gerätespezifischen Werbe-ID, an die Dienste Dritter übermittelt, so dass die Daten einem Nutzer eindeutig zugeordnet werden können. Dies erlaubt dem Datenempfänger die Bildung von Nutzerprofilen, ggf. auch über die Nutzung verschiedener Apps und Aufrufe von Internetseiten hinweg. Ein solches Auswerten von Nutzungsinformationen wird als Tracking (engl. to track = folgen) bezeichnet. Da das Tracking meist nicht unmittelbar vom App-Publisher, sondern von Dritten ausgeht, deren APIs in der App verwendet werden, spricht man in diesem Zusammenhang auch von Third-Party-Tracking. Dem Nutzer werden auf der Grundlage der gesammelten Daten persönliche Merkmale oder Interessen zugeordnet und so Nutzerprofile erstellt. Die Nutzerprofile sind umso besser verwertbar, je mehr Details sie über eine Person enthalten. Auf Basis der Nutzerprofile können dann Werbemaßnahmen gezielt und personalisiert ausgespielt werden, indem die Werbenetzwerke Werbeplätze innerhalb der Apps meistbietend verkaufen. Dies kann innerhalb von Sekundenbruchteilen im Rahmen eines sog. Real Time Bidding erfolgen.

Ende April 2021 hat *Apple* die Möglichkeiten der Nutzerverfolgung mit dem Upgrade auf *iOS 14.5* und der Einführung des sog. „App Tracking Transparency Framework“ (ATT Framework) für dritte App-Publisher eingeschränkt (soweit ersichtlich jedoch nicht für das eigene Werbenetzwerk). App-Publisher dürfen seitdem nicht mehr ohne Weiteres auf den gerätespezifischen IDFA (Identifier for advertisers), wie die Werbe-ID bei *Apple*-Produkten genannt wird, zugreifen. Apps, die Nutzungsaktivitäten erfassen wollen, müssen den Nutzer nun ausdrücklich um Erlaubnis fragen:

Abbildung 28: Hinweis auf *Apples* ATT-Framework in den Einstellungen von *iOS* (Screenshot-Ausschnitt)

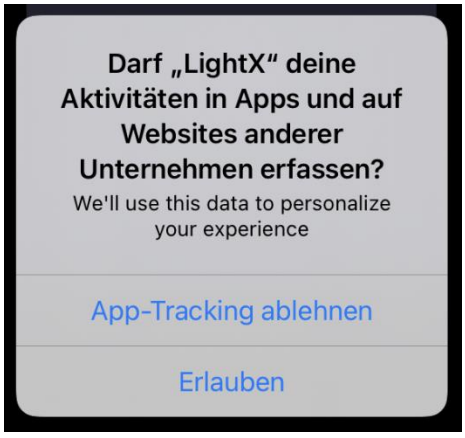


Abbildung 29: Abfrage der Trackingerlaubnis durch die App *LightX* (Screenshot-Ausschnitt)

Für *Google Android* gibt es bislang keinerlei Zustimmungsmechanismus. Es besteht bislang nur die Möglichkeit, die Werbe-ID manuell zurückzusetzen, um einem dauerhaften Tracking über diesen Identifikator zu entgehen.[142] Voraussichtlich Ende 2021 wird es aber auch für *Google Android* die Möglichkeit geben, die Werbe-ID zu deaktivieren, wobei es sich offenbar um eine Opt-out-Lösung handelt (d. h. die Werbe-ID wird nicht automatisch deaktiviert, und der Nutzer wird auch nicht gefragt, sondern muss selbst aktiv werden).[143]

Die Verbraucherbefragung des Bundeskartellamts hat ergeben, dass App-Nutzer ein ausgeprägtes Interesse daran haben zu erfahren, welche Unternehmen Daten aus der App-Nutzung erhalten. Nahezu 95 Prozent der Befragten stimmten der Aussage voll und ganz oder eher zu, dass Datenempfänger vor dem App-Download angezeigt werden sollten:

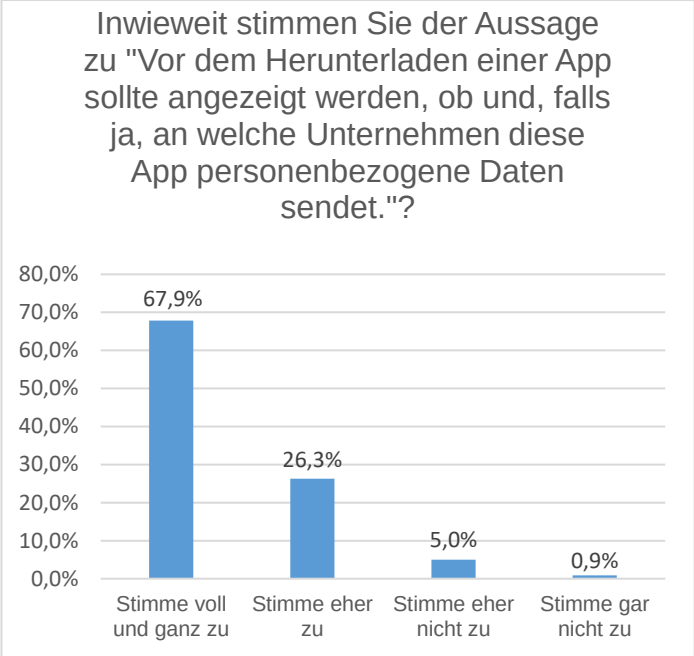


Abbildung 30: Verbrauchermeinung zur Anzeige von Datenempfängern vor dem App-Download

a) Ermittlungen

Ein häufig beschriebenes Problem im Zusammenhang mit Drittempfängern von Daten ist es, dass der App-Nutzer nicht oder nicht ausreichend darüber informiert wird, dass bei der Nutzung einer

---

142 Kritisch zur bloßen Rücksetzbarkeit *Competition and Markets Authority*, Online platforms and digital advertising market study (aktualisierte Fassung vom 01.07.2020), Appendix G, Rn. 132 a. E., abrufbar unter https://assets.publishing.service.gov.uk/media/5fe49554e90e0711ffe07d05/Appendix_G_-_Tracking_and_PETS_v.16_non-confidential_WEB.pdf.

143 S. hierzu die entsprechenden Ausführungen auf der *Google*-Support-Seite https://support.google.com/googleplay/*Android*-developer/answer/6048248?hl=de.

App personenbezogene Daten an Dritte übermittelt werden. Um dies zu ermitteln hat das Bundeskartellamt das Institut für Technik und Journalismus e. V. (ITUJ e. V.), Mitbetreiber der Website www.mobilsicher.de gebeten, eine Auswahl von *Android*-Apps daraufhin zu überprüfen, inwieweit sie Daten an andere Empfänger als den App-Publisher selbst übermitteln.

aa) Konzeption

Im Hinblick auf die begrenzten Ressourcen wurde bei der Untersuchung von Apps auf Drittempfänger von Daten nur die Situation beim Download von (Android-)Apps im App-Store *Google Play* betrachtet. Zum einen handelt es sich bei Android um das in Deutschland wesentlich weiter verbreitete Betriebssystem, zum anderen ist insbesondere die Frage des Third-Party-Tracking bei *iOS* durch die jüngsten Datenschutzmaßnahmen *Apples* etwas weniger dringlich (siehe oben).

Aufgrund des hohen mit den App-Prüfungen verbundenen Aufwands war es notwendig, die Analyse auf eine Auswahl von Apps zu beschränken. Daher wurde unter Berücksichtigung der Verbreitung, auch über Altersstufen und gesellschaftliche Schichten hinweg, der Nutzungsintensität und der Nachhaltigkeit der Nutzung der Apps eine Prüfliste von 32 Apps erstellt. Der *ITUJ e. V.* führte die entsprechenden Tests zwischen April und Juli 2021 durch.

Google-eigene Apps blieben bei der Analyse außen vor. Erstens stehen *Google* – jedenfalls bei Verwendung des Betriebssystems *Android* – grundsätzlich weitergehende Möglichkeiten zur Verfügung, Nutzungsverhalten ohne die Einschaltung von Drittempfängern zu erfassen als anderen App-Publishern[144]. Zweitens ist *Google* als größter Werbevermarkter im Online-Bereich in der Lage, Nutzungsdaten konzernintern zu analysieren und monetarisieren, ohne hierfür Dritten in seinen Apps Zugriff auf personenbezogene Nutzungsdaten einräumen zu müssen.[145]

Die Prüfung stellte jeweils auf den Aufbau von Datenverbindungen ab, ohne dass danach unterschieden wurde, ob es sich bei dem Empfänger um einen Tracker im engeren Sinne handelt, also einen Drittanbieter, der Dienstleistungen im Bereich Werbung, Marketing oder Nutzeranalyse anbietet.

---

144 S. zu den Schwierigkeiten beim Test von *Google*-Apps auch https://appcheck.mobilsicher.de/allgemein/app-auswahl-diese-apps-testen-wir.

145 Dieses Argument trifft gleichermaßen auf *Facebook* zu. Gleichwohl sollte auf die Untersuchung von Facebook-Apps aufgrund ihrer herausgehobenen Stellung im Bereich der sozialen Netzwerke bzw. Messenger nicht verzichtet werden. Die Ergebnisse für die *Facebook-, Instagram-* und *WhatsApp*-App sind mithin nicht als Beleg für eine insgesamt niedrige Datenverarbeitungsintensität zu verstehen.

bb) Durchführung

Die Tests wurden auf einem *Android*-Gerät (Pixel 2) mit der *Android*-Version 8.0 durchgeführt. Die getesteten Apps wurden aus dem Play-Store heruntergeladen, auf dem Testgerät installiert und jeweils für rund zehn Minuten von einer Person bedient. Bei Apps, die für die sinnvolle Nutzung eine Anmeldung mit einem Nutzerkonto benötigen, wurde ein Nutzerkonto mit E-Mail-Adresse und Passwort angelegt. Der Standort wurde jeweils freigegeben, wenn die App danach fragte. Einwilligungen in die Nutzungs- und Datenschutzbedingungen wurden gewährt. Bei echten Wahlmöglichkeiten wurde jeweils die Option gewählt, die der Entwickler optisch hervorgehoben hatte.

Der dabei entstandene Datenverkehr wurde mittels eines sogenannten „man-in-the-middle-setups“ abgefangen und analysiert. Bei diesem in der IT-Sicherheitsforschung gängigen Setup wird der Datenverkehr über einen sogenannten Proxy umgeleitet und kann dort gesichtet werden. Für jedes übermittelte Datenpaket wurde die Internetadresse erfasst, an die es gesendet werden sollte.

Als „Anbieter“ im Sinne der weiteren Analyse wurde die juristische Person festgelegt, welche die betreffende Internetadresse zum Testzeitpunkt besaß. Die Besitzverhältnisse wurden entweder aus Impressumsangaben oder über WHOIS-Abfragen ermittelt. Hierbei handelt es sich in der Regel um eine Firma, aber auch Vereine, öffentliche Institutionen oder Einzelpersonen können Anbieter sein.

cc) Feststellungen

Die im Rahmen der vom *ITUJ e. V.* durchgeführten dynamischen[146] Analyse erkannten Datenempfänger wurden den Ausführungen des jeweiligen App-Publishers in der Datenschutzerklärung zu der betreffenden App gegenübergestellt. Dabei wurden folgende drei Kategorien gebildet:

	Weniger als die Hälfte der Drittempfänger wird explizit genannt.
	Mindestens 50 % der Drittempfänger werden explizit genannt.
	Drittempfänger sind nicht vorhanden oder werden (nahezu) vollständig explizit genannt.

146 Im Gegensatz zur statischen Analyse, bei der lediglich der App-Programmcode daraufhin untersucht wird, ob dieser eingebettete Tracker etc. enthält, wird bei der dynamischen Analyse geprüft, ob ein Datenfluss zu einem bestimmten Empfänger tatsächlich zustande kommt.

Eine explizite Nennung setzt voraus, dass Unternehmen nicht nur nach Kategorie bezeichnet („Dritte“, „Geschäftspartner“, „Werbeunternehmen“), sondern klar benannt werden (also z. B. *AppsFlyer Inc.*).

Nachfolgend werden die geprüften Apps aufgeführt und einer der oben genannten Kategorien zugeordnet. Unter der App-Bezeichnung ist jeweils ein Link zu dem Testergebnis auf der Internetseite https://appcheck.mobilsicher.de/ hinterlegt.

Die nachfolgende Transparenzbewertung dient – unter Zugrundelegung eines groben quantitativen Maßstabs – ausschließlich der Bestandsaufnahme, in welchem Umfang App-Publisher Drittempfänger personenbezogener Daten konkret benennen. Es handelt sich dabei **nicht** um eine datenschutzrechtliche Qualitätsbewertung. So können beispielsweise nicht in einer Datenschutzerklärung deklarierte Drittempfänger datenschutzrechtlich relativ unbedenkliche Datenverarbeitungen durchführen. Umgekehrt ist es möglich, dass auch bei vollständiger Angabe aller Drittempfänger oder sogar bei völliger Abwesenheit von Drittempfängern beim App-Publisher datenschutzrechtlich problematische Verarbeitungen personenbezogener Daten stattfinden. Um sich hiervon ein Bild machen zu können, sehen Sie sich bitte die verlinkten App-Tests an.

App-Bezeichnung	Geprüfte Version[147]	Kategorie	Transparenz
Adidas Running/ Runtastic	12.0	Health and Fitness	●
Amazon Shopping	22.13.0.100	Shopping	✚
Bild.de	8.1	News and Magazines	▬
Booking.com	28.0	Travel and Local	▬
Clash of Clans	14.93.6	Game Strategy	▬
Coin Master	3.5.392	Game Casual	●
DB Navigator	21.06.p04.00	Maps and Navigation	●
Duolingo	5.19.3	Education	●

147 Die Testergebnisse werden regelmäßig aktualisiert, so dass die verlinkte Bewertung ggf. eine neuere Version der betreffenden App zum Gegenstand hat.

eBay Kleinanzeigen	12.20.0	Shopping	
Facebook	327.0.0.33.120	Social	
Idealo	19.6.0	Shopping	
Instagram	195.0.0.31.123	Social	
Kindle	8.44.0.100(1.3.244298.0)	Books and Reference	
Komoot	11.5.8	Health and Fitness	
Lieferando	7.7.2	Food and Drink	
Microsoft Teams	1416/1.0.0.2021093701	Business	
Netflix	7.112.0 build 7 35534	Entertainment	
Pinterest	9.23.0	Lifestyle	
QR & Barcode Scanner	2.7.1-L	Productivity	
Signal	5.17.3	Communication	
Skype	8.73.0.129	Communication	
Spotify	8.6.46.886	Music and Audio	
Subway Surfers	2.19.1	Game Arcade	
Telegram	7.8.1	Communication	
Tiktok	20.5.3	Social	
Tinder	12.13.0	Lifestyle	
Twitter	9.3.0-release.00	Social	

Web.de	7.2.4	Communication	
Wetter.com	2.45.5	Weather	
WhatsApp	2.21.12.21	Communication	
ZDF Mediathek	5.8.1	Entertainment	
Zoom	5.7.1.1254	Business	

Tabelle 3: Transparenz der Angabe von Drittempfängern in Datenschutzerklärungen

Wie bereits oben erwähnt, bedeutet eine positive Bewertung hinsichtlich der Nennung von Drittempfängern nicht automatisch, dass die Nutzer auch angemessen über die *Datenverarbeitungen* durch die Drittunternehmen informiert werden. Es ist daher etwa möglich, dass in den Datenschutzbestimmungen einer App zwar vollumfänglich und korrekt über Drittempfänger von personenbezogenen Daten informiert wird, es jedoch beispielsweise unklar bleibt, welche personenbezogenen Daten konkret an das betreffende Unternehmen fließen. Es geht in diesem Analyseschritt mithin ausschließlich darum zu zeigen, inwieweit Datenverarbeitungen durch Drittunternehmen *überhaupt* transparent gemacht werden. Dies wird in der nachfolgenden Abbildung für die Gesamtheit aller analysierten Apps dargestellt:

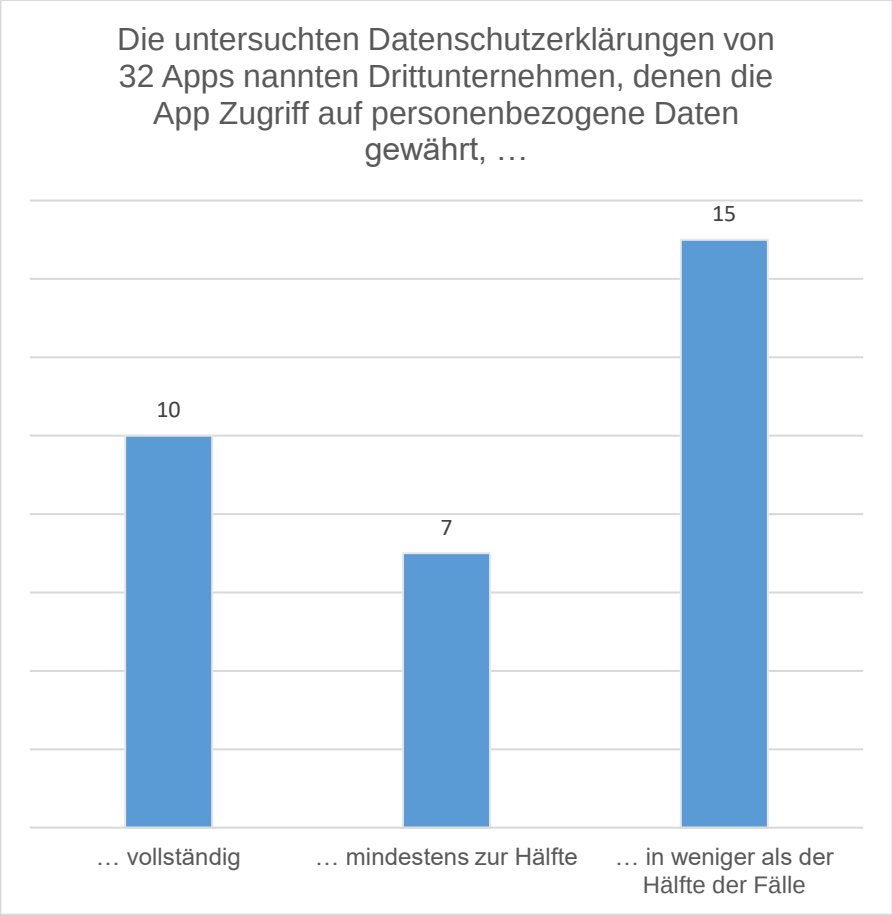


Abbildung 31: Transparenz bzgl. Drittempfängern personenbezogener Daten

b) Würdigung

Nachfolgend sollen von Apps ausgelöste Datenflüsse an Drittunternehmen näher betrachtet werden. Hauptanwendungsfall ist das sog. Third-Party-Tracking, also das Verfolgen von Nutzeraktivitäten durch andere Unternehmen als den App-Publisher selbst. Dass der App-Publisher selbst ebenfalls Nutzungsdaten erhält, ist bei vielen Online-Anwendungen für das Funktionieren der App notwendig. Zwar mag in diesen Fällen der Umfang der Datenverarbeitung häufig über das Funktionsnotwendige hinausgehen. Ob und inwieweit dies der Fall ist, ließe sich aber im Rahmen einer technischen Prüfung kaum feststellen.

Der App-Nutzer erlangt von den Datenabflüssen an Dritte häufig keine Kenntnis, obwohl die gesammelten Daten – insbesondere in ihrer Gesamtheit – hochsensibel sein können. Wie soeben gezeigt, wird der Nutzer insbesondere vor dem App-Download (und im Regelfall auch später) nicht darüber informiert, welche Drittunternehmen über die App personenbezogene Daten erhalten. Er kann sich mithin auch kein klares Bild darüber verschaffen, welche Daten konkret abfließen und wer diese erhält.

In diesem Zusammenhang müssen zunächst die vertraglichen Beziehungen im Zusammenhang mit dem Herunterladen von Apps geklärt werden. Hieran schließt sich die Frage an, wen welche

gesetzliche Informationspflichten treffen, die den Verbraucher vor einer unbewussten Datenpreisgabe schützen können.

aa) Informationspflichten nach Verbrauchervertragsrecht

Die in § § 312c, 312d Abs. 1 BGB i. V. m. Art. 246a EGBGB enthaltenen Informationspflichten sind gem. § 312 Abs. 1 BGB nur dann einschlägig, wenn eine entgeltliche Leistung des Unternehmers vorliegt. Ob die Überlassung von Daten, jedenfalls wenn sie für die Vertragserfüllung nicht erforderlich sind, als „Entgelt" einzustufen sind, ist umstritten. Eine Mehrheit der Autoren scheint der Ansicht zuzuneigen, (zumindest personenbezogene) Daten als Entgelt ausreichen zu lassen.[148] Art. 3 Abs. 1 S. 2 der EU-Richtlinie über digitale Inhalte[149] sieht nunmehr explizit vor, dass die betreffenden Verbraucherinformationsvorschriften auch für solche Verträge gelten sollen, bei denen der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder sich hierzu verpflichtet. Diese Vorgabe wird in Deutschland durch § 312 Abs. 1a BGB n. F. umgesetzt[150], der am 1. Januar 2022 in Kraft treten wird.

Ungeachtet der genauen rechtlichen Einordnung des Vertragsverhältnisses beim Download einer App aus dem App-Store kommt dieses unter ausschließlicher Verwendung von Fernkommunikationsmitteln zustande, so dass ein Fernabsatzvertrag im Sinne des § 312c Abs. 1 BGB vorliegt. Für Verbraucherverträge in Form solcher Fernabsatzverträge erlegt das BGB dem Unternehmer diverse vorvertragliche Informationspflichten auf. Die entsprechenden Vorschriften erfassen erkennbar nur die am Vertrag unmittelbar beteiligten Parteien, hier also – jedenfalls im Hinblick auf *Google Play* – den App-Store-Betreiber und den Verbraucher[151]. Neben den allgemeinen Informationspflichten im Sinne des § 312d Abs. 1 BGB i. V. m. Art. 246a § 1 Abs. 1 S. 1 Nr. 1 EGBGB, wonach der Unternehmer verpflichtet ist, den Verbraucher über die wesentlichen Eigenschaften

---

148 Für eine Entgeltlichkeit im Sinne von § 312 Abs. 1 BGB bei der Hingabe von Daten etwa *Wendehorst* in: Münchener Kommentar zum BGB, 8. Aufl. 2019, § 312 Rn. 38; Martens in: BeckOK BGB, 58. Ed. 1.5.2021, § 312 Rn. 10; *Schulte-Nölke* in: Schulze [Hrsg.], Bürgerliches Gesetzbuch, 10. Aufl. 2019, § 312 Rn. 5; *Thüsing* in: Staudinger [Hrsg.], BGB, Neubearbeitung 2019, § 312 Rn. 6 (m. w. N.); dagegen etwa Schirmbacher in Spindler/Schuster [Hrsg.], Recht der elektronischen Medien, 4. Aufl. 2019, BGB § 312 Rn. 32.

149 Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, ABl. EU Nr. L136 vom 22.05.2019, S. 1, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L0770.

150 S. Art. 1 Nr. 2 des Gesetzes zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (BGBl I vom 30.06.2021, Seite 2123).

151 Bei *Apple* ist dies weniger klar, so dass die einschlägigen Verpflichtungen womöglich den App-Publisher treffen könnten, s. dazu oben S. 26 ff.

der Waren oder Dienstleistungen zu informieren, hat der Gesetzgeber im Jahr 2014[152] zudem besondere Informationspflichten in Bezug auf digitale Inhalte geschaffen, vgl. § 312d Abs. 1 BGB i. V. m. Art. 246a § 1 Abs. 1 S. 1 Nr. 14 und 15 EGBGB. Gemäß § 312d Abs. 1 i. V. m. Art. 246a § 1 Abs. 1 S. 1 Nr. 14 EGBGB muss der Unternehmer den Verbraucher „gegebenenfalls über die Funktionsweise digitaler Inhalte, einschließlich anwendbarer technischer Schutzmaßnahmen für solche Inhalte“ informieren. Die Vorschrift geht auf den wortlautgleichen Art. 6 Abs. 1 lit. r der Verbraucherrechte-Richtlinie zurück. Zweck ist es – wie bei sonstigen vertraglichen Informationspflichten – das grundsätzlich bestehende Informationsgefälle zwischen Unternehmer und Verbraucher auszugleichen und sicherzustellen, dass der Verbraucher über genügend Informationen verfügt, um eine überlegte Entscheidung zu treffen.[153] Der Begriff der digitalen Inhalte ist in § 312f Abs. 3 BGB legaldefiniert als „nicht auf einem körperlichen Datenträger befindliche Daten, die in digitaler Form hergestellt und bereitgestellt werden“. In Erwägungsgrund 19 genannte Beispiele sind Computerprogramme, Anwendungen (Apps), Spiele, Musik, Videos oder E-Books.

Der Begriff der Funktionsweise bezieht sich ausweislich Erwägungsgrund 19 der Verbraucherrechte-Richtlinie darauf, wie digitale Inhalte verwendet werden können, etwa für die Nachverfolgung des Verhaltens des Verbrauchers (in der englischen Fassung: „tracking of consumer behaviour“).

Die Generaldirektion Justiz und Verbraucher der Europäischen Kommission hat im Juni 2014 einen Leitfaden zur wirksamen Anwendung der Verbraucherrechte-Richtlinie veröffentlicht.[154] Zwar handelt es sich dabei nicht um ein rechtsverbindliches Dokument, sondern vielmehr um eine Orientierungshilfe. Dennoch können dem Leitfaden wichtige Informationen entnommen werden, die für die Auslegung und Anwendung der Richtlinie von Bedeutung sind.

---

152 Gesetz zur Umsetzung der Verbraucherrechterichtlinie und zur Änderung des Gesetzes zur Regelung der Wohnungsvermittlung vom 20. September 2013 (BGBl. I, S. 3642) m. W. v. 13.06.2014.

153 *Wendehorst* in: Münchener Kommentar BGB, 8. Aufl. 2019, § 312a Rn. 6.

154 Leitfaden der Europäischen Kommission, Generaldirektion Justiz zur Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates (Juni 2014), abrufbar unter https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Leitfaden_RLV.pdf (im Folgenden: „Leitfaden zur Verbraucherrechte-Richtlinie“).

Der Leitfaden enthält eine indikative Liste von Angaben zur Funktionsweise. Dort sind unter Nr. 6 „Nutzungsbedingungen, die nicht unmittelbar mit der Interoperabilität des Produkts zusammenhängen, etwa […] Tracking und/oder Personalisierung“ ausdrücklich aufgeführt.[155]

Zwar wird in der Kommentarliteratur[156] teilweise darauf hingewiesen, dass an die Informationspflichten im vorvertraglichen Stadium keine überhöhten Anforderungen zu stellen seien. Zu informieren sei daher nur über die wesentlichen Hinweise, die notwendig seien, damit dem Verbraucher verständlich werde, wie die digitalen Inhalte verwendet werden können.[157] Dem ist allerdings entgegenzuhalten, dass der Wortlaut des Art. 246a § 1 Abs. 1 Nr. 14 EGBGB, etwa im Gegensatz zu Nr. 15, gerade kein Wesentlichkeitserfordernis enthält. Selbst bei Annahme eines Wesentlichkeitserfordernisses würde dies zudem im Ergebnis nichts an der Informationspflicht ändern, da es sich bei der Tatsache, dass Nutzerdaten getrackt werden, aufgrund des nicht unerheblichen Eingriffes in die Privatsphäre um eine solche wesentliche Information handelt. Dies gilt umso mehr, als es sich beim Tracking um eine verdeckte und für den Verbraucher letztlich nicht mehr kontrollierbare Datenverarbeitung handelt.

Eine verbrauchervertragsrechtliche Informationspflicht jedenfalls darüber, dass über eine App Nutzertracking erfolgt, ist demnach zu bejahen.

Im Anschluss an die Frage, ob der Verbraucher über den Einsatz von Trackern informiert werden muss, stellt sich die Folgefrage, zu welchem Zeitpunkt und in welcher Form dies zu geschehen hat. Bei der Beantwortung dieser Fragen sind insbesondere die beschränkten Möglichkeiten der Darstellung auf einem Smartphone oder Tablet im Gegensatz zu den Möglichkeiten auf einer Webseite zu beachten. Diesem Umstand hat der Gesetzgeber in Art. 246a § 3 S. 1 EGBGB Rechnung getragen, wonach im Rahmen von Fernabsatzverträgen mittels eines Kommunikationsmittels, das nur einen begrenzten Raum oder begrenzte Zeit für die dem Verbraucher zu erteilende Information bietet, nur bestimmte Informationen zur Verfügung gestellt werden müssen, darunter nach Nr. 1 die wesentlichen Eigenschaften der Waren oder Dienstleistungen.[158]

---

155 Ebenda (Fn. 154), S. 82. Datenverbindungen zu anderen Zwecken fallen hingegen nicht ausdrücklich unter diese verbraucherrechtliche Informationspflicht.

156 § 312d Abs. 1 BGB i. V. m. Art. 246a § 1 Abs. 1 S. 1 Nr. 14 EGBGB entspricht § 312a Abs. 2 BGB i. V. m. Art. 246 Abs. 1 Nr. 7 EGBGB, weshalb teilweise auf dessen Kommentierung verwiesen wird.

157 *Thüsinger* in: Staudinger [Hrsg.], BGB, Neubearbeitung 2019, § 312a Rn. 34.

158 Die weiteren Angaben nach § 1 hat der Unternehmer gemäß Art. 246a § 3 Satz 2, § 4 Abs. 3 S. 2 EGBGB dem Verbraucher „in geeigneter Weise“ zugänglich zu machen.

Der Leitfaden zur Verbraucherrechte-Richtlinie enthält im Anhang I Muster für die Darstellung von Verbraucherinformationen zu digitalen Online-Produkten.[159] Auch diese sind nicht als verbindliche Vorgaben zu verstehen, sondern sollen den Unternehmen lediglich eine von vielen denkbaren Möglichkeiten aufzeigen, wie sie der Informationspflicht in der Praxis nachkommen können. An den Beispielen einer Wettervorhersage-App und einem Video-on-Demand-Abonnement ist dort demonstriert, welche Informationen dem Verbraucher bereits vor dem Download der App zur Verfügung gestellt werden müssen. Der Leitfaden schlägt zunächst eine einheitliche Symbolik vor. Für den Bereich der Smartphone-Umgebung sollen die Informationen auf einer zusätzlichen Seite verfügbar gemacht werden, zusammen mit der Schaltfläche für den Vertragsabschluss. Unter dem Punkt „Funktionalität“ und dort unter „Tracking“ ist in diesem Muster die Information enthalten: „Wir verarbeiten Informationen über Ihre Nutzung des Produkts zu Marktforschungszwecken.“ Tracking durch ein anderes Unternehmen als den App-Publisher ist für den Verbraucher noch weniger absehbar als das durch den App-Publisher selbst und die Information hierüber zumindest gleichermaßen wesentlich. Umfassende Informationen zum Tracking durch den App-Publisher oder Drittunternehmen sind mithin bereits vor Vertragsschluss zur Verfügung zu stellen.

Bislang nicht geklärt ist indessen, wie weit die Informationspflicht des Art. 246a § 1 Abs. 1 S. 1 Nr. 14 EGBGB reicht. So ließe sich durchaus vertreten, zur umfassenden Information des Verbrauchers müssten – aus Platzgründen wohl über eine Verlinkung – alle Empfänger von personenbezogenen Nutzerdaten dargestellt werden. Andererseits ließe sich auch argumentieren, die „Funktionsweise“ der betreffenden Software sei mit dem Hinweis, dass und zu welchen Zwecken Tracking stattfindet, hinreichend erläutert.

Rechtsfolge eines Verstoßes gegen die verbrauchervertragsrechtliche Informationspflicht ist zunächst, dass sich der Beginn der Widerrufsfrist verzögert (§ 356 Abs. 3 BGB). Zudem können Verstöße gegen verbrauchervertragsrechtliche Informationspflichten unter Umständen auch wettbewerbsrechtlich wegen Rechtsbruchs abgemahnt werden (§ 3a UWG). Daneben kommen bei der Verletzung der Informationspflichten Schadensersatzansprüche des Verbrauchers aus allgemeinen Grundsätzen gemäß § § 280 Abs. 1, 241 Abs. 2 BGB[160], ggf. i. V. m. § 311 Abs. 2 BGB, in Betracht.

---

159 Leitfaden zur Verbraucherrechte-Richtlinie (Fn. 154), S. 83 ff.

160 Siehe dazu den Entwurf der Bundesregierung eines Gesetzes zur Umsetzung der Verbraucherrechterichtlinie und zur Änderung des Gesetzes zur Regelung der Wohnungsvermittlung, BT-Drucks. 17/12637 vom 06.03.2013, S. 54, abrufbar unter http://dipbt.bundestag.de/dip21/btd/17/126/1712637.pdf.

bb) Informationspflichten nach der DSGVO

Nachfolgend wird *nicht* untersucht, welche Pflichten einen Verantwortlichen treffen, der personenbezogene Daten *weitergibt* (dazu unten S. 89 ff.). Es geht in diesem Abschnitt vielmehr um die Situation, in der Unternehmen personenbezogene Daten direkt vom (mobilen Gerät des) Betroffenen erheben – insbesondere, aber nicht nur, über Third-Party-Tracker in Apps, ohne dass diese Daten vom App-Publisher aktiv weitergegeben werden. Letzterer hat möglicherweise nicht einmal Kenntnis davon, welche konkreten Daten an den Drittempfänger übermittelt werden.[161]

Die Informationspflichten der DSGVO sind in deren Artikeln 13 und 14 niedergelegt. Demnach muss der Verantwortliche, soweit er personenbezogene Daten verarbeitet, umfangreiche Informationen zur Verfügung zu stellen, wie die Speicherdauer, die Art der personenbezogenen Daten, mögliche Empfänger der Daten sowie die Bekanntgabe diverser Betroffenenrechte. Die Bestimmung des bzw. der Verantwortlichen ist somit von entscheidender Bedeutung.

Das Verhältnis zwischen App-Publisher und Drittempfänger kann so ausgestaltet sein, dass der Drittempfänger nach Anweisungen des App-Publishers handelt und mit der Datenverarbeitung keine eigenen Zwecke verfolgt. In diesem Fall wäre der App-Publisher Verantwortlicher und der Drittempfänger nicht verantwortlicher Auftragsverarbeiter.[162] In Frage kommt daneben insbesondere eine gemeinsame Verantwortlichkeit von App-Publisher und Drittempfänger für die Datenverarbeitung. Nach der Legaldefinition in Artikel 4 Nummer 7 DSGVO ist Verantwortlicher „jede

---

161 Falls Datenschutzerklärungen überhaupt explizite Angaben zu Datenempfängern enthalten, ist diesen meist nicht mit hinreichender Genauigkeit zu entnehmen, welche personenbezogenen Daten dem konkreten Datentransfer unterliegen.

162 Auftragsverarbeiter ist nach Artikel 4 Nummer 8 und Artikel 29 DSGVO derjenige, der personenbezogene Daten in funktioneller und tatsächlicher Hinsicht im Auftrag und nach Weisung des Verantwortlichen verarbeitet. Die Verarbeitung durch den Auftragsverarbeiter wird in einem solchen Fall daher grundsätzlich auch nur dem Verantwortlichen zugerechnet, weil er derjenige ist, der nach Artikel 4 Nummer 7 DSGVO allein über Mittel und Zwecke der Datenverarbeitung entscheidet.

Nach Auffassung der Datenschutzkonferenz ist der Einsatz von *Google Analytics* kein Fall der Auftragsverarbeitung, sondern begründet eine gemeinsame Verantwortlichkeit. Beim Einsatz von *Google Analytics* seien Zwecke und Mittel der Datenverarbeitung zum Teil ausschließlich von *Google* vorgegeben. Es liege insoweit keine Weisungsgebundenheit vor; vielmehr habe sich der Anbieter das Recht eingeräumt, die Daten der Nutzer (auch) zu eigenen Zwecken zu verwenden. Siehe dazu Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12.05.2020 – Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich, S. 2 f., abrufbar unter https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_google_analytics.pdf. Der Beschluss bezieht sich zwar in erster Linie auf Websites, dürfte aber für Apps, die *Google-Analytics* einbinden, gleichermaßen gelten.

natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Eine gemeinsame Entscheidung über die Mittel der Datenverarbeitung (Programmierung einer Anwendungsprogrammierschnittstelle im App-Code für den Drittempfänger) wird man im Verhältnis von App-Publisher und Drittempfänger stets annehmen können. Schwieriger zu beurteilen ist hingegen, ob auch eine gemeinsame Entscheidung über die Zwecke der Datenverarbeitung vorliegt. Wohl anzunehmen wäre dies in Fällen, in denen der App-Publisher seinerseits vom Drittverarbeiter in irgendeiner Form Daten erhält, die aus dessen Datenerhebung bei App-Nutzern stammen; gerade bei Analyse-Anbietern ist dies häufig der Fall. In diesem Zusammenhang gibt es indessen viele Streitfragen, und die Rechtsprechung des EuGH lässt einigen Interpretationsspielraum[163] Es steht jedoch zu erwarten, dass die Rechtsprechung schon aus Praktikabilitätserwägungen eher dazu tendieren wird, den Begriff der gemeinsamen Verantwortung weit auszulegen und den App-Publisher bei der Einschaltung von Drittunternehmen als (mit[164]-)verantwortlich anzusehen.

Eine Verantwortlichkeit des App-Store-Betreibers dürfte hingegen (außer als Publisher konzerneigener Apps) tendenziell ausscheiden, da er jedenfalls im Regelfall keinen Einfluss auf den Zweck der Datenverarbeitung haben dürfte[165], was nach Art. 26 Abs. 1 S. 1 DSGVO jedoch zwingende Voraussetzung für die Annahme gemeinsamer Verantwortung ist.

Der Betroffene muss nach Artikel 13 Abs. 1, 2 DSGVO zum Zeitpunkt der Erhebung der Daten informiert werden. Dabei spielt es zunächst keine Rolle, zu welchem Zweck die empfangenen Daten verwendet werden und insoweit ein wirkliches Nutzertracking vorliegt.

---

163 S. dazu die Ausführungen im Abschlussbericht zur Sektoruntersuchung Smart-TVs (Fn. 71), S. 155 ff.

164 Bei einer gemeinsamen Verarbeitung treffen die Verantwortlichen die sich aus Artikel 13 und Artikel 14 ergebenden allgemeinen Informationspflichten gemeinsam. Die Verantwortlichen müssen in einem solchen Fall in einer Vereinbarung festlegen, wer welchen Informationspflichten nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten festgelegt sind. Der wesentliche Inhalt dieser Vereinbarung ist den Betroffenen zur Verfügung zu stellen.

165 Etwas Anderes würde freilich in dem Fall gelten, in dem der App-Store-Betreiber selbst via Tracking oder anderweitig, z. B. über Funktionalitäten des Betriebssystems, personenbezogene Daten erhielte.

In der Literatur herrscht zwar keine terminologische Einigkeit darüber, wann genau die Information dem Betroffenen vorliegen muss.[166] Es dürfte jedoch unstreitig sein, dass der Betroffene effektiv noch die Möglichkeit haben muss, nach der Kenntnisnahme der Information die Datenverarbeitung zu verweigern.[167] Die Information wird zudem in einem engen zeitlichen und visuellen Zusammenhang zum Download-Vorgang durch Betätigung der entsprechenden Schaltflächen (im Regelfall bezeichnet mit „Installieren“ oder „Laden“) stehen müssen. Einschlägige Informationen könnten demnach etwa in App-Beschreibungen oder deutlich verlinkten Datenschutzbestimmungen in App-Stores platziert werden.[168] Sofern gewährleistet ist, dass vor der erstmaligen App-Nutzung keine personenbezogenen Datenverarbeitungen stattfinden, wäre – jedenfalls bei Gratis-Apps, deren Download nicht kostenpflichtig ist – ggf. auch ein Hinweis beim ersten Aufrufen der App denkbar.

Es fällt jedoch auf, dass in entsprechenden Texten oftmals

- Verantwortlichkeiten nicht oder nicht klar benannt werden,
- Angaben über aktive Tracker/Datenempfänger fehlen, unpräzise oder unvollständig sind,
- wo App-Publisher als Verantwortliche genannt werden, essentielle nach Artikel 13 DSGVO erforderliche Informationen fehlen.

Ungeachtet der jeweiligen Verantwortlichkeitskonstellation liegen somit in den meisten Fällen Verstöße der datenschutzrechtlich Verantwortlichen gegen Artikel 13 DSGVO vor. Bemerkenswert ist dabei, dass die datenempfangenden Unternehmen sehr häufig selbst als Verantwortliche in der Pflicht stehen – ggf. gemeinsam mit dem jeweiligen App-Publisher. Im Ergebnis müssen diese Unternehmen daher dafür sorgen, dass die von ihrer Datenverarbeitung betroffenen Personen in DSGVO-konformer Weise informiert werden, etwa dadurch, dass in der App-Beschreibung im App-Store auf sie hingewiesen wird und die Datenschutzerklärung des App-Publishers

166 Z. T. wird nur eine Information „vor“ der Datenerhebung für zulässig erachtet (*Bäcker* in: Kühling/Buchner [Hrsg.], DSGVO BDSG, 3. Aufl. 2020, Rn. 56, Art. 13 DSGVO Rn. 27), z. T. auch „vor oder mit der Datenerhebung“ (*Knyrim* in: Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 13 Rn. 39; *Schmidt-Wudy* in: BeckOK Datenschutzrecht, 35. Ed., 01.05.2021, Art. 13 DSGVO Rn. 79).

167 So auch *Kühling* (vorhergehende Fn.), a. a. O.

168 Für eine Anzeige im App-Store auch *Franck* in: Gola u. a. [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 13 Rn. 36.

sie explizit benennt und, ggf. neben einer Verlinkung zur eigenen Datenschutzerklärung, die Datenverarbeitungen zumindest in wesentlichen Grundzügen dargestellt werden.[169]

cc) Lauterkeitsrechtliche Informationspflichten

Die Nichtinformation des Verbrauchers über Drittempfänger personenbezogener Daten könnte zudem eine Irreführung durch Unterlassen gemäß § 5a Abs. 2 Satz 1 UWG darstellen, zumindest für den Fall, dass Nutzerverhalten tatsächlich nachverfolgt wird, also z. B. Werbetracker eingesetzt werden[170]. Eine solche Irreführung begeht, „wer im konkreten Fall unter Berücksichtigung aller Umstände dem Verbraucher eine wesentliche Information vorenthält, die dieser je nach den Umständen benötigt, um eine informierte geschäftliche Entscheidung zu treffen und deren Vorenthalten geeignet ist, ihn zu einer geschäftlichen Entscheidung zu veranlassen, die er anderenfalls nicht getroffen hätte“. Grundsätzlich ist demnach hier die Frage maßgeblich, ob es sich bei der Information, dass das Nutzerverhalten mittels Tracking nachverfolgt wird, um eine wesentliche Information handelt.

In diesem Zusammenhang ist § 5a Abs. 4 UWG zu beachten. Hiernach gelten auch solche Informationen als wesentlich im Sinne des Absatzes 2, die dem Verbraucher auf Grund unionsrechtlicher Verordnungen oder nach Rechtsvorschriften zur Umsetzung unionsrechtlicher Richtlinien für kommerzielle Kommunikation einschließlich Werbung und Marketing nicht vorenthalten werden dürfen. Aus Art. 7 Abs. 5 der UGP-Richtlinie, dessen Umsetzung § 5a UWG dient, folgt die Wertung, dass unionsrechtlich vorgesehene Informationspflichten zugunsten des Verbrauchers stets als wesentliche Informationen anzusehen sind. Die Regelung präzisiert somit das in § 5a Abs. 2 UWG erwähnte Merkmal der Wesentlichkeit und ist immer im Zusammenhang mit den übrigen dort genannten Voraussetzungen zu sehen.[171]

Da die oben bereits erwähnte Informationspflicht über die Funktionsweise digitaler Inhalte in Art. 246a § 1 Abs. 1 S. 1 Nr. 14 EGBGB auf Art. 6 Abs. 1 lit. r) der Verbraucherrechte-Richtlinie

---

169 Soweit ersichtlich, gibt es zu der Frage der angemessenen Information der betroffenen Person bei mehreren parallelen Datenverarbeitungen bislang keine Rechtsprechung, Leitlinien oder best practices. Es liegt auf der Hand, dass in einer solchen Konstellation die leichte Zugänglichkeit der Informationen im Widerstreit steht zu den umfassenden Angaben, die die DSGVO erfordert. Nach hier vertretener Auffassung muss der Verbraucher vor der ersten Datenverarbeitung über jegliche Nutzerverfolgung in allen wesentlichen Grundzügen informiert sein, andernfalls wären die Datenverarbeitungen offensichtlich nicht transparent; Details könnten hingegen in verlinkten Datenschutzerklärungen erläutert werden.

170 Wie bereits ausgeführt, ist dies nicht notwendigerweise bei jedem Datenfluss an einen Drittempfänger der Fall.

171 *Alexander* in: Münchener Kommentar zum Lauterkeitsrecht, 3. Aufl. 2020, § 5a UWG Rn. 407.

zurückgeht, handelt es sich dabei um eine per se wesentliche Information, die keiner Wesentlichkeitsprüfung im Einzelfall zu unterziehen ist. Die übrigen Tatbestandsmerkmale des § 5a Abs. 2 UWG müssen jedoch ebenfalls erfüllt sein, wobei den Unternehmer eine sekundäre Beweislast trifft.[172] Der Verbraucher muss die ihm vorenthaltene wesentliche Information daher „je nach den Umständen benötig[en], um eine informierte Entscheidung zu treffen" und „deren Vorenthalten [muss] geeignet [sein], den Verbraucher zu einer geschäftlichen Entscheidung zu veranlassen, die er andernfalls nicht getroffen hätte". Dabei genügt eine Eignung zur Beeinflussung des Verbraucherverhaltens; es kommt nicht darauf an, ob und ggf. wie viele Marktteilnehmer tatsächlich durch eine geschäftliche Handlung betroffen und beeinflusst werden.[173] Vielmehr ist eine wertende Betrachtung erforderlich, ob die geschäftliche Handlung einen durchschnittlichen Verbraucher tatsächlich oder potentiell beeinflussen kann. Das ist insbesondere der Fall, wenn der Verbraucher dazu veranlasst werden kann, eine bestimmte geschäftliche Entscheidung zu treffen und ein Produkt zu erwerben oder nicht.[174]

Hiervon ist bei der Information, dass das Nutzerverhalten nachverfolgt und analysiert wird, auszugehen. Es kann nicht unterstellt werden, dass der Verbraucher an einer solchen Information nicht interessiert ist und diese unbeachtet lässt. Vielmehr kann angenommen werden, dass vielen App-Nutzern mangels Transparenz seitens der App-Store-Betreiber und der App-Publisher nicht bewusst ist, dass umfangreiche Informationen über ihr Nutzungsverhalten, ihr Gerät, ihr Betriebssystem u. v. m. an Dritte gesendet und von diesen ggf. auch weitergegeben werden. Die unzureichende Information kann den Verbraucher zu falschen Vorstellungen über die Erhebung von und den Umgang mit seinen Daten veranlassen. Dies wiederum lässt das Fehlen der Information geeignet erscheinen, Verbraucher zu veranlassen, ggf. eine App herunterzuladen, anstatt hiervon Abstand zu nehmen und sich nach einer Alternative umzusehen. Dies gilt umso mehr, als die jüngsten Erfahrungen mit der Datenschutz-Abfrage von *Apple*[175] darauf hindeuten, dass eine

172 BGH, Urteil vom 02.03.2017, Az. I ZR 41/16, juris Rn. 31 f. – *Komplettküchen*.

173 Vgl. *Alexander* in: Münchener Kommentar zum Lauterkeitsrecht, 3. Aufl. 2020, § 5a UWG Rn. 119 (m. w. N.).

174 A. a. O. (Fn. 173).

175 S. dazu oben S. 58.

große Menge von *iOS*-Nutzern die Verwendung von Trackern ablehnt, wenn ihnen eine entsprechende Entscheidungsmöglichkeit eingeräumt wird.[176]

Demnach lässt sich eine Informationspflicht auch aus dem Lauterkeitsrecht herleiten. Diese ist allerdings ebenso wie die verbrauchervertragsrechtliche Informationspflicht aufgrund des Abstellens auf die „Funktionsweise" der Software womöglich insoweit beschränkt, als zwar eine Information über Einsatz und Funktionsweise von Trackern, aber eine detaillierte Angabe von Datenempfängern nicht als erforderlich angesehen werden kann.

Ein anderes Bild ergibt sich, wenn man § 13 DSGVO als Marktverhaltensregel ansieht. § 3a UWG zufolge ist ein Verstoß gegen eine solche Marktverhaltensregel als unlautere Handlung anzusehen, sofern der Verstoß geeignet ist, die Interessen von Verbrauchern spürbar zu beeinträchtigen. Die Spürbarkeit der Beeinträchtigung wird man annehmen können, da es sich um eine (bevorstehende) Verletzung der informationellen Selbstbestimmung handelt, die mehr als Bagatellcharakter aufweist.[177] Heftig umstritten ist hingegen, ob sich die verletzten Vorschriften der DSGVO als Marktverhaltensregelungen im Sinne des § 3a UWG einstufen lassen bzw. ob die DSGVO ein abschließendes System darstellt, das für eine Anwendung des § 3a UWG in Verbindung mit Marktverhaltensregeln der DSGVO keinen Raum mehr lässt.[178] Letztere Ansicht wird damit begründet, dass in der DSGVO der Schutz der Persönlichkeitsrechte im Vordergrund stehe und dieser gerade nicht Zweck des Wettbewerbsrechts sei.[179] Nur die in der DSGVO genannten

---

176 *Laziuk*, *iOS 14.5* Opt-in Rate – Daily Updates Since Launch (Flurry.com, aktualisiert am 25.05.2021), abrufbar unter https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/, zufolge entschieden sich zum Stichtag 16. Mai 2021 76 Prozent der Nutzer gegen Tracking durch Dritte. In den USA lag die Quote mit 86 Prozent noch deutlich darüber, Daten für andere Staaten außer den USA werden nicht genannt. S. auch oben Abbildung 30 auf S. 59 zum Informationsinteresse der Verbraucher bzgl. des Datensendeverhaltens von Apps.

177 Schützt die Marktverhaltensregel nicht Wettbewerber, sondern Verbraucher, ist die Spürbarkeit von Verstößen nur ganz ausnahmsweise zu verneinen, s. *Schaffert* in: Münchener Kommentar zum Lauterkeitsrecht, 3. Aufl. 2020, § 3a Rn. 112.

178 Bejahend für diverse Informationspflichten des Art. 13 DSGVO OLG Stuttgart, Urteil vom 27.02.2020, Az. 2 U 257/19, juris Rn. 77 ff., allgemein bejahend für DSGVO-Vorschriften zur Nutzung von Daten zu Werbezwecken sowie speziell für Art. 9 DSGVO OLG Naumburg, Urteil vom 07.11.2019, Az. 9 U 39/18, juris Rn. 52 ff., ablehnend etwa *Köhler* in: Köhler/Bornkamm/Feddersen [Hrsg.], Gesetz gegen den unlauteren Wettbewerb, 39. Aufl. 2021, § 3a Rn. 1.74b; *Ohly*, UWG-Rechtsschutz bei Verstößen gegen die Datenschutz-Grundverordnung?, GRUR 2019, 686, 688 ff. Die Frage einer möglichen abschließenden Natur des Durchsetzungsregimes der DSGVO hat der BGH dem EuGH zur Vorabentscheidung vorgelegt, vgl. BGH, Beschluss vom 28.05.2020, Az. I ZR 186/17, juris.

179 *Köhler*, a. a. O. (vorhergehende Fn.); *Schaffert* in: Münchener Kommentar zum Lauterkeitsrecht, 3. Aufl. 2020, § 3a Rn. 84.

Einrichtungen könnten demnach Verstöße gegen die DSGVO nach den dort festgelegten Regelungen unabhängig von der Verletzung konkreter Rechte einzelner Personen geltend machen.[180] Eine andere Ansicht weist hingegen darauf hin, dass Daten zunehmend als Wirtschaftsgut zu betrachten seien, Datenschutz zunehmend zum Wettbewerbsfaktor würde und Datenschutzverstöße damit ausnahmslos als Marktverhaltensregel anzusehen seien.[181] Letzterer Ansicht ist jedenfalls zuzugeben, dass bei Datenverarbeitungen in der heutigen digitalisierten Welt Wettbewerbsbezug und Persönlichkeitsschutz in vielen Fällen eng miteinander verbunden sind. Werden etwa unter Verletzung des Rechts auf informationelle Selbstbestimmung personenbezogene Daten erhoben, kann sich dies in einem bedeutenden Wettbewerbsvorteil niederschlagen, etwa indem sie für eine zielgerichtete Werbeansprache verwendet oder weiterverkauft werden.

Sieht man mit dem OLG Stuttgart als relevantes Marktverhalten i. S. v. § 3a UWG jede Tätigkeit auf einem Markt an, die objektiv der Förderung des Absatzes oder des Bezugs von Waren oder Dienstleistungen dient und durch die ein Unternehmer auf Mitbewerber, Verbraucher oder sonstige Marktteilnehmer einwirkt[182], so lassen sich in den Kreis des § 3a UWG durchaus auch Verhaltensweisen einbeziehen, die lediglich indirekt das Marktgeschehen beeinflussen. So hat es das OLG Stuttgart genügen lassen, dass die in dem entschiedenen Fall in Frage stehenden Informationspflichten der DSGVO für die Entscheidung des Interessenten für eine Vertragsanbahnung und somit dessen Entscheidungs- und Verhaltensfreiheit in Bezug auf die Marktteilnahme maßgeblich sein können.[183]

Geht man von einem nach § 3a UWG relevanten Marktverhaltensregelverstoß aus, so würde dies bedeuten, dass jeder Verantwortliche auch nach Lauterkeitsrecht dafür Sorge tragen müsste, dass den Nutzern vor dem Download einer App oder spätestens vor der ersten Datenverarbeitung alle nach der DSGVO erforderlichen Informationen mitgeteilt werden. Letztlich würde dies dazu führen, dass sich (über Tracking-Unternehmen hinaus) dem Nutzer sämtliche verantwortlichen Unternehmen offenbaren müssten, die dessen Daten verarbeiten.

Ansprüche nach dem UWG können bislang vom einzelnen Verbraucher nicht geltend gemacht werden, sondern allenfalls von Verbraucherverbänden als qualifizierten Einrichtungen i. S. d. § 8 Abs. 3 Nr. 3 UWG. Dies wird sich zum 28. Mai 2022 mit dem Inkrafttreten des § 9 Abs. 2 UWG n. F. ändern, der auch einen Individual-Schadensersatzanspruch einräumt. Bei widerrechtlichen

---

180 Diese Frage wird nun durch den Europäischen Gerichtshof im Verfahren C-319/20 geprüft; s. dazu den Vorlagebeschluss des BGH vom 28.05.2020, Az. I ZR 186/17, juris – App-Zentrum.

181 *Wolff*, UWG und DS-GVO: Zwei separate Kreise?, ZD 2018, 248, 251.

182 OLG Stuttgart, Urteil vom 08.06.2017, Az. 2 U 127/16, juris Rn. 28.

183 OLG Stuttgart, Urteil vom 27.02.2020, Az. 2 U 257/19, juris Rn. 81 ff.

Datenverarbeitungen dürfte es dem Einzelnen zwar schon kaum möglich sein, einen erlittenen Schaden überhaupt monetär zu beziffern. Die Abschreckungswirkung dürfte daher in diesem Zusammenhang äußerst gering ausfallen. Allerdings gilt im Rahmen des aktuellen § 9 Abs. 1 UWG, dass auf den dort vorgesehenen Schadensersatzanspruch von Wettbewerbern in Ermangelung spezieller UWG-Regelungen die § § 249 ff. BGB anwendbar sind und damit auch der Grundsatz der Naturalrestitution nach § 249 Abs. 1 BGB einschlägig ist.[184] In Anbetracht der Vorgabe des europäischen Rechts im neuen Art. 11a Abs. 1 S. 1 der UGP-Richtlinie[185], dass Verbraucher, die durch unlautere Geschäftspraktiken geschädigt wurden, Zugang zu angemessenen und wirksamen Rechtsbehelfen, einschließlich Schadensersatz sowie gegebenenfalls Preisminderung oder Beendigung des Vertrags haben müssen, kann der Verbraucherschadensersatzanspruch des § 9 Abs. 2 UWG n. F. nicht hinter den Möglichkeiten des § 9 Abs.1 UWG zurückbleiben. Es wird abzuwarten bleiben, wie die Rechtsprechung diesen Schadensersatzanspruch letztlich ausfüllt. Es wäre indessen konsequent, dem einzelnen Verbraucher einen Folgenbeseitigungsanspruch zuzugestehen, der die Löschung aller widerrechtlich erhaltenen personenbezogenen Daten beinhaltet – und zwar beim Verantwortlichen ebenso wie bei sämtlichen Dritten, an die der Verantwortliche personenbezogene Daten weitergegeben hat (wofür der in Anspruch genommene Verantwortliche sorgen müsste).

4. Notwendigkeit von Einwilligungen

Senden Apps personenbezogene Daten an Drittempfänger, so stellt sich über eine entsprechende Pflicht zur Information der betroffenen Personen hinaus die Frage, ob diese nicht womöglich sogar in eine solche Datenverarbeitung einwilligen müssten. Derzeit werden App-Nutzer nur selten um Einwilligungen ersucht. So forderten einer Studie von Forschern der Universität Oxford zufolge nur rund 10 % der untersuchten Apps eine Einwilligung an, obwohl rund 70 % hiervon Trackingsoftware einsetzten.[186]

a) Einwilligungspflicht nach DSGVO

Es lässt sich schwer pauschal beurteilen, inwieweit der durch den App-Code ausgelöste Empfang personenbezogener Daten durch Dritte nicht nur gegenüber der betroffenen Person transparent

---

184 S. *Fritzsche* in: Münchener Kommentar zum Lauterkeitsrecht, 2. Aufl. 2014, § 9, Rn. 64; *Köhler* in: Köhler/Bornkamm/Feddersen [Hrsg.], Gesetz gegen den unlauteren Wettbewerb, 39. Aufl. 2021, § 9 UWG, Rn. 1.24.

185 Eingeführt durch Art. 3 Ziff. 5 der Omnibus-Richtlinie von 2019 (Fn. 86).

186 *Kollnig u. a.*, A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps, S. 7, vorläufige Fassung abrufbar unter https://ora.ox.ac.uk/objects/uuid:67012963-64c3-496e-b793-abb5f868a47e.

gemacht werden muss, sondern darüber hinaus jeweils eine Einwilligung der betroffenen Person nach Art. 6 Abs. 1 lit. a) DSGVO erfordert. Soweit App-Publisher[187] in ihren Datenschutzerklärungen hierzu überhaupt substantielle Ausführungen machen, verweisen sie zumeist auf die Rechtfertigungsgründe der Erforderlichkeit zur Vertragserfüllung (Art. 6 Abs. 1 lit. b) DSGVO) oder der berechtigten Interessen (Art. 6 Abs. 1 lit. f) DSGVO).

Wie bereits im Rahmen des Abschlussberichts der Sektoruntersuchung Smart-TVs vertreten, ist beim Rechtfertigungsgrund der Erforderlichkeit der Datenverarbeitung zur Vertragserfüllung ein enger Maßstab anzulegen.[188] Insbesondere ist die Monetarisierung eines Dienstes ein Interesse des App-Publishers und die zu Werbezwecken erfolgende Verarbeitung personenbezogener Daten des Nutzers nicht im hier relevanten technischen Sinne erforderlich, um die vertragliche Leistung zu erbringen. Jedenfalls insoweit wäre die Berufung auf Art. 6 Abs. 1 lit. b) DSGVO nicht tragfähig.

Der Rechtfertigungsgrund der berechtigten Interessen setzt eine umfassende Abwägung der vom Verantwortlichen ins Feld geführten Interessen mit denen der betroffenen Person voraus. Dabei sind alle Umstände des Einzelfalls einzubeziehen. Von wesentlicher Bedeutung ist dabei insbesondere, wie schwer sich die Datenverarbeitung aufseiten der betroffenen Person auswirkt.[189] Letzteres hängt wiederum ganz maßgeblich von den konkret erhobenen Daten und Aspekten wie Speicherdauer oder Datenweitergabe an Dritte ab.[190] Hierzu finden sich in den Datenschutzerklärungen der App-Publisher ganz überwiegend keine oder nur unvollständige Angaben. Auf dieser Basis ist eine Abwägung somit kaum möglich, denn das Ausmaß der Beeinträchtigung der informationellen Selbstbestimmung der betroffenen Person lässt sich nicht ermessen. In diesem Zusammenhang wird mitunter vertreten, dass eine Rechtfertigung aufgrund berechtigter Interessen zumindest im Falle von Nutzertracking regelmäßig ausscheidet, da es sich hierbei aus Sicht der betroffenen Person um Hochrisiko-Datenverarbeitungen handelt.[191] Es ließe sich auch argu-

---

187 Zur Verantwortlicheneigenschaft von App-Publishern siehe oben, S. 70.

188 Siehe dazu Abschlussbericht der Sektoruntersuchung Smart-TVs (Fn. 71), S. 114 ff.

189 Ausführlich dazu Abschlussbericht der Sektoruntersuchung Smart-TVs (Fn. 71), S. 119 ff.

190 Die Datenschutzkonferenz nennt als wichtige Abwägungskriterien die vernünftige Erwartung der betroffenen Personen, Vorhersehbarkeit / Transparenz, Interventionsmöglichkeiten der betroffenen Personen, Verkettung von Datend, beteiligte Akteure, Dauer der Beobachtung, Kreis der Betroffenen, Datenkategorien und Umfang der Datenverarbeitung, s. *Datenschutzkonferenz*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien (Stand: März 2019), S. 16, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/04/Orientierungshilfe-der-Aufsichtsbeh%C3%B6rden-f%C3%BCr-Anbieter-von-Telemedien.pdf.

191 *Kollnig u. a.*, a. a. O. (Fn. 186), S. 5.

mentieren, dass im Rahmen der Erforderlichkeitsprüfung stets die Frage nach möglichen milderen Mitteln zu stellen wäre. Zu Monetarisierungszwecken wären mithin etwa das Einblenden nicht interessenbasierter Werbung oder das Angebot eines Trackingverzichts gegen Bezahlung vorstellbar. Vor diesem Hintergrund erscheint die Berufung auf berechtigte Interessen zur Rechtfertigung der Verarbeitung personenbezogener Daten in vielen Fällen fragwürdig.

b) Einwilligungspflicht nach TMG/TTDSG

Art. 5 Abs. 3 der ePrivacy-Richtlinie[192] sieht sinngemäß vor, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn dieser hierzu seine informierte Einwilligung gegeben hat. Diese Pflicht gilt unabhängig davon, wer die Daten empfängt und sogar unabhängig davon, ob es sich um personenbezogene Daten handelt oder nicht.

Art. 5 Abs. 3 der ePrivacy-Richtlinie wurde zwar in Deutschland bislang nicht in nationales Recht umgesetzt. Der BGH hat jedoch in seinem Urteil *Planet 49* entschieden, dass § 15 Abs. 3 TMG – obwohl er nie als Art. 5 Abs. 3 der ePrivacy-Richtlinie umsetzende Norm konzipiert war – im Lichte der der ePrivacy-Richtlinie ausgelegt werden könne.[193] § 15 Abs. 3 S. 1 TMG zufolge darf ein Diensteanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Unter Berücksichtigung des EuGH-Urteils[194], welches auf einen Vorlagebeschluss des BGH hin zuvor in der gleichen Sache ergangen war, führte der BGH aus, dass eine richtlinienkonforme Auslegung im Wege der teleologischen Reduktion auch über den Wortlaut der nationalen Norm hinaus möglich sei.[195] § 15 Abs. 3 TMG ist nach Auffassung des BGH mithin dahingehend auszulegen, dass ein fehlender Nutzerwiderspruch nicht ausreicht. Vielmehr dürfe der Diensteanbieter Cookies zur Erstellung von Nutzungsprofilen für Zwecke der Werbung oder Marktforschung nicht einsetzen, wenn die Einwilligung des Nutzers mittels eines

---

192 Richtlinie 2002/58/EG des Europäischen Parlaments und Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. EU L 201 vom 31.7.2002, S. 37), in der durch Art. 2 Nr. 5 der Richtlinie 2009/136/EG geänderten Fassung, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02002L0058-20091219&from=EN.

193 BGH, Urteil vom 28.05.2020, Az. I ZR 7/16, juris Rn. 54 – *Planet 49*.

194 EuGH, Urteil vom 01.10.2019 in der Rs. C-673/17, ECLI:EU:C:2019:801 – *Verbraucherzentrale Bundesverband/Planet49*.

195 BGH, a. a. O. (Fn. 193), juris Rn. 53.

voreingestellten Ankreuzkästchens eingeholt werde, das der Nutzer zur Verweigerung seiner Einwilligung abwählen müsse.[196]

Vor diesem Hintergrund ließe sich § 15 Abs. 3 TMG in der europarechtskonformen Auslegung durch den Bundesgerichtshof grundsätzlich auch auf Telemediendienste anbietende App-Publisher anwenden, die für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien pseudonymisierte Nutzungsprofile erstellen. Greifen solche App-Publisher aus diesem Grund auf (personenbezogene oder auch sonstige) Daten auf einem Smartphone oder Tablet zu, wäre hierfür eine informierte Einwilligung der betroffenen Person erforderlich. Inwieweit die explizit auf den Diensteanbieter abstellende Norm jedoch auch auf Datenerhebungen anwendbar wäre, die im Ergebnis nicht zu einer Nutzerprofilbildung durch den Telemedienanbieter selbst (wie im Fall *Planet 49*), sondern ausschließlich bei Drittunternehmen führen würden, ist fraglich.

Eine Anpassung der Regelungen von TKG und TMG an DSGVO und ePrivacy-Richtlinie bringt nunmehr das am 01.12.2021 in Kraft tretende TTDSG[197] mit sich. Jeglicher Zugriff auf Daten, die auf einem Endgerät des Nutzers gespeichert sind, erfordert nach § 25 Abs. 1 TTDSG grundsätzlich eine Einwilligung des Nutzers auf der Grundlage von klaren und umfassenden Informationen, wobei die Regelungen der DSGVO hinsichtlich der Einwilligung und der vorab zu erteilenden Informationen einzuhalten sind. Weitestgehend gleichlaufend mit Art. 5 Abs. 3 der ePrivacy-Richtlinie sieht § 25 Abs. 2 TTDSG eng umrissene Ausnahmen von der Einwilligungspflicht nur in Fällen vor, in denen

- der alleinige Zweck der betreffenden Datenverarbeitungen die Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist (Nr. 1) oder
- die Datenverarbeitungen unbedingt erforderlich sind, damit der Telemediendienstanbieter einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann (Nr. 2).

Eine weitere Ausnahme zur Einholung einer Einwilligung, wie sie etwa Art. 6 Abs. 1 lit. f) DSGVO für die Datenverarbeitung bei Vorliegen berechtigter Interessen ermöglicht, sieht das TTDSG nicht vor. Ein Zugriff auf Daten auf dem Endgerät eines Nutzers würde somit (vorbehaltlich der vorgenannten Ausnahmen) zwingend eine Einwilligung erfordern, die gem. § 25 Abs. 1 S. 2 TTDSG den Anforderungen der DSGVO entsprechen müsste.

196 Vgl. BGH, a. a. O. (Fn. 193), juris Rn. 52.

197 S. Fn. 127.

5. Einzelne Transparenzaspekte

Im zeitlichen Rahmen der Ermittlungen war es nicht möglich, eine umfassende Analyse der Datenschutzerklärungen der 32 ausgesuchten *Android*-Apps vorzunehmen. Zumindest auf einige wesentliche Transparenz-Aspekte hin hat das Bundeskartellamt die Texte dennoch untersucht.

a) Ermittlungen

Im Gegensatz zur oben dargestellten Prüfung auf das Abfließen personenbezogener Daten an Drittunternehmen und entsprechende Information der Verbraucher soll in diesem Abschnitt anhand einiger wesentlicher Datenschutz-Gesichtspunkte darauf eingegangen werden, wie die App-Publisher *selbst* mit den Daten der Verbraucher umgehen. Die Datenschutzbestimmungen der App-Publisher sind in *Google Play* jeweils unter „Kontaktdaten des Entwicklers" verlinkt. Das bedeutet, dass zunächst die App-Seite aufgerufen und nach unten bis zum Abschnitt *Kontaktdaten des Entwicklers* gescrollt werden muss, der sich unterhalb einer kurzen App-Beschreibung und in der Regel mehreren Nutzerrezensionen befindet. Der Abschnitt muss sodann durch Klicken auf das Symbol ⌄ geöffnet werden. Ein Klick auf die dort verlinkte Datenschutzerklärung führt dann zu einer Internetseite des App-Publishers, die im Standardbrowser geöffnet wird.

aa) Einfache Zugänglichkeit der Datenschutzerklärungen

Zunächst wurde geprüft, inwieweit bei den 32 ausgesuchten *Android*-Apps Datenschutzerklärungen in der App-Beschreibung verlinkt waren oder jedenfalls bei Erstnutzung einer App die Datenschutzerklärung angezeigt oder verlinkt wurde, bevor[198] personenbezogene Daten übermittelt wurden (etwa im Rahmen einer Registrierung). Des Weiteren wurde untersucht, ob auf den Datenschutzerklärungs-Webseiten eine Nachverfolgung (falls vorhanden) über ein fair gestaltetes Abfragebanner schnell und effektiv[199] abgestellt werden kann.

Die folgende Übersicht zeigt, wie Datenschutzerklärungen der Apps von *Google Play* aus abrufbar sind bzw. ob diese bei der Erstnutzung einer App angezeigt werden:

---

198 Es wurde hierbei nicht forensisch geprüft, ob ggf. bereits vor Abrufbarkeit der Datenschutzerklärung womöglich bereits personenbezogene Daten übermittelt wurden (z. B. Geräte-ID o- Ä.).

199 Hier wurde davon ausgegangen, dass der Nutzer – bei fairer und klarer Darstellung der Privatsphäre-Optionen – mit einem Klick alle nicht erforderlichen Datenübermittlungen abschalten können muss.

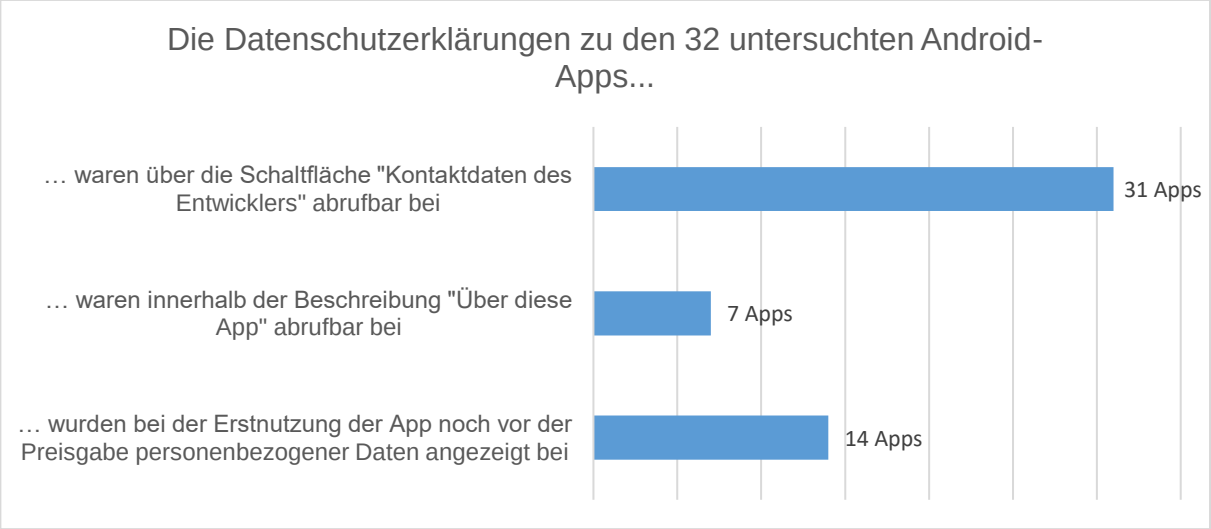


Abbildung 32: Abrufbarkeit/Anzeige von App-Datenschutzerklärungen

Des Weiteren wurden die für die betreffenden Apps auf *Google Play* verlinkten Datenschutzerklärungs-Webseiten daraufhin untersucht, in welcher Sprache sie zur Verfügung standen[200], ob sie Nutzertrackingmethoden enthielten und, falls ja, ob das Nutzertracking mit einem Klick abgestellt werden konnte:

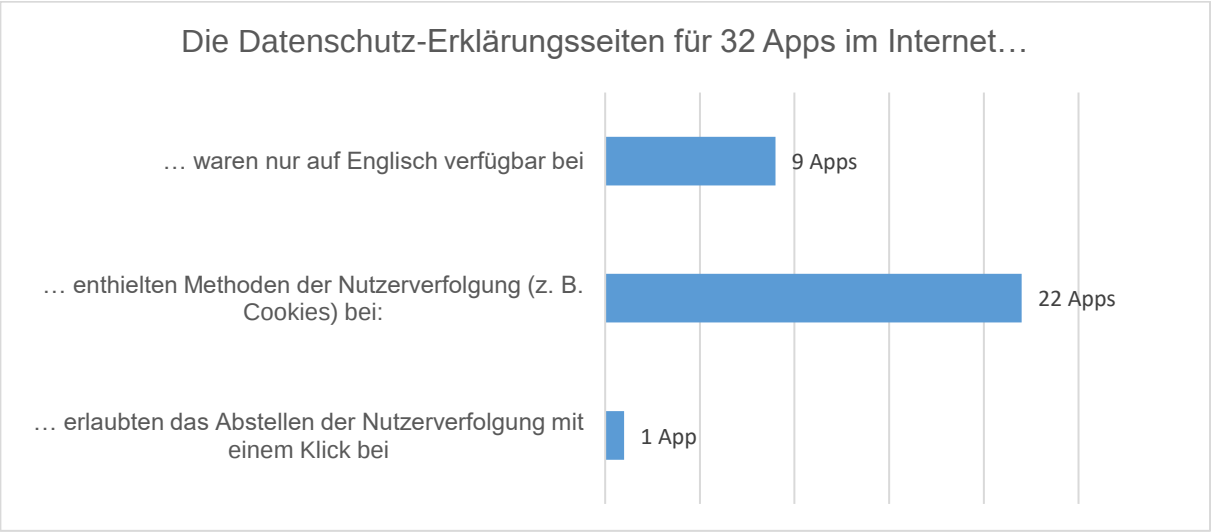


Abbildung 33: Nutzertracking auf Webseiten mit Datenschutzerklärungen

bb) Inhalt der Datenschutzerklärungen

Für die 32 ausgesuchten Apps wurden ferner jeweils die in *Google Play* verlinkten Datenschutzerklärungen daraufhin analysiert, ob

200 Als auf Deutsch zur Verfügung stehend wurden auch Datenschutzerklärungen angesehen, die man problemlos auf Deutsch umstellen konnte, etwa in einem Pulldown-Menü.

- bei einer Datenübermittlung in Drittstaaten die Drittstaaten genau benannt sind,
- bei einer Weitergabe personenbezogener Daten an Dritte genau dargestellt ist, wer diese Daten erhalten soll,
- ob die Speicherdauer erhobener personenbezogener Daten erkennbar ist.

Dem Nutzer wird so ermöglicht, die Konditionen zu erfassen und ggf. zu vergleichen und sich ggf. für eine alternative App zu entscheiden, sofern eine solche existiert. Ob die transparente Darstellung auch inhaltlich den Vorgaben der DSGVO genügt, wird dabei nicht beurteilt.

Die Untersuchung zeigt, dass rund zwei Drittel der Datenschutzerklärungen die Empfänger von personenbezogenen Daten nicht oder allenfalls in sehr groben Kategorien (z. B. „unsere Geschäftspartner“) bezeichneten.

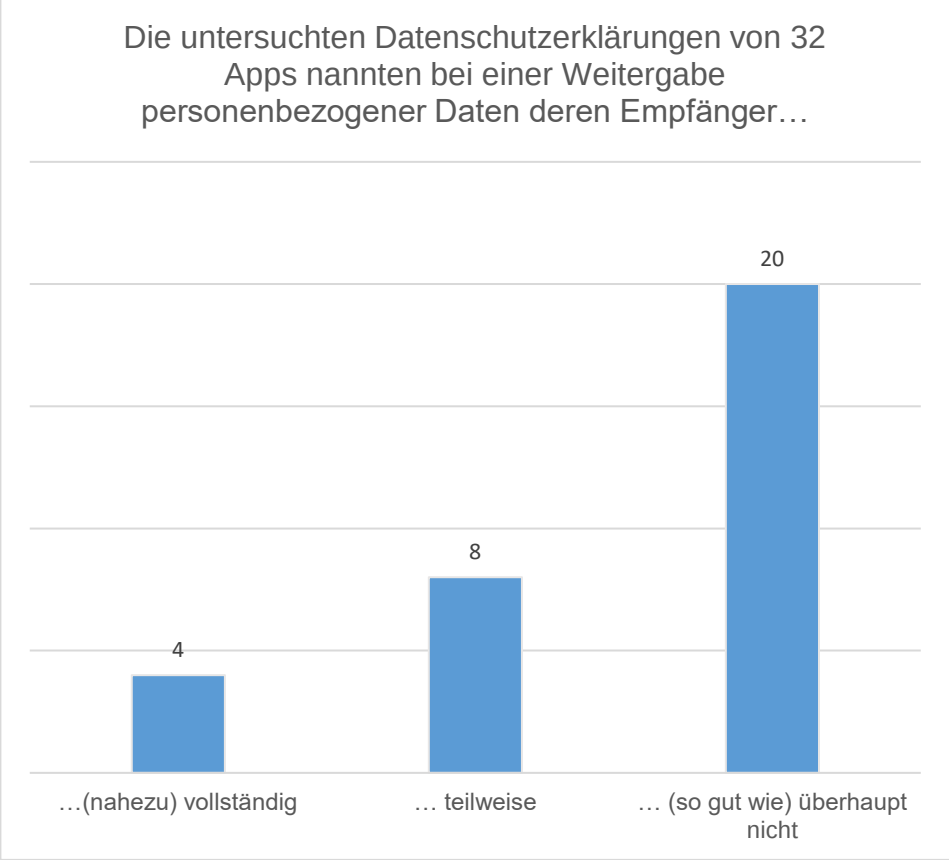


Abbildung 34: Konkrete Nennung von Datenempfängern in mit Datenschutzerklärungen

Nahezu alle untersuchten Apps lassen die Nutzer darüber im Unklaren, in welchen Staaten personenbezogenen Daten konkret gespeichert werden, die vom Nutzer erhoben werden:

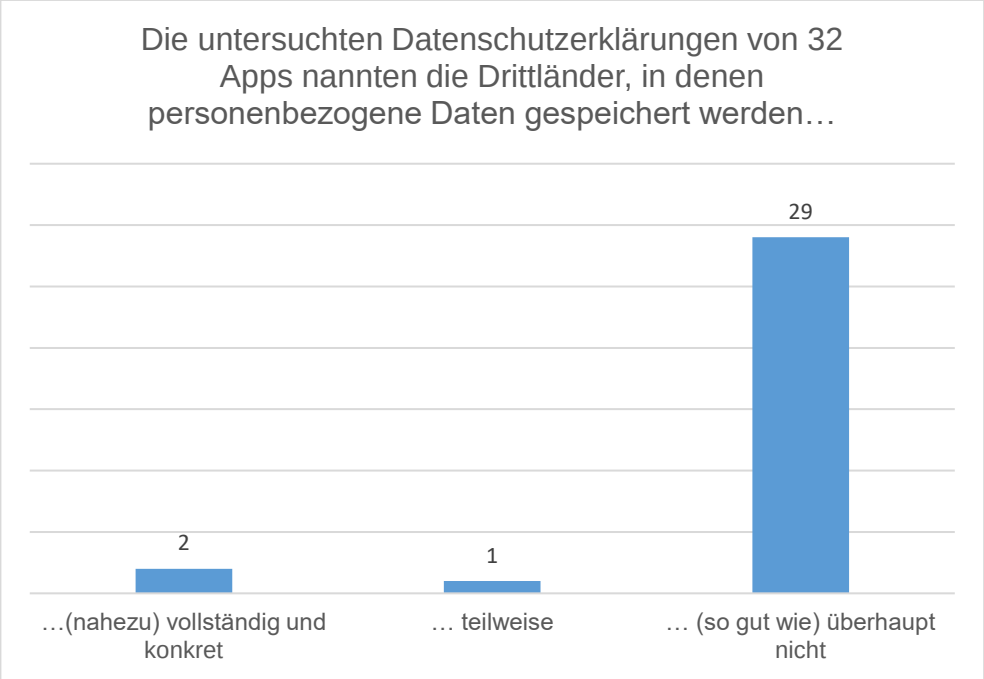


Abbildung 35: Konkrete Nennung von Speicherorten in Datenschutzerklärungen

Schließlich finden sich nur in den wenigsten Datenschutzerklärungen belastbare Aussagen dazu, welche personenbezogenen Daten wie lange gespeichert werden. Die meisten Datenschutzerklärungen begnügen sich hier mit Standardformeln wie „Wir speichern Ihre Daten so lange wie dies für unsere Zwecke erforderlich ist."

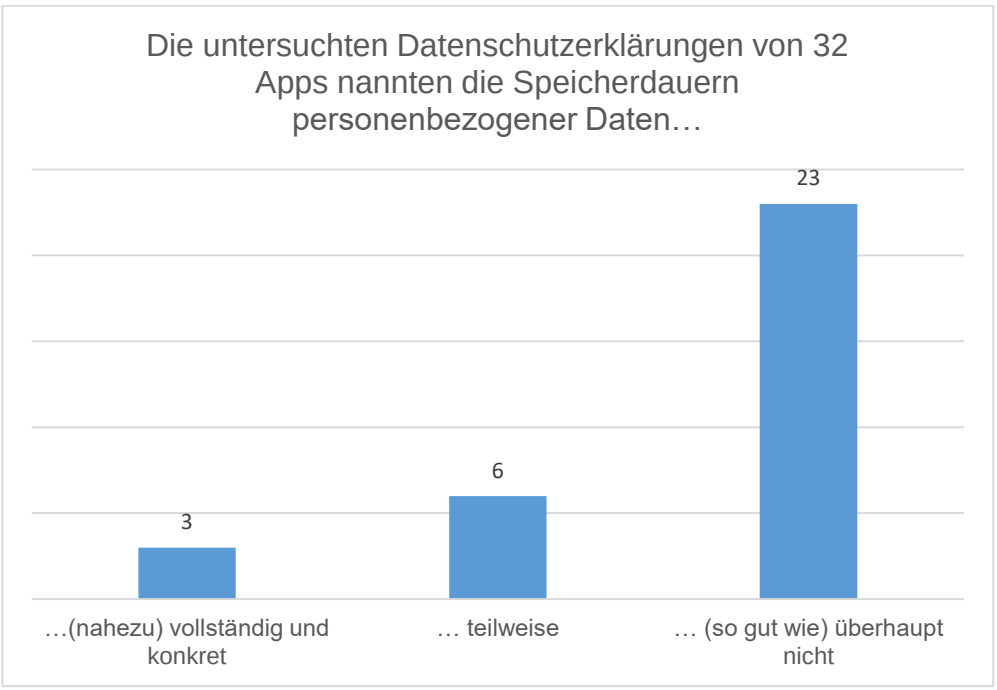


Abbildung 36: Konkrete Nennung von Speicherdauern in Datenschutzerklärungen

b) Würdigung

Praktisch alle untersuchten Datenschutzerklärungen wiesen dieselben Unzulänglichkeiten auf, die bereits in der Sektoruntersuchung Smart-TVs[201] festgestellt wurden. Nach hier vertretener Auffassung muss dem Nutzer stets verdeutlicht werden, welche Daten genau für welchen Zweck verarbeitet werden und was anschließend mit diesen Daten geschieht. An einer solchen Legitimationskette für die einzelnen Datenverarbeitungen fehlt es in nahezu allen betrachteten Datenschutzerklärungen.

Nachfolgend soll dargestellt werden, ob und inwieweit die Zugänglichkeit der Datenschutzerklärungen und die (ggf. unterbliebene) Darstellung der oben unter a) untersuchten Datenverarbeitungsaspekte rechtlichen Bedenken begegnen.

aa) Auffinden der Datenschutzerklärungswebseiten

Will sich der Nutzer umfassend über die Datenschutzbestimmungen eines App-Publishers informieren, muss er diese in der Regel auf dessen Website nachlesen. Hier stellt sich bereits das erste wesentliche Problem: Der Nutzer von *Google Play* muss den Link zur Datenschutzerklärung finden. Unter der Rubrik *Kontaktdaten des Entwicklers* wird ein unbefangener Nutzer jedoch normalerweise die Nennung der Firma des App-Publishers samt E-Mail-Adresse sowie ggf. Unternehmenswebsite und Telefonnummer vermuten. Eine Datenschutzerklärung hat hingegen mit Kontaktdaten nichts zu tun.

Der Verantwortliche muss gemäß Artikel 12 Abs. 1 DSGVO jedoch geeignete Maßnahmen ergreifen, um der betroffenen Person alle Informationen, die sich auf die Verarbeitung ihrer personenbezogenen Daten beziehen, „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache […] zu übermitteln“. Hier fehlt es bereits an einer leichten Zugänglichkeit, da die gesamte Datenschutzerklärung unter dem Abschnitt Kontaktdaten des Entwicklers nicht zu erwarten ist.

Zwar kann der App-Publisher die Präsentation seiner App nicht in allen Details bestimmen; er hat jedoch grundsätzlich die Möglichkeit, die Beschreibung seiner App frei zu gestalten und auch Links einzufügen. Es wäre in diesem Rahmen also möglich, eine Verlinkung zur eigenen Datenschutzerklärung an prominenter Stelle und hervorgehoben zu platzieren.

Die meisten App-Publisher haben von dieser Möglichkeit jedoch bislang keinen Gebrauch gemacht.

---

201 Siehe Abschlussbericht der Sektoruntersuchung Smart-TVs (Fn. 71), insb. S. 58 ff.

bb) Sprache der Datenschutzerklärungswebseiten

Für 9 der untersuchten Apps standen den Verbrauchern in *Google Play* die Datenschutzerklärungen nur in englischer Sprache zur Verfügung.[202]

Art. 12 Abs. 1 DSGVO regelt nicht ausdrücklich, in welcher Sprache die notwendigen Informationen zu Datenverarbeitungen zu übermitteln sind.[203] Allerdings wird die Verwendung einer verständlichen Sprache vorgeschrieben. Entscheidend für die Verständlichkeit und damit für die Auswahl der richtigen Sprache ist der vom Verantwortlichen intendierte Empfängerkreis[204], zu dem grundsätzlich auch Kinder[205] zählen können. Eine solche Auslegung des Verständlichkeitsgebots legt auch Erwägungsgrund 58 der DSGVO nahe, der eine verständliche Sprache hinsichtlich einer „für die Öffentlichkeit oder die betroffene Person bestimmte Information" fordert.[206] Bei der Bestimmung der jeweiligen Sprache ist das in Art. 3 Abs. 2 DSGVO normierte Marktortprinzip zu berücksichtigen, so dass die Datenschutzerklärung jedenfalls in den Sprachen der Länder verfügbar sein muss, in denen der Verantwortliche seine Leistung anbietet.[207] Bei einer Übersetzung muss der Verantwortliche zudem darauf achten, dass alle Übersetzungen korrekt sind und die Ausdrucksweise und der Satzbau Sinn ergeben, sodass der Text nicht erneut interpretationsbedürftig ist.[208]

---

202 Davon konnten in zwei Fällen zumindest bei der Erstnutzung der App die Datenschutzerklärungen in deutscher Sprache aufgerufen werden.

203 *Hennemann* in: Paal/Pauly [Hrsg.], DSGVO BDSG, Art. 12 DSGVO Rn. 35; *Steinrötter* in: BeckOK IT-Recht, 2. Ed. 1.5.2021, DS-GVO Art. 12 Rn. 17.

204 *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679" (WP 260 rev. 01 vom 11.04.2018), Rn. 13, abrufbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 (zip-Datei); *Quaas* in: BeckOK DatenschutzR, 36. Ed. 1.5.2021, DS-GVO Art. 12 Rn. 20.

205 Die niederländische Datenschutzaufsichtsbehörde hat *TikTok* im April ein Bußgeld von 750.000 Euro dafür auferlegt, dass das Unternehmen gut zwei Jahre lang keine Datenschutzerklärung in niederländischer Sprache angeboten hatte; die Entscheidung, die maßgeblich darauf abstellt, dass zu den Kunden *TikToks* auch viele Kinder zählen, ist abrufbar unter https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/decision_to_impose_a_fine_on_tiktok.pdf (in Englisch) .

206 *Quaas* in: BeckOK DatenschutzR, 36. Ed. 1.5.2021, DS-GVO Art. 12 Rn. 20.

207 *Franck* in: Gola DS-GVO, 2. Aufl. 2018, DS-GVO Art. 12 Rn. 20; *Heckmann/Scheurer* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl., Kap. 9 (Stand: 01.06.2021); *Hennemann* in: Paal/Pauly [Hrsg.], DSGVO BDSG, Art. 12 DSGVO Rn. 35; *Paschke* in: Ehmann/Selmayr/Heckmann, 2. Aufl. 2018, DS-GVO Art. 12 Rn. 19; *Steinrötter* in: BeckOK IT-Recht, 2. Ed. 1.5.2021, DS-GVO Art. 12 Rn. 17; s. auch Abschlussbericht der Sektoruntersuchung Smart-TVs (Fn. 71), S. 66 f.

208 S. hierzu *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (Fn.204), Rn. 13.

Da die getesteten Apps im *Google Play*-Store deutschen Verbrauchern angeboten werden, müssen die entsprechenden Datenschutzerklärungen folglich jedenfalls auch auf Deutsch abrufbar sein.[209] Eine Datenschutzerklärung, die für deutsche Verbraucher nur in englischer Sprache zur Verfügung steht, verstößt daher gegen Art. 12 Abs. 1 S. 1 DSGVO.

cc) Nutzertracking auf Datenschutzerklärungswebseiten

Klickt der Nutzer auf die Verlinkung zur Datenschutzerklärung eines App-Publishers, so verlässt er die Umgebung von *Google Play* und begibt sich auf die verlinkte Internetseite des App-Publishers. Es kann vorkommen, dass auf der Webseite mit der Datenschutzerklärung Tracker eingesetzt werden, die personenbezogene Daten des Nutzers an den App-Publisher oder Dritte übermitteln können. Ein solches Vorgehen seitens des App-Publishers ist jedoch unter mehreren Aspekten bedenklich. Will nämlich der Nutzer die Verarbeitung seiner personenbezogenen Daten durch eine App, für die er sich interessiert, vermeiden, so muss er sich zusätzlich gegen die Verarbeitung seiner personenbezogenen Daten auf der Webseite des App-Publishers zur Wehr setzen. Der Einsatz von Trackingmethoden auf Datenschutzerklärungsseiten ist daher zum einen im Hinblick auf Art. 12 Abs. 1 DSGVO bedenklich. Diesem zufolge muss der Verantwortliche insbesondere die nach Artikel 13 DSGVO erforderlichen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form zugänglich machen. Ferner verlangt Art. 5 Abs. 1 lit. a) DSGVO, dass personenbezogene Daten nach Treu und Glauben und in nachvollziehbarer Weise verarbeitet werden. Jedenfalls die Grundsätze von Treu und Glauben sowie der leichten Zugänglichkeit sind allenfalls dann gewahrt, wenn eine auf der Datenschutzerklärungswebsite stattfindende Erhebung personenbezogener Daten ohne Weiteres verhindert werden kann. Sofern eine entsprechende Webseite nicht gänzlich ohne Trackingmethoden auskommt, muss die Nutzerverfolgung daher schnell und effektiv abstellbar sein, ohne dass der Nutzer durch optische oder anderweitige Anreize dazu verleitet wird, der Datenverarbeitung zuzustimmen. Als Maßstab kann dabei auf die Grundsätze zu Cookie-Bannern, die sich in Behördenpraxis, Rechtsprechung und Gesetzgebung herausgebildet haben, abgestellt werden.

Wie bereits oben dargestellt[210], wäre zurzeit noch § 15 Abs. 3 TMG in unionsrechtskonformer Auslegung anwendbar auf die Anforderungen an die Nachverfolgung des Nutzerverhaltens (z. B. in Form des Setzens von Cookies). Der Websitebetreiber als Diensteanbieter müsste demnach

---

209 Ob darüber hinaus auch Übersetzungen in andere Sprachen als die Landessprache notwendig sind, ist in der Literatur umstritten (dies bejahend: *Dix* in: Simitis/Hornung/Spiecker, Datenschutzrecht, 1. Aufl. 2019, DSGVO Art. 12, Rn. 15; *Hennemann* in: Paal/Pauly [Hrsg.], DSGVO BDSG, Art. 12 DSGVO Rn. 35; ablehnend: *Steinrötter* in: BeckOK IT-Recht, 2. Ed. 1.5.2021, DS-GVO Art. 12 Rn. 17).

210 S. dazu Abschnitt E.III.4.b) auf S. 79.

eine Einwilligung des Endgerätenutzers einholen, sollte er dessen Daten zu Werbe-, Marktforschungs- oder Produktweiterentwicklungszwecken für eine Nutzerprofilbildung verwenden. Der am 01.12.2021 in Kraft tretende § 25 TTDSG sieht hingegen in Umsetzung von Art. 5 Abs. 3 der ePrivacy-Richtlinie ausdrücklich vor, dass jeglicher Datenzugriff auf dem Endgerät eines Nutzers eine informierte Einwilligung erfordert, die den Anforderungen der DSGVO entspricht.

Bislang ist indessen nicht abschließend geklärt, wie Cookie-Banner konkret gestaltet werden müssen, um den Vorgaben von Transparenz und Fairness Genüge zu tun, wie sie insbesondere in der DSGVO zum Ausdruck kommen.

Ganz offensichtlich unzulässig ist es, wenn App-Publisher auf ihren Datenschutzerklärungsseiten Third-Party-Tracker einsetzen, die der Nutzer nur blockieren kann, wenn er sich per Klick auf verlinkte Datenschutzerklärungen von datenempfangenden Drittunternehmen begibt. Eine solche Datenschutzerklärungskaskade kann sich theoretisch unendlich fortsetzen. Die Verweisung auf Drittseiten zur Abstellung von weiteren Datenverarbeitungen widerspricht daher bereits im Ansatz der Notwendigkeit, dem Nutzer die zu einer App gehörige Datenschutzerklärung unter Wahrung insbesondere der Grundsätze von Treu und Glauben und leichter Zugänglichkeit anzuzeigen.

Mit Fragen der Einwilligung in die Nutzung von Cookies und anderen Tracking-Tools hat sich u. a. die französische Datenschutzbehörde *Commission nationale de l'informatique et des libertés* (CNIL) beschäftigt und eine entsprechende Empfehlung[211] sowie Leitlinien[212] erlassen. Diesen Texten ist zu entnehmen, dass eine wirksame Cookie-Einwilligung insbesondere voraussetzt, dass eine Ablehnung von Cookies und anderen Tracking-Tools ebenso einfach sein muss wie deren Annahme[213], wobei von Designelementen abzusehen ist, die den Nutzer zur Einwilligung verleiten.[214] Des Weiteren nennt die *CNIL* als wesentliche Voraussetzungen einer wirksamen Einwilligung klare Angaben bzgl. der für die Datenverarbeitung Verantwortlichen, der Zwecke der

---

211 CNIL, Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux «cookies et autres traceurs», abrufbar unter https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf.

212 CNIL, Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux «cookies et autres traceurs») et abrogeant la délibération n°2019-093 du 4 juillet 2019, abrufbar unter https://www.cnil.fr/sites/default/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf.

213 *CNIL*-Empfehlung (Fn. 211), Rn. 30 ff.

214 *CNIL*-Empfehlung (Fn. 211), Rn. 34.

Verarbeitung, der Folgen einer Annahme/Ablehnung und des Bestehens eines Widerrufsrechts.[215]

Für die Zwecke der Sektoruntersuchung wurde auf den aus Sicht des Bundeskartellamts wichtigsten Punkt, die einfache Ablehnungsmöglichkeit des Nutzertrackings, maßgeblich abgestellt. Das Ergebnis der Prüfung kann man nur als ernüchternd bezeichnen. Lediglich bei 10 der 32 geprüften *Android*-Apps kamen entweder keine Nutzungsverfolgungsmethoden zum Einsatz oder ließen sich diese datenschutzrechtlich einwandfrei schnell und effektiv abstellen.[216] Die anderen Webseiten weisen, jedenfalls nach hier vertretener Auffassung, datenschutzrechtliche Verstöße auf.

dd) Angabe von Datenempfängern bei Weitergabe von Daten

Übermittelt ein Verantwortlicher Daten an Andere, so muss er nach Art. 13 Abs. 1 lit. e) DSGVO diese Empfänger konkret oder nach Kategorien benennen. Dem Wortlaut nach kann er sich somit auch dann auf die Nennung von Empfängerkategorien beschränken, wenn ihm eine konkrete Nennung der einzelnen Empfänger möglich wäre. Demgegenüber hat die Artikel-29-Datenschutzgruppe die Auffassung vertreten, der Verantwortliche müsse die für die betroffene Person aussagekräftigste Variante wählen. Nur dies genüge dem in Art. 5 Abs. 1 lit. a) DSGVO niedergelegten Grundsatz von Treu und Glauben. Empfänger personenbezogener Daten wären demnach im Regelfall konkret zu benennen.[217] Dem ist – auch vor dem Hintergrund des Präzisions-

215 *CNIL*-Leitlinien (Fn. 212), Rn. 24.

216 Dass dies ein Problem ist, das eine Vielzahl von Websites betrifft, zeigt die entsprechende Untersuchung der Datenschutz-Organisation *noyb* (31.05.2021), abrufbar unter https://noyb.eu/de/noyb-setzt-dem-cookie-banner-wahnsinn-ein-ende.

217 *Artikel-29-Datenschutzgruppe*, a. a. O. (Fn.204), S. 47; gegen ein Wahlrecht bei bereits bekannten Empfängern etwa auch *Dix* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 13 DSGVO Rn. 11; *Lorenz*, Datenschutzrechtliche Informationspflichten, VuR 2019, 213, 216. *Knyrim* verlangt, dass der Verantwortliche ggf. nach Treu und Glauben nachweisen können muss, warum die Angabe bloßer Kategorien ausreichen soll, s. *Knyrim* in: Ehmann/Selmayr [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 13 Rn. 40.

und Transparenzerfordernisses in Art. 12 Abs. 1 S. 1 DSGVO – zuzustimmen. Die jeweils aktuellen Datenempfänger einschließlich der Auftragsverarbeiter[218] sollten daher konkret und abschließend offengelegt werden (z. B. auf einer regelmäßig aktualisierten Website). Eine möglichst präzise Angabe von Datenempfängern dürfte zudem erfordern, dass den betroffenen Personen auch mitgeteilt wird, welche Gesellschaft eines Konzerns die Daten an welchem Standort empfängt.[219]

Die Frage, wie genau Datenempfänger genannt werden müssen (jedenfalls, wenn diese bereits feststehen), hat der Oberste Gerichtshof Österreichs im Februar 2021 dem Europäischen Gerichtshof zur Klärung vorgelegt.[220] Die Datenschutzerklärung in dem zu Grunde liegenden Fall enthielt u. a. folgende Formulierung:

> „Weitere Empfänger: Im Rahmen der Vertragsbeziehung und insbesondere im Zusammenhang mit unserer Leistungsverpflichtung, kann es – je nach Einzelfall – zu weiteren Übermittlungen Ihrer personenbezogenen Daten kommen (wie andere Postdienstleister [z.B. UPU, IPC], Frächter, Ärzte, Krankenanstalten, Versicherungsunternehmen und -makler, Sachverständige, Gutachter, Rechtsanwälte, Interessenvertretungen, Adressverlage und Direktmarketingunternehmen, Banken und Kapitalanlagegesellschaften, Versicherungen, Wirtschaftsprüfer, Berater, Förderstellen, Aktionäre, Investoren). Außerdem können unter bestimmten Voraussetzungen Ihre Daten an werbetreibende Unternehmen weitergegeben werden. Das sind

---

218 Diese sind ebenfalls anzugeben, s. *Dix* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 13 DSGVO Rn. 11. Ggf. könnte man in diesem Zusammenhang Kategorieangaben genügen lassen, soweit Auftragsverarbeiter ausschließlich als solche auftreten (also keine Datenverarbeitungen zu eigenen Zwecken vornehmen), nur in sehr begrenztem Umfang nicht-sensible personenbezogene Daten erhalten und diese nach kurzer Speicherdauer wieder löschen. Eine Angabe von Kategorien ist zudem nachvollziehbar, soweit es sich um nur potentielle Datenempfänger handelt, die noch nicht konkret benannt werden können, z. B. Inkassodienstleister im Falle eines Zahlungsrückstands.

219 Viele Unternehmen erwecken in ihren Datenschutzerklärungen den Eindruck, konzerninterne Übermittlungen personenbezogener Daten seien stets zulässig und müssten nicht weiter konkretisiert werden. Dies trifft jedoch nicht zu. DSGVO-Erwägungsgrund 48 S. 1 zufolge kann ein berechtigtes Interesse an einem Datentransfer zwischen Unternehmen innerhalb eines Konzerns bestehen, jedoch ist dieses Fallbeispiel ausdrücklich auf „interne Verwaltungszwecke“ beschränkt. Selbst bei Vorliegen eines berechtigten Interesses müsste die konzerninterne Übermittlung personenbezogener Daten offengelegt werden.

220 Oberster Gerichtshof, Beschluss vom 18.02.2021, Az. 6 Ob 159/20f, abrufbar unter https://www.ris.bka.gv.at/Dokumente/Justiz/JJT_20210218_OGH0002_0060OB00159_20F0000_000/JJT_20210218_OGH0002_0060OB00159_20F0000_000.pdf.

> zum Beispiel Unternehmen wie Handelsunternehmen oder Vereine, die Konsumenten ansprechen wollen.“[221]

Es ist offensichtlich, dass die Bezeichnung von Datenempfängern in einer solchen Pauschalität es betroffenen Personen praktisch unmöglich macht, das mit der Datenübertragung einhergehende Risiko einzuschätzen.[222] Der vorgelegte Fall betrifft indessen nicht die Vorab-Informationspflichten des Verantwortlichen gegenüber betroffenen Personen nach Art. 13 Abs. 1 lit. e) DSGVO, sondern die Beantwortung einer Auskunftsanfrage nach Art 15 Abs 1 lit. c) DSGVO. Bei einer solchen Auskunftserteilung liegt es auf der Hand, dass es dem Verantwortlichen möglich ist, bereits erfolgte Datentransfers zu bestimmten Dritten offenzulegen.

Nach hier vertretener Auffassung muss jedoch aus o. g. Gründen auch bei der Vorabinformation betroffener Personen eine genaue Benennung der Empfänger personenbezogener Daten erfolgen, sofern diese bereits bekannt sind. Die untersuchten Datenschutzerklärungen nahezu aller Unternehmen benennen indessen Datenempfänger nur undifferenziert und pauschal, obwohl sie präzisere Informationen – ggf. auch auf einer verlinkten Webseite – zur Verfügung stellen könnten. Dies stellt insbesondere aufgrund mangelnder Transparenz einen Verstoß gegen Art. 13 Abs. 1 lit. e) DSGVO i. V. m. Art. 12 Abs. 1 S. 1 DSGVO dar.

ee) Angabe von Drittländern

Art. 13 Abs. 1 lit. f) DSGVO zufolge muss der Verantwortliche darüber informieren, dass er beabsichtigt, personenbezogene Daten an ein Drittland[223] zu übermitteln. Drittland bezeichnet jeden Staat, in dem die DSGVO nicht direkt[224] anwendbar ist, mithin Staaten außerhalb der EU und des EWR[225]. Empfänger ist dabei im Regelfall natürlich nicht der Staat selbst, sondern jegliche in

---

221 Zitiert im Beschluss des OGH (vorhergehende Fußnote), Rn. 5.

222 Dies gilt umso mehr, als – wie in den meisten Datenschutzerklärungen – bereits nicht genau kenntlich gemacht wird, *welche personenbezogenen Daten* an Dritte übermittelt werden. Auch diese Nichtoffenlegung widerspricht bereits dem Transparenzgrundsatz des Art. 5 Abs. 1 lit. a) DSGVO.

223 Oder an eine internationale Organisation, was aber in der Praxis selten vorkommen dürfte.

224 Extraterritoriale Wirkungen bleiben an dieser Stelle außer Betracht.

225 Mit Wirkung ab dem 20.07.2018 hat der gemeinsame EWR-Ausschuss am 06.07.2018 die Übernahme der DSGVO in das EWR-Abkommen beschlossen. Somit zählen Island, Liechtenstein und Norwegen nicht mehr als Drittländer. Hingegen ist das Vereinigte Königreich seit dem Ende des Übergangszeitraums, also seit dem 01.01.2021, ein Drittland.

diesem Staat ansässige Empfänger[226]. Dies schließt auch Auftragsverarbeiter[227] und Unternehmensniederlassungen[228] ein. Der Verantwortliche muss aufgrund von Art. 12 Abs. 1 S. 1 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache über die Drittländer informieren, in die personenbezogene Daten der betroffenen Personen übermittelt werden. Nach Auffassung der Artikel-29-Datenschutzgruppe genügt es im Rahmen von Art. 13 Abs. 1 lit. f) DSGVO dabei nicht, dass pauschal angegeben wird, dass ein Drittlandtransfer von Daten stattfindet. Die Drittländer müssten vielmehr im Hinblick auf den Grundsatz von Treu und Glauben genau bezeichnet werden.[229] Die obligatorische Angabe der Drittländer erlaubt den betroffenen Personen, sich über das Datenschutzniveau in den jeweiligen Drittländern zu informieren und das Übermittlungsrisiko einzuschätzen[230].

Wie oben gezeigt, entsprechen die meisten untersuchten Datenschutzerklärungen diesen Anforderungen nicht.

ff) Angabe von Speicherdauern

Für die betroffene Person ist es von erheblicher Bedeutung, wie lange ihre personenbezogenen Daten gespeichert werden. Je länger Daten gespeichert werden, desto länger können sie in ggf. von der betroffenen Person nicht gewünschte Nutzerprofile einfließen. Auch besteht während der Speicherung stets das Risiko, dass persönliche Informationen aufgrund eines Datenlecks in falsche Hände geraten.

Gemäß Art. 13 Abs. 2 lit. a) DSGVO ist der datenschutzrechtlich Verantwortliche verpflichtet, die Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer anzugeben. Art. 13 Abs. 2 lit. a) DSGVO steht dabei in engem Zusammenhang mit den in Art. 5 Abs. 1 lit. c) bzw. e) DSGVO enthaltenen

---

226 S. etwa *Dix* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 13 DSGVO Rn. 12; *Franck* in: Gola u. a. [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 13 Rn. 19.

227 In diesem Sinne *Knyrim* in: Ehmann/Selmayr [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 13 Rn. 49.

228 Vgl. *Schantz* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 44 DSGVO Rn. 11.

229 S. hierzu *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (Fn.204), S. 48.

230 Vgl. *Bäcker* in: Kühling/Buchner/Bäcker [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 13 Rn. 34. Auch hier besteht das Problem, dass die betroffene Person häufig gar nicht erkennen kann, welche personenbezogenen Daten überhaupt von einem möglichen Drittlandtransfer betroffen sind.

Grundsätzen der Datensparsamkeit und der „Speicherbegrenzung“.[231] Es genügt vor diesem Hintergrund insbesondere nicht darauf hinzuweisen, dass eine Speicherung so lange erfolgt, wie dies für den jeweiligen Zweck erforderlich ist.[232] Dies lässt sich zum einen Art. 13 Abs. 2 lit. a) DSGVO selbst entnehmen, dem zufolge die bloße Nennung von Kriterien für die Speicherdauer nur dann zulässig ist, wenn eine präzise Information zu den Speicherdauern *unmöglich* ist; insoweit können dann verallgemeinerte Angaben ausnahmsweise genügen. Zum anderen spricht auch das Transparenzgebot des Art. 12 Abs. 1 S. 2 DSGVO für eine detaillierte Angabe.

In den geprüften Datenschutzerklärungen fanden sich zu Speicherfristen ganz überwiegend nur pauschale Angaben. Dies war praktisch durchgängig selbst dann der Fall, wenn zumindest eine Beschreibung der Speicherdauern für Daten, die bei typischen Nutzungsvorgängen anfallen, mit zumutbarem Aufwand möglich gewesen wäre. Für die betroffenen Personen ist so nicht ersichtlich, wie lange ihre personenbezogenen Daten gespeichert werden. Dem Informationserfordernis des Art. 13 Abs. 2 lit. a) DSGVO ist damit nicht Genüge getan. Die meisten App-Publisher verstoßen somit gegen die Vorgaben der DSGVO.

6. Informationen über In-App-Käufe

Weder im *Apple App Store* noch auf *Google Play* lassen sich bei der Suche Apps ausschließen, die sich über In-App-Käufe finanzieren. In-App-Käufe sind einerseits eine legitime Möglichkeit, Nutzer zunächst eine App ausprobieren zu lassen und die dauerhafte Nutzung oder einen erweiterten Leistungsumfang gegen Zahlung eines Entgelts freizuschalten („Freemium“-Modell). Auch lassen sich in den App-Stores von *Google* und *Apple* Zahlungen durch Kinder ohne Autorisierung der Eltern relativ einfach ausschließen. Andererseits wird in etlichen, zumeist Spiele betreffenden, App-Rezensionen in den App-Stores beklagt, dass eine sinnvolle App-Nutzung oder ein Spielfortschritt nur noch gegen Zahlung relativ hoher Geldbeträge möglich sei. Dieses Phänomen ist unter der Bezeichnung „Pay-to-win“ bekannt.

---

231 S. hierzu *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (Fn.204), S. 48 f.; s. auch *Knyrim* in: Ehmann/Selmayr [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 13 Rn. 52, *Lorenz*, Datenschutzrechtliche Informationspflichten, VuR 2019, 213, 217.

232 Vgl. hierzu *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (Fn.204), S. 49, abrufbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227; *Dix* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 13 DSGVO Rn. 15.

a) Ermittlungen

Während bei *Google Play* Preise für In-App-Käufe lediglich als Spanne dargestellt werden, werden im App-Store von *Apple* die jeweiligen Preise einzeln aufgelistet:

Abbildung 37: Screenshot App-Infos auf *Google Play* (Ausschnitt)

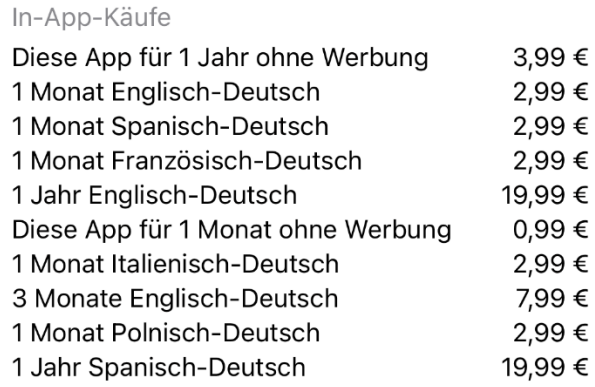


Abbildung 38: Screenshot App-Infos im App-Store von *Apple* (Ausschnitt)

In diesem Zusammenhang sollte nicht unerwähnt bleiben, dass auch die detaillierteren Informationen über In-App-Käufe oftmals wenig aussagekräftig oder gar verwirrend sind und Verbrauchern keinen nennenswerten Mehrwert bieten, wie die folgenden beiden Beispiele zeigen:[233]

[233] Auch im Rahmen der von der australischen Wettbewerbsbehörde ACCC durchgeführten Verbraucherbefragung gaben viele befragte Nutzer an, sie würden nicht ausreichend über die Kosten der In-App-Käufe informiert werden, s. Fn. 122.

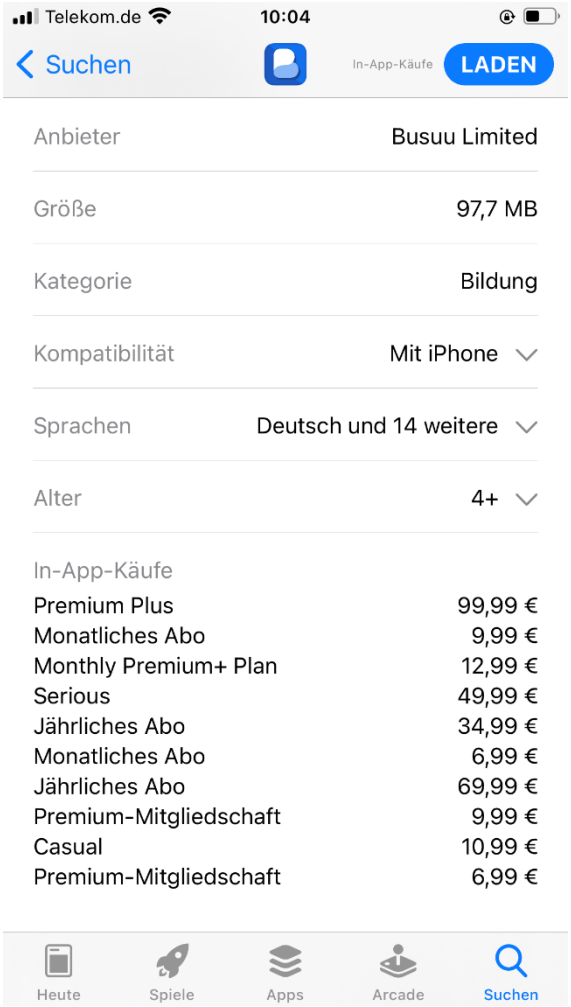


Abbildung 39: In-App-Käufe-Preisliste der App „Busuu“

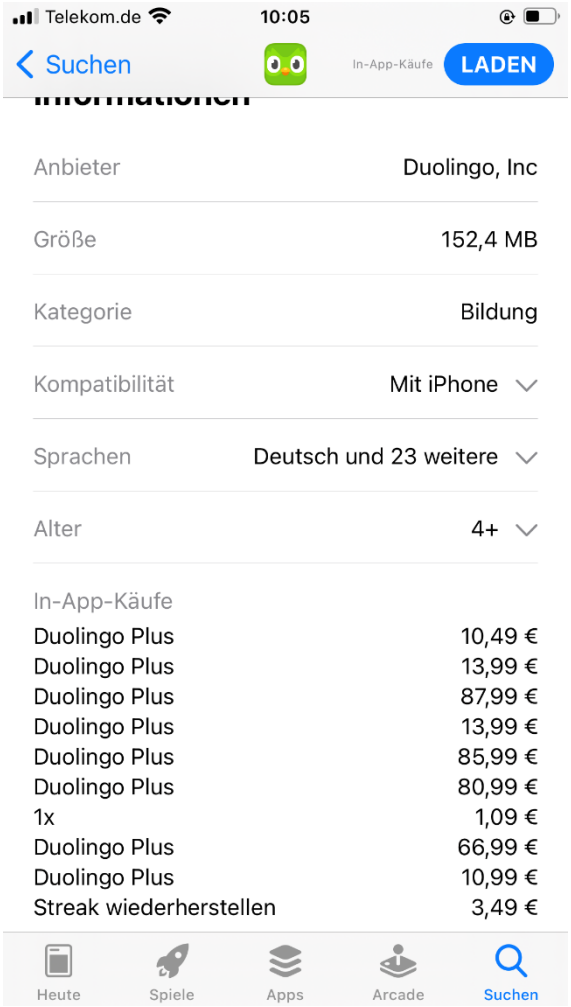


Abbildung 40: In-App-Käufe-Preisliste der App „Duolingo“

Bei Spiele-Apps lässt sich den Preisübersichten in der Regel nicht oder aufgrund der jeweiligen Bezeichnung nicht eindeutig entnehmen, ob sog. Lootboxen käuflich angeboten werden. Der Begriff Lootbox setzt sich zusammen aus den englischen Wörtern „loot“ für Beute bzw. Raubgut und „box“ für Kiste. Es handelt sich dabei um einen virtuellen Behälter in Computerspielen, der eine zufällige Sammlung bestimmter virtueller Gegenstände enthält, z. B. Waffen oder Ausrüstung.[234] Ebenso wenig ist erkennbar, ob ein Spiel sog. „Pay-to-win“-Elemente enthält. Das bedeutet, dass echte Spielfortschritte ab einem gewissen Zeitpunkt nur noch durch In-App-Käufe erzielt werden können, was bei den Spielenden zu Frustration oder hohen Geldausgaben führen kann.

234 Vgl. Wikipedia-Eintrag *Lootbox*, abrufbar unter https://de.wikipedia.org/wiki/Lootbox.

Abbildung 41: Lootbox (Wikimedia/Sameboat, CC BY-SA 4.0)

Zahlreiche wissenschaftliche Studien weisen auf Gefahren von Lootboxen und ähnlichen zufallsbasierten Spieleelementen hin.[235] Mehrere Staaten haben Lootboxen entweder als Glücksspiel verboten oder reglementiert.[236] Das US-amerikanische Entertainment Software Ratings Board (ESRB), das US-amerikanische Pendant zur deutschen Unterhaltungssoftware Selbstkontrolle (USK), weist seit April 2020 In-Game-Käufe mit randomisierten Inhalten aus:

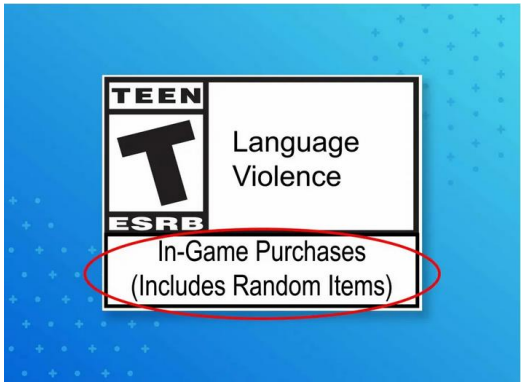


Abbildung 42: Hinweis des ESRB auf In-Game-Käufe mit Zufallselementen[237]

235 S. etwa *Close/Lloyd*, Lifting the Lid on Loot-Boxes – Chance-Based Purchases in Video Games and the Convergence of Gaming and Gambling (März 2021), abrufbar unter https://www.begambleaware.org/sites/default/files/2021-03/Gaming_and_Gambling_Report_Final.pdf; *Rockloff u. a.*, Young people who purchase loot boxes are more likely to have gambling problems: An online survey of adolescents and young adults living in NSW Australia, Journal of Behavioural Addictions 2021, 35, abrufbar unter https://akjournals.com/view/journals/2006/10/1/article-p35.xml; *Zendle/Cairns*, Video Game Loot Boxes are Linked to Problem Gambling: Results of a Large-Scale Survey, PLOS ONE (21.11.2018), abrufbar unter https://doi.org/10.1371/journal.pone.0206767.

236 *Maties*, a. a. O. (Fn. 240), 3685, 3687.

237 Quelle: https://www.esrb.org/blog/in-game-purchases-includes-random-items.

Apple gibt seit 2017 in seinen „App Store Review Guidelines“ vor, dass die Chancen, bestimmte Gegenstände mit einem Lootbox-Kauf zu erhalten, vor deren Erwerb angezeigt werden müssen.[238] Eine gesonderte Kennzeichnung von Spiele-Apps, die Lootboxen o. Ä. enthalten, findet in den App-Stores von *Apple* bzw. *Google* nicht statt.

b) Würdigung

In rechtlicher Hinsicht ist es aufgrund der Vielgestaltigkeit möglicher Fallkonstellationen kaum möglich, eine einheitliche Beurteilung zu In-App-Käufen zu treffen. So gestaltet sich etwa eine systematische Einordnung von „Pay-to-win“-Modellen schwierig, da häufig nicht objektiv feststellbar ist, ob ein Spielfortschritt nur durch eine quasi erzwungene Bezahlung ermöglicht wird oder auch ohne finanziellen Einsatz mit vertretbarem Spielaufwand möglich wäre. Selbst bei einer quasi erzwungenen Bezahlung steht nicht notwendigerweise fest, dass der bis zur „Pay-to-win“-Grenze ermöglichte Spielspaß überteuert erkauft wurde. Eine lauterkeitsrechtlich relevante Verbrauchertäuschung oder ein Vorenthalten wesentlicher Informationen dürfte sich so nur in seltenen Fällen feststellen lassen.

Vor diesem Hintergrund kommt einer möglichst aussagekräftigen Verbraucherinformation vor dem App-Download eine wichtige Rolle zu. In der Verbraucherbefragung des Bundeskartellamts sprachen sich die Teilnehmer ganz überwiegend dafür aus, Preise für In-App-Käufe nicht nur als Spanne anzuzeigen, sondern die jeweiligen Kaufpositionen einzeln aufzuführen[239] (entspricht der von *Apple* gewählten Variante“):

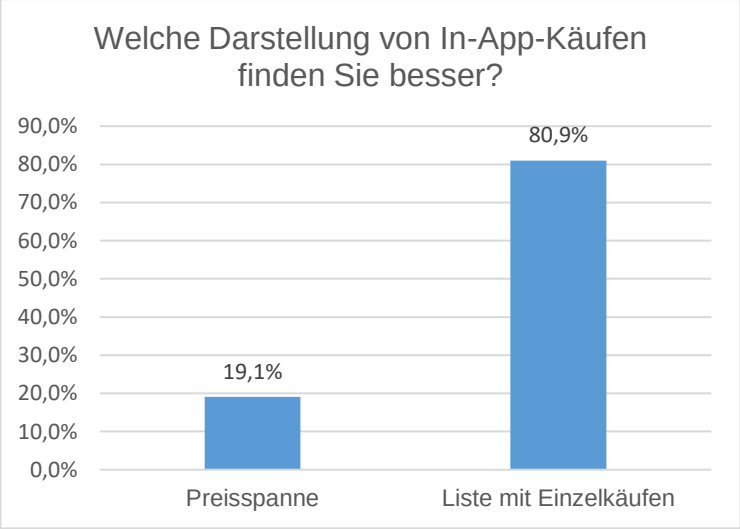


Abbildung 43: Bevorzugte Darstellungsart für In-App-Käufe im App-Store

238 App Store Review Guidelines vom 07.06.2021, Punkt 3.1.1., abrufbar unter https://developer.apple.com/app-store/review/guidelines/.

239 Siehe oben Abbildung 37 und Abbildung 38 auf S. 94

In der Verbraucherbefragung wurden die Teilnehmer ferner danach gefragt, ob sie persönlich eine zusätzliche Nennung durchschnittlicher Ausgaben für In-App-Käufe hilfreich fänden, die in etwa folgendermaßen aussehen könnte:

In-App-Käufe : …	
durchschnittliche Ausgaben je Nutzer bei Nutzung im vergangenen Monat:	**€ 4,87**

Abbildung 44: Beispiel für Darstellung durchschnittlicher monatlicher App-Ausgaben

Eine solche Darstellung könnte dem Verbraucher zumindest einen Eindruck davon geben, welche Kosten bei Nutzung der App auf ihn zukommen können. Rund drei Viertel der Befragten bewerteten eine solche Darstellung als hilfreich.

Abbildung 45: Bewertung einer Angabe monatlicher Durchschnittskosten der App-Nutzung

In der juristischen Literatur ist streitig, ob bzw. unter welchen Umständen das Angebot käuflicher Lootboxen als Glücksspiel im Sinne von § 284 des Strafgesetzbuchs bzw. § 4 Abs. 1 des Glücksspielstaatsvertrags einzustufen ist.[240] Als Glücksspiel gilt jedes Spiel, bei dem die Beteiligten zur

240 Gegen einen Glücksspielcharakter *Nickel/Feuerhake/Schelinski*, Lootboxen in Computerspielen: Legitimes Geschäftsmodell oder illegales Glücksspiel?, MMR 2018, 586; *Falk*, Games!, MMR 2018, 493; differenzierend *Hollering* in: BeckOK StGB, 49. Ed. 1.2.2021, § 284 Rn. 10 (m. w. N.); *Maties*, Lootboxen aus zivilrechtlicher Sicht, NJW 2020, 3685.

Unterhaltung oder aus Gewinnstreben über den Gewinn oder Verlust eines nicht ganz unbeträchtlichen Vermögenswertes ein ungewisses Ereignis entscheiden lassen, dessen Eintritt nicht wesentlich von Aufmerksamkeiten, Fähigkeiten oder Kenntnissen der Spieler, sondern allein oder hauptsächlich vom Zufall abhängt.[241] Konsens besteht zwar hinsichtlich der Tatsache, dass Lootboxen ein erhebliches Zufallselement innewohnt. Unklar und von den Umständen des Einzelfalls abhängig ist hingegen, inwiefern ein nicht unerheblicher Einsatz erbracht wird bzw. das Risiko eines (Total-)Verlusts besteht, da der Käufer im Regelfall in Form von virtuellen Gegenständen stets eine Gegenleistung erhält.[242] Auch wird angenommen, dass es an der – für das Vorliegen eines Glücksspiels konstitutiven – Möglichkeit eines positiven Vermögenssaldos nach Kauf einer Lootbox jedenfalls dann fehle, wenn für die enthaltenen Gegenstände kein Markt bestehe.[243] In der überwiegenden Anzahl der Fälle dürfte das Angebot von Lootboxen somit eher kein Glücksspiel darstellen. Da mithin im Regelfall die Schwelle des Glücksspiels nicht erreicht wird, würde auch das Unterbleiben eines expliziten Hinweises auf Lootboxen o. Ä. kein lauterkeitsrechtlich relevantes Vorenthalten einer für den Verbraucher wesentlichen Information bedeuten.

IV. Gewährleistung

Oben wurde bereits festgestellt, dass im Verhältnis zum Verbraucher *Google* beim Download von Apps aus *Google Play* als Vertragspartner anzusehen ist, wohingegen dies beim App-Store von *Apple* weniger klar ist und womöglich mehr dafür spricht, *Apple* als bloßen Vermittler und den jeweiligen App-Publisher als Vertragspartner zu betrachten.

1. Ermittlungen

Google hat für den Fall nicht funktionierender Apps Erstattungsregelungen veröffentlicht; bei *Apple* werden die Voraussetzungen für Erstattungen nur in den Bedingungen der *Apple* Media Services erwähnt. Das Bundeskartellamt hat die jeweiligen Regelungen der App-Stores zur Abwicklung von Gewährleistungsansprüchen näher untersucht.

---

241 *Hollering* in: BeckOK StGB, 49. Ed. 01.02.2021, § 284 Rn. 9 (m. w. N.).

242 S. dazu *Hentsch* in: Hoeren/Sieber/Holznagel [Hrsg.], MMR-HdB, 55. EL Februar 2021, Teil 22 Games Rn. 62; *Nickel/Feuerhake/Schelinski*, a. a. O. (Fn. 240), 586, 588. *Kubiciel*, Entwicklung des eSports und Schutz seiner Integrität, ZRP 2019, 200, 203 weist in diesem Zusammenhang darauf hin, dass der Inhalt von Lootboxen durchaus für den Fortgang des Spiels mehr oder weniger wertlos sein könne.

243 *Maties*, a. a. O. (Fn. 240), 3685, 3689.

a) Google

Bei *Google* finden sich zu Erstattungsfragen in den Nutzungsbedingungen von *Google Play* folgende Angaben[244]:

> **„Endgültigkeit von Bestellungen**. In den Erstattungsrichtlinien von Google Play finden Sie weitere Informationen dazu, wann Sie das Recht haben, Bestellungen rückgängig zu machen, zu stornieren oder gegen eine Erstattung zurückzugeben. Soweit es in den Erstattungsrichtlinien von Google Play oder den Erstattungsrichtlinien des Anbieters nicht ausdrücklich anders angegeben ist, gilt jeder Erwerb als endgültig und Rückgaben, Ersatz oder Erstattungen sind nicht zulässig. Falls ein Ersatz, eine Rückgabe oder eine Erstattung für eine Bestellung gewährt wird, kann diese Bestellung rückgängig gemacht werden und Sie können möglicherweise nicht mehr auf die Inhalte zugreifen, die Sie im Rahmen dieser Bestellung erworben haben."

sowie

> „**Fehlerhafte Inhalte**. Sobald Inhalte in Ihrem Konto verfügbar sind, sollten Sie diese so bald wie möglich dahingehend überprüfen, ob sie wie angegeben funktionieren und verwendet werden können. Bei Fehlern oder Mängeln sollten Sie uns bzw. den Anbieter so früh wie möglich informieren. Weitere Informationen finden Sie in den Erstattungsrichtlinien von Google Play."

Die verlinkten Erstattungsrichtlinien lauten wie folgt:

> **„Google Play-Erstattungsrichtlinien**
>
> Die Erstattungsrichtlinien unterscheiden sich je nach gekauftem Artikel. Wenn Sie mehr erfahren möchten, folgen Sie dem entsprechenden Link zum Thema.
>
> […]
>
> Apps, Spiele und In-App-Käufe (einschließlich Abos)
>
> Für die meisten Google Play-Käufe gewährt Google keine Erstattungen. Dabei gelten jedoch die weiter unten stehenden Ausnahmen. Außerdem können Sie sich auch direkt an den Entwickler wenden. Der Entwickler

244 *Google Play*-Nutzungsbedingungen vom 4. Augsut 2020 (Fn. 50).

> kann Ihnen bei Problemen mit Ihren Käufen helfen und gemäß seinen Richtlinien und den geltenden Gesetzen Erstattungen gewähren.
>
> Erstattungsrichtlinien
>
> **Innerhalb von 48 Stunden**: Abhängig von den Einzelheiten des Kaufs können Sie möglicherweise eine Erstattung erhalten. Gehen Sie entsprechend dieser Anleitung vor.
>
> **Nach 48 Stunden**: Kontaktieren Sie den Entwickler, um Hilfe zu erhalten und zu erfahren, ob eine Erstattung möglich ist. Je nach eigenen Richtlinien und den speziellen rechtlichen Bedingungen, an die Entwickler gebunden sind, können sie möglicherweise eine Erstattung vornehmen.
>
> **Hinweis**: Die Erstattung für eine App oder ein Spiel kann immer nur einmal beantragt werden. Wenn Sie die App oder das Spiel danach noch einmal kaufen, können Sie keine Erstattung mehr dafür erhalten. Nachdem eine Erstattung erfolgt ist, können Sie auf den betreffenden Artikel nicht mehr zugreifen.
>
> Informationen für Kunden in der EU und im Vereinigten Königreich
>
> Für einige Käufe in der EU und in Großbritannien gelten abweichende Erstattungsrichtlinien:
>
> Wenn Sie bei Google Play digitale Inhalte wie In-App-Artikel, Apps, Spiele, Musik oder Filme kaufen, verzichten Sie auf das automatische Widerrufsrecht und unsere Standard-Erstattungsregeln gelten.
>
> Wenn Sie einen Dienst von einem Entwickler oder einem anderen Drittanbieter gekauft haben, wenden Sie sich bitte an den Verkäufer, wenn Sie vom Kauf zurückzutreten und eine Erstattung erhalten möchten. Dies gilt auch dann, wenn Sie diesen Dienst bei Google Play gekauft haben."

Auf der Supportseite „Probleme mit Apps beheben, die nicht funktionieren"[245] heißt es u. a.:

> **„Wichtig**: Wenn Sie die Schritte zur Fehlerbehebung durchgeführt haben, das Problem aber weiterhin besteht, wenden Sie sich an uns oder den App-Entwickler.
>
> Wenn Sie keine Apps aktualisieren können oder Probleme mit *Google*-Apps haben, wenden Sie sich an *Google Play*.

[245] Abrufbar unter https://support.google.com/googleplay/answer/2668665?hl=de.

> Wenn Sie Probleme mit einer App haben, andere Apps jedoch problemlos verwenden können, wenden Sie sich an den App-Entwickler."

b) Apple

In den Bedingungen der *Apple Media Services*[246] findet sich im Abschnitt *G. Zusätzliche Bedingungen für den App-Store* folgende Aussage:

> „App-Lizenzen werden Ihnen von Apple oder einem Drittentwickler („App-Provider") zur Verfügung gestellt. Eine von Apple lizenzierte App ist eine „Apple-App" […] Der App-Provider einer Dritt-App ist allein verantwortlich für deren Inhalte, Gewährleistungen und für Ansprüche, die Sie ggf. in Bezug auf die Dritt-App haben."

Für die Abwicklung von App-Rückgaben verweist *Apple* auf seinen Support-Seiten[247] auf die Website reportaproblem.*Apple*.com, ohne diesbezüglich weitere Bedingungen oder Fristen zu nennen.

2. Würdigung

Die Frage, welche Gewährleistungsansprüche geltend gemacht werden können, wenn eine App nicht oder nur eingeschränkt funktioniert, ist bislang wenig erforscht. Die Gewährleistungspflichten bestimmen sich dabei nach der jeweils verletzten vertraglichen Pflicht.[248] Es können so etwa Regelungen aus dem Kauf-, Miet- oder Schenkungsrecht[249] einschlägig sein. Bei Beträgen von zumeist nur wenigen Euro werden in der Praxis allerdings viele Verbraucher davon absehen, in Anbetracht des hiermit verbundenen Aufwands überhaupt eine Rückerstattung[250] zu verlangen, geschweige denn diese auf dem Rechtsweg durchzusetzen.

Ungeachtet der Tatsache, dass womöglich sowohl *Google* als auch *Apple* Rückerstattungsansprüchen über die eigens formulierten Voraussetzungen hinaus nachkommen, werfen die Regelungen in den Nutzungsbedingungen der beiden Unternehmen Fragen auf.

---

246 Abrufbar unter https://www.apple.com/legal/internet-services/itunes/at/terms.html.

247 Siehe https://support.apple.com/de-de/HT204084.

248 Vgl. hierzu BGH, Urteil vom 15.11.2006, Az. XII ZR 120/04, juris Rn. 21.

249 Jedenfalls nach herrschender Meinung ist eine Schenkung nicht dadurch ausgeschlossen, dass eine Übermittlung (personenbezogener) Daten impliziert wird.

250 Eine Nacherfüllung (Lieferung einer mangelfreien Sache) dürfte in der Regel keine realistische Option darstellen.

a) Google

Anspruchsgegner von Gewährleistungsansprüchen ist, außer in Sonderkonstellationen, die hier nicht vorliegen, der unmittelbare Vertragspartner. Nach den oben getroffenen Feststellungen also *Google* bzw. genauer gesagt *Google Commerce Ltd*. Davon ausgehend, dass bei Mängeln kostenpflichtig heruntergeladener Apps im Regelfall das Kaufgewährleistungsrecht einschlägig ist, stehen dem Nutzer grundsätzlich die Mängelgewährleistungsrechte des § 440 BGB offen.[251] Gemäß § 438 Abs. 1 Nr. 3 BGB können diese Rechte zwei Jahre lang geltend gemacht werden, wobei in der Regel ein Verbrauchsgüterkauf vorliegen dürfte, so dass § 477 BGB zufolge eine sechsmonatige Beweislastumkehr zugunsten des Verbrauchers eingreift.

Dessen ungeachtet sieht *Google* in den *Google*-Play-Nutzungsbedingungen nur eine 48-stündige Stornofrist vor und verweist den Nutzer ansonsten auf den Entwickler der App. Zwar können auch Verjährungsfristen grundsätzlich abbedungen werden; § 476 Abs. 2 BGB verbietet jedoch gegenüber Verbrauchern eine Verkürzung der Gewährleistungsfrist auf weniger als zwei Jahre für nicht gebrauchte Sachen. Eine Interpretation dahingehend, dass *Googles* Regelungen nur Kulanzrückerstattungen betreffen, verbietet sich, da unter der Unterüberschrift „Fehlerhafte Inhalte“ explizit auf die Erstattungsregelungen Bezug genommen wird (die somit als Teil der Nutzungsbedingungen anzusehen sind). Auch lässt sich die *Google*-Supportseite „Probleme mit Apps beheben, die nicht funktionieren“ bei realistischer Betrachtung nur so verstehen, dass *Google* die Zuständigkeit für die Geltendmachung gesetzlicher Gewährleistungsrechte von sich weist.

Aufgrund Verstoßes gegen höherrangiges Recht sind die oben beschriebenen Klauseln in *Googles* Regelwerken daher unwirksam.

b) Apple

In den o. g. Passagen aus den *Bedingungen der Apple Media Services* bezeichnet sich *Apple* – jedenfalls für europäische Kunden – als Vertragspartner[252], erklärt sich aber in den Bedingungen auch als unzuständig für die Geltendmachung von Gewährleistungsansprüchen und verweist den

---

251 Bei einem Massengeschäft wie dem Anbieten von Apps erscheint indessen vor allem der Rücktritt vom Vertrag, einhergehend mit der Rückgabe der App (durch Löschung) und Erstattung des Kaufpreises, als realistische Option.

252 Siehe oben, S. 27 f. Die Bedingungen der Apple Media Services sehen gegenüber Verbrauchern die Geltung des Rechts des gewöhnlichen Aufenthalts vor („Wenn Sie ein Bewohner eines Landes der Europäischen Union, […] sind, sind das anwendbare Recht und der Gerichtsstand das Recht und die Gerichte Ihres gewöhnlichen Aufenthaltsortes.“).

Kunden diesbezüglich auf den „App-Provider“[253]. Unter Zugrundelegung eines objektiven Empfängerhorizonts muss man diese Ausführungen so verstehen, dass *Apple* zwar Vertragspartner des Endabnehmers sein, gleichzeitig aber nicht die hiermit einhergehenden Gewährleistungspflichten übernehmen will.[254]

Sähe man *Apple* als Vertragspartner an, so läge im Ausschluss der Gewährleistung ein direkter Verstoß gegen § 476 Abs. 1 BGB.

Ginge man hingegen davon aus, dass *Apple* aufgrund der Gesamtumstände des App-Downloads nicht als Vertragspartner bzgl. des App-Erwerbs anzusehen wäre, so wären die *Bedingungen der Apple Media Services* gleichwohl im Rahmen des allgemeinen App-Store-Nutzungsverhältnisses anwendbar. Diese unterlägen wiederum grundsätzlich der AGB-Kontrolle. Noch bevor aber eine inhaltliche Kontrolle der AGB stattfinden kann, müssten die zu prüfenden Klauseln ausgelegt werden. Für die Auslegung gilt der Grundsatz der objektiven Auslegung.[255] Dies bedeutet, dass die Vertragsbestimmung nach objektiven Maßstäben und losgelöst von der zufälligen Gestaltung des Einzelfalls sowie den individuellen Vorstellungen der Vertragsparteien zu ermitteln ist.[256] Ist allerdings der Wortlaut eindeutig, gibt es keinen Raum für eine Auslegung mehr.[257] Der Wortlaut der vorliegenden Klausel bestimmt *Apple* eindeutig als Vertragspartner und lässt keine Mehrdeutigkeit zu, sodass sich eine gegenteilige Auslegung dahingehend, *Apple* sei nicht als Vertragspartner anzusehen, nicht ergeben könnte. Mithin wäre *Apple* trotz der gegenteiligen Gesamtumstände Vertragspartner. Dies hätte zur Folge, dass der Anwendungsbereich des Verbrauchsgüterkaufs eröffnet und der Gewährleistungsausschluss gemäß § 476 Abs. 1 BGB unwirksam wäre (siehe oben). Die Frage der Wirksamkeit nach AGB-Recht würde sich demnach nicht mehr stellen.

---

253 Siehe oben, S. 102.

254 Dass diese widersprüchliche Regelung auf eine unzureichende Übersetzung der englischsprachigen Geschäftsbedingungen zurückzuführen sein mag, ist im Kontext der Verwendung der deutschen Sprachfassung für den deutschen Markt unerheblich.

255 *Basedow* in: Münchener Kommentar zum BGB, 8. Aufl. 2019, BGB § 305c Rn. 33.

256 BGH, Urteil vom 29.10.1956, Az. II ZR 64/56, juris; *Basedow* in: Münchener Kommentar zum BGB, 8. Aufl. 2019, BGB § 305c Rn. 33.

257 H. M., statt vieler BGH, Urteil vom 04.02.2002, Az. II ZR 37/00, juris; *Schmidt* in: BeckOK BGB, 57. Ed. 1.2.2021, BGB § 305c BGB Rn. 46.

V. Berechtigungsmanagement

Wie die Befragung des Bundeskartellamts ergeben hat, wünschen sich Verbraucher effektivere Möglichkeiten, den Zugriff von Apps auf Gerätefunktionen (und damit – ggf. auch personenbezogene – Daten) einzuschränken:

Abbildung 46: Verbrauchermeinung zur Möglichkeit, Apps alle nicht funktionsrelevanten Berechtigungen[258] zu entziehen

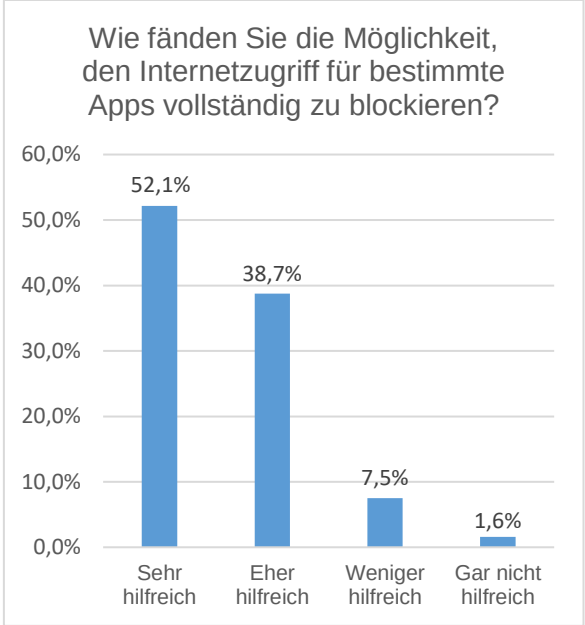


Abbildung 47: Verbrauchermeinung zur Möglichkeit, Apps den Internetzugriff zu verwehren

Die Verbraucherbefragung des Bundeskartellamts hat ferner gezeigt, dass eine große Mehrheit der Nutzer eine App oder Funktion zur zentralen Steuerung von Zugriffsrechten für alle Apps[259] hilfreich fände:

---

258 In der Praxis wäre die Umsetzung einer solchen Funktionalität keineswegs trivial, die Fragestellung diente indessen der Messung, inwieweit ein entsprechender Verbraucherwunsch besteht.

259 *Android* verfügt zwar über eine Übersicht von App-Berechtigungen; der Berechtigungsentzug muss aber für jede App einzeln erfolgen.

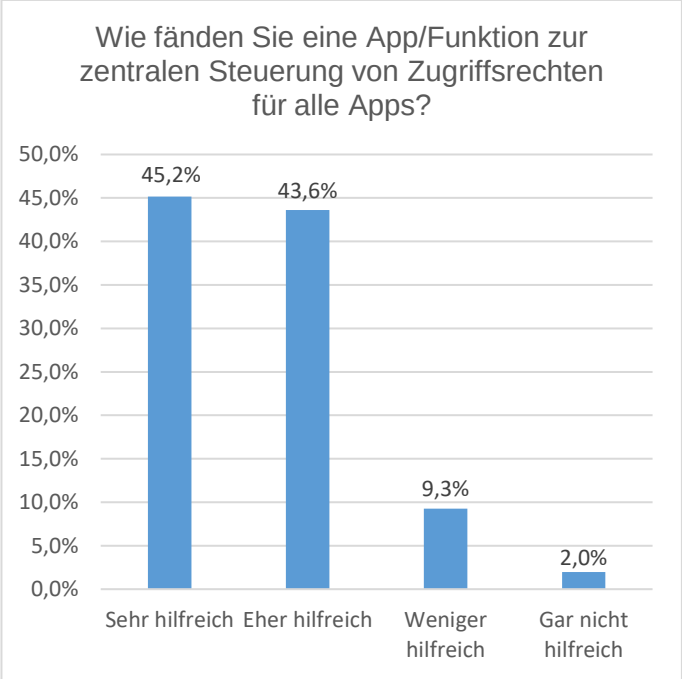


Abbildung 48: Haltung der Verbraucher zu zentraler Zugriffsrechtesteuerung für alle Apps.

Mit einer solchen App oder Funktionalität könnte dann auch weiteren Verbraucherwünschen entsprochen werden, etwa Apps den Zugriff auf eindeutige Identifikatoren zu verweigern:

Abbildung 49: Verbrauchermeinung zur Möglichkeit der Zugriffsverweigerung auf eindeutige Identifikatoren

1. Ermittlungen

Bei vorinstallierten Apps sind Datenzugriffsberechtigungen im Auslieferungszustand häufig bereits gewährt, auch ist die Hintergrunddatennutzung[260] bei sämtlichen Apps im Regelfall zugelassen. Veranschaulicht wird dies in der folgenden Abbildung anhand der *Google*-Suche-App:

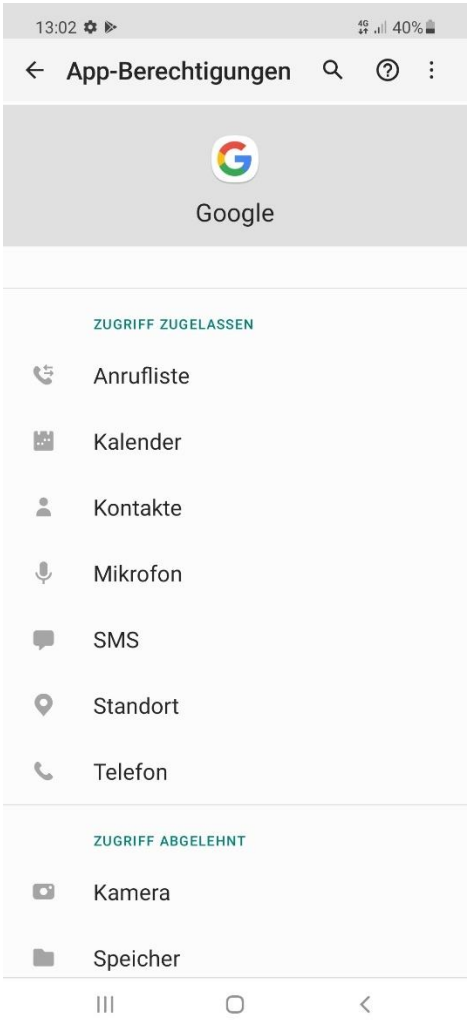


Abbildung 50: Berechtigungen der *Google*-App im Auslieferungszustand (Samsung Note 10 Lite)

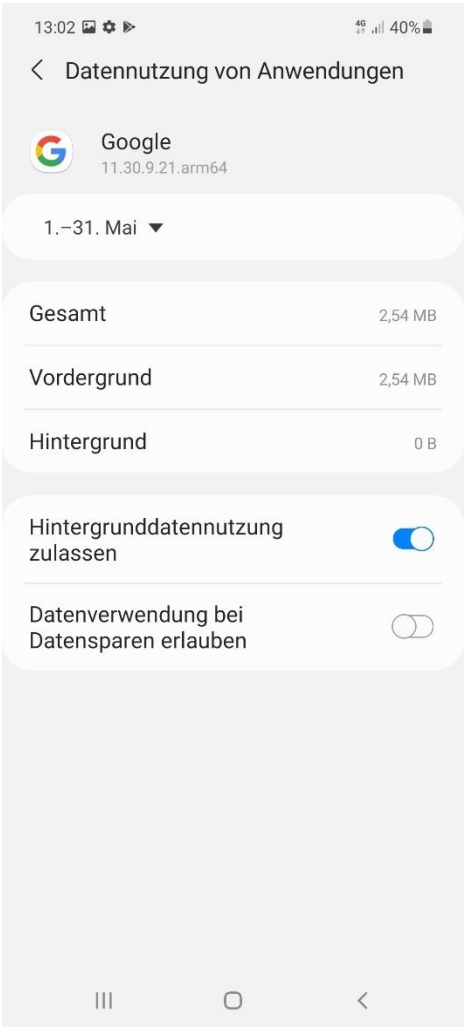


Abbildung 51: Hintergrunddatennutzung ist im Auslieferungszustand standardmäßig aktiviert

Laden Nutzer eine App aus *Google Play* herunter, können sie sich zuvor deren Funktions-/Datenzugriffsberechtigungen ansehen. Dabei können Anzahl und Umfang der Berechtigungen auch bei funktional gleichen Apps erheblich variieren, wie folgendes Beispiel zeigt:

260 Mobile Datennutzung durch die App, ohne dass diese aktiv genutzt wird.

Abbildung 52: Berechtigungen der App „Schlichte Taschenlampe“

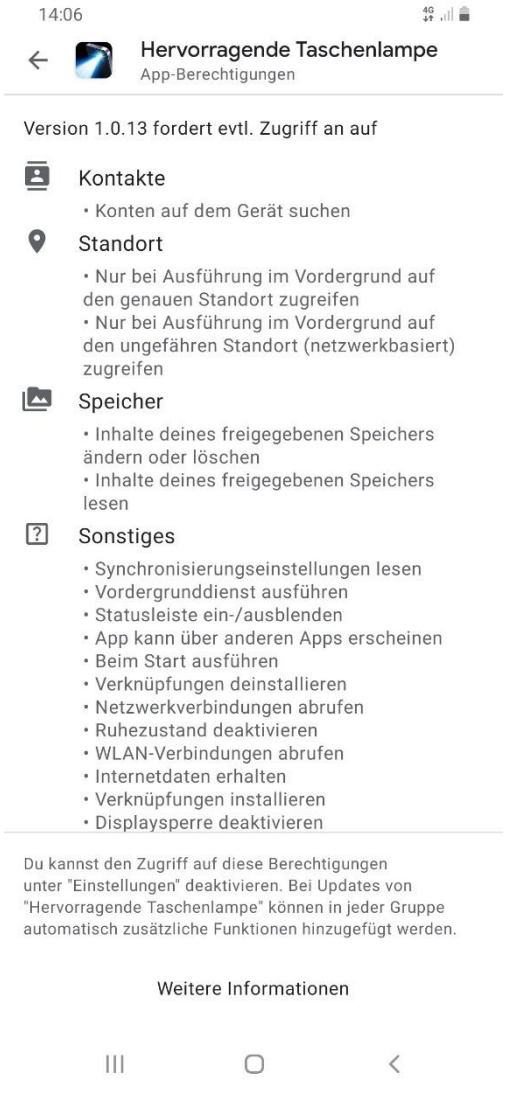


Abbildung 53: Berechtigungen der App „Hervorragende Taschenlampe“[261]

Bei *Apple* hingegen werden Datenzugriffsberechtigungen nicht vor dem Download angezeigt. Stattdessen hat *Apple* seit dem Betriebssystem-Upgrade auf *iOS 14.5* eine Datenschutz-Übersicht eingeführt. Diese beruht auf Angaben der App-Publisher und wird bei den Apps, wo dies noch nicht umgesetzt ist, mit dem nächsten Update verpflichtend. Nachfolgend ein Beispiel für die von *Apple* eingeführte Datenschutzübersicht für dritte App-Publisher (App: Kompass von *Tim O’s Studios, LLC*):

261 Drei weitere Berechtigungen werden erst bei weiterem Herunterscrollen dargestellt.

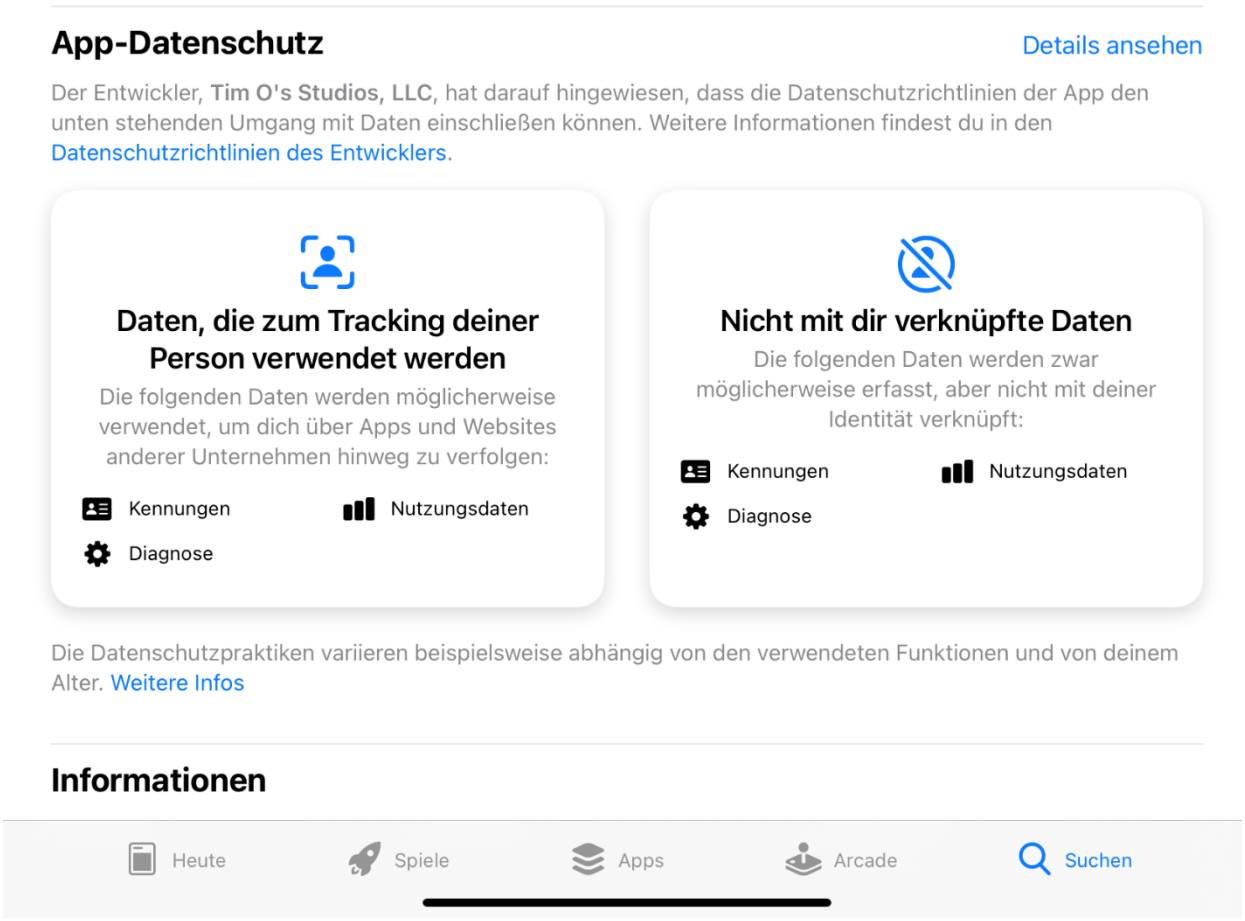


Abbildung 54: Screenshot (Ausschnitt) Datenschutzangaben seit Einführung von *iOS 14.5*

Das obige Beispiel zeigt indessen auch die Problematik einer Datenschutzsymbolik, die auf einer Selbsteinschätzung der App-Publisher beruht. Die Angabe, Daten würden nicht mit einer Person verknüpft, jedoch trotzdem zum Tracking ebendieser Person verwendet, ist in sich widersprüchlich. Auch ein Blick auf die Details hilft hier nicht weiter:

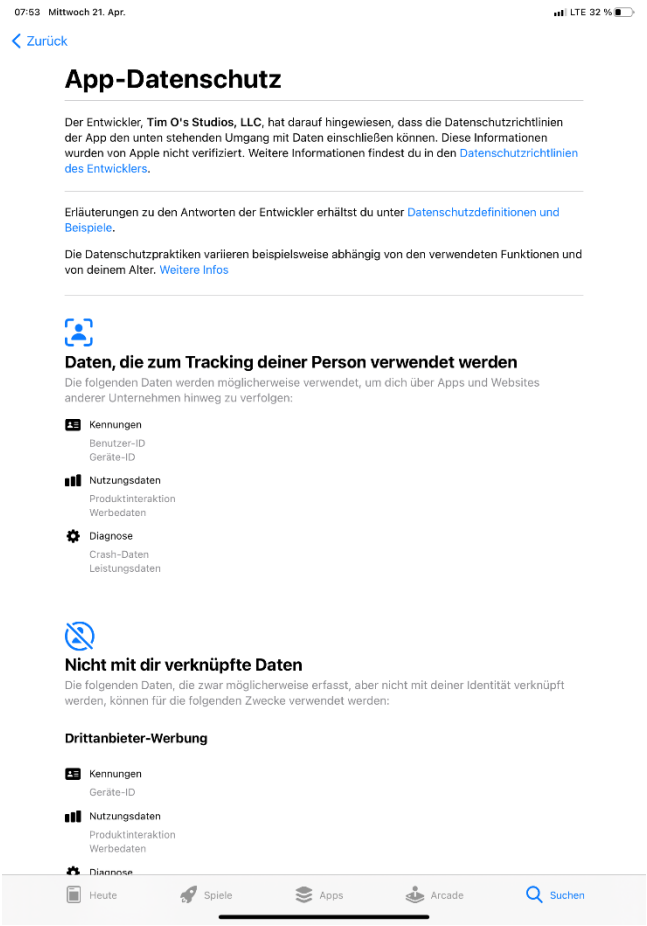


Abbildung 55: Screenshot Details zu Datenschutzangaben (*iOS 14.5*)

Sowohl *Apple iOS* als auch *Google Android* bieten Nutzern die Möglichkeit, Datenzugriffsberechtigungen von Apps einzuschränken. Allerdings sind die Steuerungsmöglichkeiten des Nutzers begrenzt, denn nicht alle Datenzugriffe sind kontrollierbar ausgestaltet; so kann der Nutzer beispielsweise nicht verhindern, dass eine App Internetdaten sendet oder erhält, wenn sich das Gerät im WLAN-Modus befindet. *Android* bietet hier zwar detailliertere Einblicke und dem Nutzer zumindest die Möglichkeit, einige wesentliche Datenzugriffe grundsätzlich zu kontrollieren.[262] Dies gilt jedoch nicht für alle Apps. Bei einigen Apps, insbesondere solchen des Geräteherstellers, ist dies nur teilweise oder gar nicht möglich, wie die folgenden Beispiele zeigen:

262 Siehe hierzu *Sievers*, Zugriffsrechte: Was darf meine App? (mobilsicher.de, aktualisierte Fassung vom 06.04.2021), abrufbar unter https://mobilsicher.de/ratgeber/berechtigungen-zugriffsrechte-was-darf-meine-app.

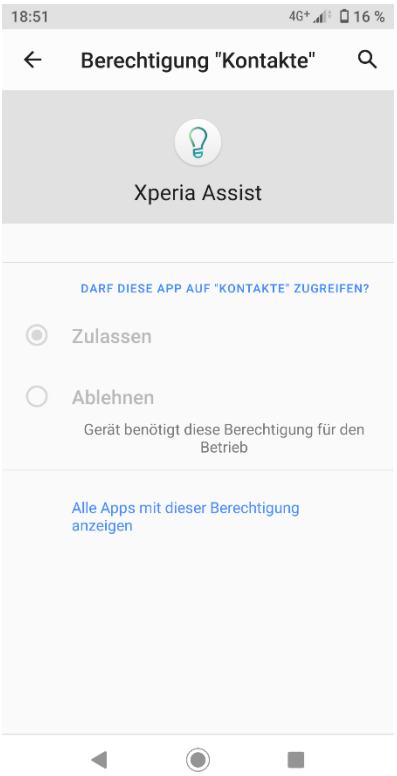


Abbildung 56: „Sony Xperia Assist“: Kontakte-Zugriff kann nicht abgelehnt werden[263]

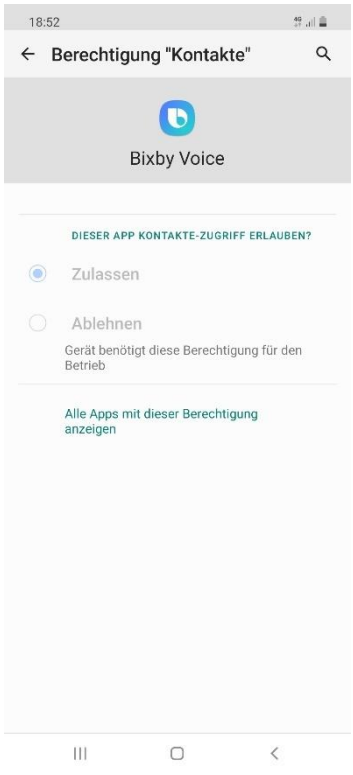


Abbildung 57: „Bixby Voice“: Kontakte-Zugriff kann nicht abgelehnt werden[264]

Manche Apps verlangen deutlich mehr Berechtigungen als sie zum Funktionieren benötigen. Zumindest die zustimmungspflichtigen Berechtigungen werden in der aktuellen Version des *Android*-Betriebssystem nach dem Download standardmäßig zunächst deaktiviert; die App muss sich solche Berechtigungen bei der ersten Nutzung daher zunächst neu einräumen lassen. Es kommt nur noch selten vor, dass Apps ihren Dienst verweigern, wenn sie oder die *Google-Play*-Dienste bestimmte Berechtigungen nicht erhalten, selbst wenn diese für das Funktionieren der App nicht erforderlich sind. Ganz ausgeschlossen ist dies aber nicht, wie die folgenden Beispiele zeigen:

263 Ebenso wenig wie die zustimmungspflichtigen Berechtigungen Kalender, Körpersensoren, SMS, Speicher, Telefon und die sog. signaturpflichtigen (ebenfalls zustimmungspflichtigen) Berechtigungen Akkuverbrauch optimieren, Zugriff während „Bitte nicht stören“ zulassen sowie etliche weitere nicht zustimmungspflichtigen Berechtigungen.

264 Ebenso wenig wie die zustimmungspflichtigen Berechtigungen Kamera, Mikrofon, Speicher, Standort, Telefon und die sog. signaturpflichtigen (ebenfalls zustimmungspflichtigen) Berechtigungen Akkuverbrauch optimieren, WLAN steuern sowie etliche weitere nicht zustimmungspflichtigen Berechtigungen.

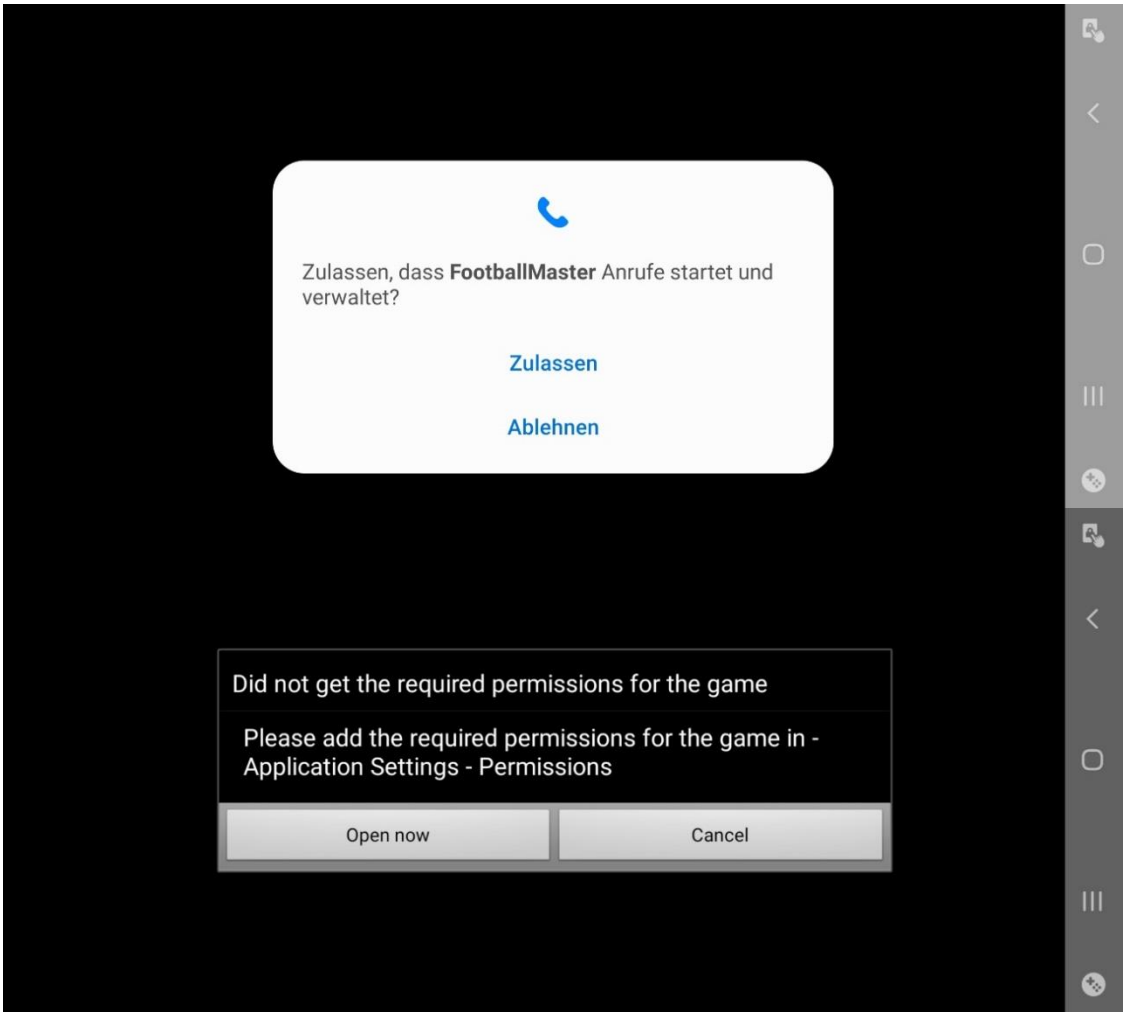


Abbildung 58: Die App „FootballMaster" kann (u. a.) ohne Telefonzugriff nicht gestartet werden

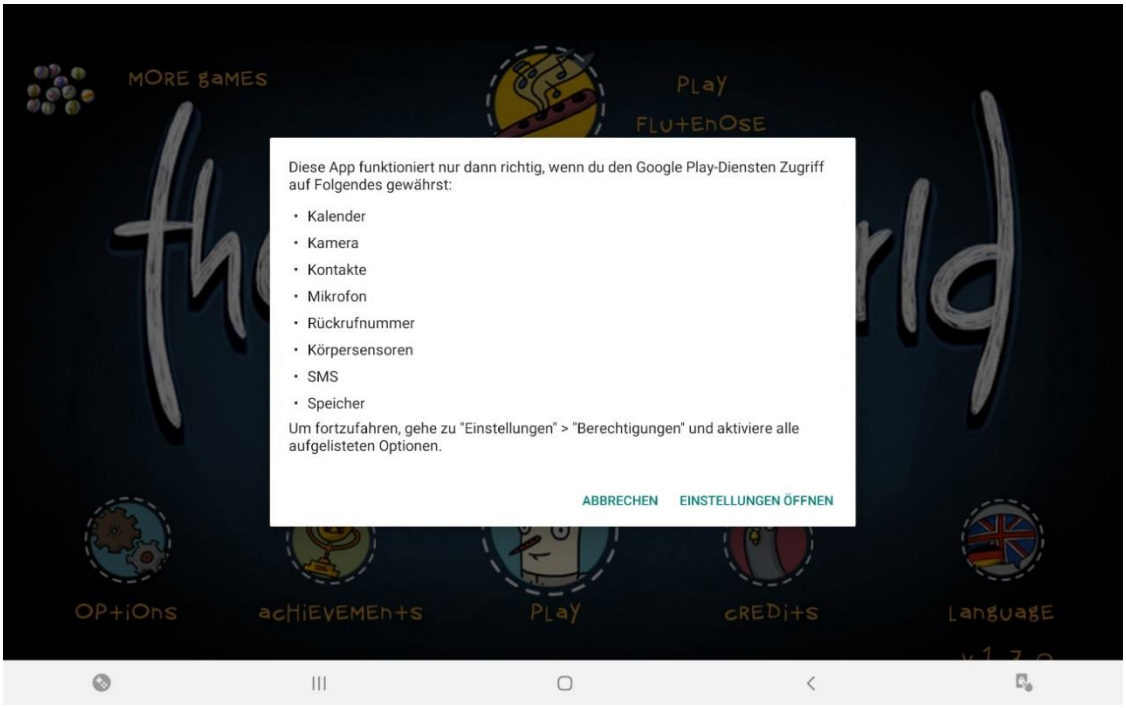


Abbildung 59: Angeforderte Berechtigungen der App „The Inner World" (ein sog. Point-and-Click-Adventure)

In diesem Zusammenhang ist auch erwähnenswert, dass das Entziehen von Berechtigungen bei den meisten Smartphones und Tablets relativ komplex ausgestaltet ist. So lassen sich derzeit Berechtigungen nur einzeln je App entziehen. Es kann also beispielsweise weder ein Berechtigungstyp für mehrere oder alle Apps auf einmal entzogen werden noch ist es möglich, einer App mehrere Berechtigungen auf einmal zu entziehen.

2. Würdigung

Nutzer smarter Mobilgeräte können Datenzugriffe von Apps nur in eingeschränktem Umfang blockieren. Dies liegt insbesondere daran, dass

- Apps nicht effektiv gelöscht oder abgeschaltet werden können,
- manche Berechtigungen überhaupt nicht entzogen werden können,
- bei manchen Apps der Berechtigungsentzug ganz oder teilweise gesperrt ist,
- der Überblick über eingeräumte Berechtigungen nur schwer zu behalten ist.

a) Datenschutzrecht

An dieser Stelle muss gedanklich zwischen zwei Ebenen unterscheiden werden: Die Einräumung von Zugriffserlaubnissen auf Gerätefunktionen hat zunächst nichts mit der Rechtmäßigkeit einer hierauf folgenden Übermittlung personenbezogener Daten zu tun. Die Einräumung von Zugriffsrechten ist lediglich eine technische Vorbedingung für eine später ggf. erfolgende Datenverarbeitung. Selbst wenn ein App-Publisher vom Nutzer alle nur möglichen Berechtigungen erhält, benötigt er nach der DSGVO für jede einzelne Verarbeitung personenbezogener Daten nach wie vor einen Rechtfertigungsgrund. Ein App-Publisher, der sich alle Zugriffsrechte vom Nutzer einräumen lässt, kann sich also dennoch im Hinblick auf die tatsächlich erfolgenden Datenverarbeitungen DSGVO-konform verhalten, wenn er nicht umfassend personenbezogene Daten des Nutzers abruft, sondern für jede einzelne Datenverarbeitung ein DSGVO-Rechtfertigungsgrund eingreift. Das Ersuchen einer App um Einräumung von Zugriffsberechtigungen bedeutet mithin auch kein Ersuchen um Einwilligung im Sinne von Art. 6 Abs. 1 lit. a) DSGVO. Eine wirksame Einwilligung kann nur unter diversen Voraussetzungen erteilt werden. Insbesondere müsste sich der Einwilligende im Zeitpunkt der Einwilligung darüber bewusst sein, welche konkreten personenbezogenen Daten von wem für welche Zwecke verarbeitet werden sollen. Diese Voraussetzungen erfüllen die kurz gehaltenen Zustimmungsanfragen, wie sie bei der Erstnutzung von Apps typischerweise angezeigt werden, nicht einmal ansatzweise. So enthalten die betreffenden Anfragen

beispielsweise so gut wie nie einen Hinweis auf die Widerruflichkeit der Einwilligung, welcher nach Art. 13 Abs. 2 lit. c) DSGVO zwingend erforderlich ist.[265]

Somit hat die Einholung von Zugriffsberechtigungen für die Frage der datenschutzrechtlichen Rechtmäßigkeit nachfolgender Verarbeitungen personenbezogener Daten keine unmittelbare Bedeutung. Die Legitimität der Verarbeitung personenbezogener Daten lässt sich vielmehr danach bemessen, ob die Datenverarbeitungen des App-Publishers, so wie sie in dessen Datenschutzerklärung beschrieben sind, den Verarbeitungs- und Informationsvorgaben der DSGVO genügen.[266] Allerdings zeigt die Praxis, dass Datenempfänger insbesondere die Rechtfertigungsgründe der berechtigten Interessen und der Erforderlichkeit zur Vertragserfüllung mitunter extrem weit, mutmaßlich in vielen Fällen zu weit, auslegen. Da sich von Apps initiierte Datenübermittlungen jedenfalls für Laien nicht nachvollziehen lassen, geht deshalb mit der Einräumung von nicht notwendigen Zugriffsrechten eine reale Gefahr rechtswidriger Verarbeitungen personenbezogener Daten einher.

Das Phänomen der überschießenden Zugriffsrechte wirft indessen im Hinblick auf den Grundsatz der datenschutzfreundlichen Voreinstellungen Fragen auf. Dieser Grundsatz ist in Art. 25 Abs. 2 DSGVO festgehalten. Demnach müssen geeignete technische und organisatorische Maßnahmen getroffen werden, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten (legitimen[267]) Verarbeitungszweck erforderlich sind, verarbeitet werden. Zwar bedeutet die Einräumung von Zugriffsrechten noch nicht, dass eine Datenverarbeitung auch tatsächlich stattfindet. Art. 25 Abs. 2 S. 2 DSGVO stellt jedoch klar, dass sich die Verpflichtung, personenbezogene Daten der betroffenen Person zu schützen, auch auf die Zugänglichkeit der Daten bezieht. Dabei geht es nicht nur um den Datenzugang Dritter, sondern auch um den Zugang durch den Verantwortlichen selbst, so dass dieser sich zulasten des Privatheitsschutzes der betroffenen Person selbst beschränken muss.[268] Dies untermauert auch § 71 Abs. 2 S.1 BDSG.[269] Dort heißt es nämlich:

---

265 Zu den Voraussetzungen einer wirksamen Einwilligung im Einzelnen s. den Abschlussbericht der Sektoruntersuchung Smart-TVs (Fn. 71), S. 130 ff.

266 Dabei besteht freilich häufig die Schwierigkeit, dass diese schwammig und unverständlich formuliert sind (was wiederum zur Rechtswidrigkeit der Datenverarbeitung führen kann).

267 Die Formulierung ist hier etwas unscharf; im Ergebnis dürfte unstreitig sein, dass die Verarbeitung auf dasjenige Maß beschränkt werden soll, welches nach der DSGVO zulässig ist. Abzustellen ist mithin nicht auf isolierte Zwecke, sondern auf Zwecke im Rahmen von Verarbeitungen, die nach der DSGVO gerechtfertigt sind.

268 *Martini* in: Paal/Pauly [Hrsg.], DSGVO BDSG, 3. Aufl. 2021, Art. 25 DSGVO Rn. 52 f.

269 Zwar wurde mit § 71 BDSG Art. 20 der EU-Richtlinie 2016/680 umgesetzt, dessen Wortlaut ist indessen mit Art. 25 DSGVO weitestgehend identisch.

> „Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden **können**, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist.“ [Hervorhebung hinzugefügt]

Eine Maßnahme zur Verwirklichung datenschutzfreundlicher Voreinstellungen in diesem Sinne wäre daher vorliegend, Apps aufgrund entsprechender Software-Einstellungen in den Voreinstellungen keinerlei überschießenden Zugriffsberechtigungen einzuräumen bzw. die Einräumung von Berechtigungen, die über das funktional Erforderliche und datenschutzrechtlich Gerechtfertigte hinausgehen, von einem Opt-in der betroffenen Person abhängig zu machen.[270]

Die Pflicht des Art. 25 DSGVO trifft jeweils den datenschutzrechtlich Verantwortlichen, also hier den App-Publisher. Dieser kann freilich – gerade bei vorinstallierten Apps – mit dem Gerätehersteller zusammenfallen.

b) Lauterkeitsrecht

Es stellt sich die Frage, ob die Nichtinformation über eine überschießende Einräumung von Berechtigungen als Verstoß gegen § 5a Abs. 2 S. 1 UWG gewertet werden könnte. Gemäß § 5a Abs. 2 UWG handelt unlauter, wer unter Berücksichtigung aller Umstände dem Verbraucher eine wesentliche Information vorenthält, die dieser benötigt, um eine informierte geschäftliche Entscheidung zu treffen, und deren Vorenthalten geeignet ist, den Verbraucher zu einer geschäftlichen Entscheidung zu veranlassen, die er andernfalls nicht getroffen hätte. Bei der überschießenden Einräumung von Berechtigungen mag man zweifeln, ob eine diesbezügliche Information die Wesentlichkeitsschwelle überschreitet. Der Rechtsprechung des Bundesgerichtshofs zufolge ist eine Information nur dann wesentlich, wenn ihre Angabe unter Berücksichtigung der beiderseitigen Interessen vom Unternehmer erwartet werden kann und ihr für die vom Verbraucher zu treffende geschäftliche Entscheidung ein erhebliches Gewicht zukommt.[271] Die geschäftliche Entscheidung des Verbrauchers wäre hier bei vorinstallierten Apps der Kauf des Smartphones bzw.

---

[270] Dies wäre beispielsweise denkbar, wenn die betroffene Person in eine weitergehende Datenpreisgabe zu Werbezwecken wirksam einwilligt.

[271] BGH, Urteil vom 16.05.2012, Az. I ZR 74/11, juris Rn. 36; BGH, Urteil vom 27.04.2017, Az. I ZR 55/16, BGHZ 215, 12, Rn. 19 – *Preisportal*.

Tablets, bei neu zu ladenden Apps die Entscheidung über die Vornahme des Downloads[272]. Informationen über überschießende Zugriffsrechte wären vor dem Gerätekauf/App-Download aufgrund ihrer Komplexität und der zur Verfügung stehenden Anzeigefläche schwer zu kommunizieren. Einwenden ließe sich auch, dass wichtige Informationen über tatsächlich erfolgende Datenverarbeitungen für den Verbraucher vorrangig wären und ein Hinausgehen über essentielle Kerninformationen aufgrund beschränkter Informationsaufnahme- und Informationsverarbeitungskapazitäten des Verbrauchers auch zu einer informationellen Überforderung führen kann.[273] Es kann somit nicht davon ausgegangen werden, dass fehlende Angaben zu überschießenden Berechtigungen sei lauterkeitsrechtlich als wesentlich einzustufen sind. Ein Verstoß gegen § 5a Abs. 2 S. 1 UWG scheidet unter diesen Umständen aus.

Qualifizierte man Art. 25 DSGVO als Marktverhaltensregel[274] im Sinne des § 3a UWG, so käme insoweit grundsätzlich auch ein Lauterkeitsrechtsverstoß in Betracht. Auch hier dürfte es aber an einer Eignung zur wesentlichen Beeinflussung des Verbraucherverhaltens fehlen, da es nicht wahrscheinlich ist, dass eine datensparsame Inanspruchnahme von Zugriffsberechtigungen für App-Nutzer unmittelbar ersichtlich und (anders als tatsächliche Datenzugriffe) für die App-Auswahl von großer Bedeutung wäre.

Eine Beschränkung der Zugriffsberechtigungen auf das technisch und datenschutzrechtlich zulässige Maß lässt sich somit nicht mit den Mitteln des Lauterkeitsrechts durchsetzen.

F. Verbesserungsmöglichkeiten und Handlungsempfehlungen

Um die oben dargestellten Defizite zu beseitigen oder zumindest zu verringern, schlägt das Bundeskartellamt eine Reihe von Maßnahmen vor.

I. Mehr Transparenz

Wie die vorliegende Sektoruntersuchung gezeigt hat, muss im Hinblick auf die Darstellung von App-spezifischen Verbraucherinformationen ein grundlegendes Umdenken stattfinden. So müs-

---

272 Man könnte zumindest bei Gratis-Apps als relevanten Zeitpunkt auch die Entscheidung ansehen, die App tatsächlich zu nutzen (Zeitpunkt des Erstaufrufs der App nach Installation). Im Ergebnis würde dies keinen Unterschied machen.

273 Vgl. *Obergfell* in: Fezer/Büscher/Obergfell [Hrsg.], Lauterkeitsrecht: UWG, 3. Aufl. 2016, § 5a Rn. 77 (m. w. N.).

274 Zum diesbezüglichen Meinungsstreit s. oben S. 75.

sen einerseits Datenschutzerklärungen nutzerfreundlicher, d. h. präzise, transparent, verständlich und leicht zugänglich ausgestaltet sein (dazu nachfolgend unter 1.). Andererseits wäre es realitätsfern zu glauben, eine umfassende Verbraucherinformation könnte allein mit der Verbesserung von Texten erreicht werden, die jedenfalls die Mehrheit der Verbraucher in der Regel allenfalls überfliegt. Es steht zwar zu hoffen, dass qualitativ verbesserte und vor allem verständlichere und übersichtlichere Datenschutzerklärungen künftig dazu führen werden, dass mehr Verbraucher sich die Mühe machen, diese gründlich durchzulesen. Aufgrund der allgemeinen Informationsüberflutung und nur begrenzt zur Verfügung stehender Zeit müssen sich Verbraucher aber auch ohne Lektüre von Datenschutzerklärungen über alle wesentlichen Aspekte von Datenverarbeitungen niederschwellig und schnell informieren können. Um dies zu unterstützen, sollten dem Verbraucher zum einen wichtige Produktinformationen schon vor dem Download einer App schriftlich zur Verfügung gestellt werden (dazu nachfolgend unter 2.). Zum anderen können knappe Darstellungen und Symbolik eine schnellen Verbraucherinformation bewirken (dazu nachfolgend unter 3.).

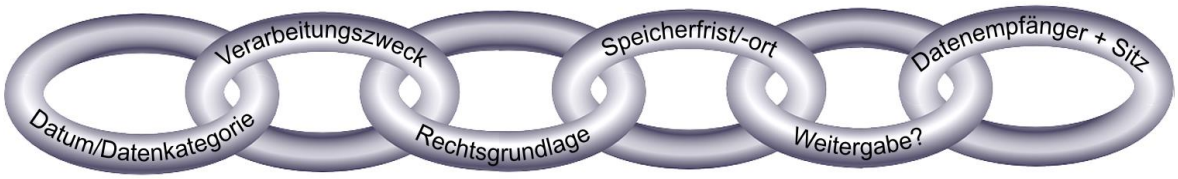
1. Präzise, verständliche und leicht zugängliche Datenschutzerklärungen

Wie bereits bei der Sektoruntersuchung Smart-TVs wurde auch im Rahmen der vorliegenden Sektoruntersuchung festgestellt, dass der größte Teil der Datenschutzerklärungen – bei Weitem nicht nur im Bereich mobiler Apps – daran krankt, dass diese für möglichst viele Anwendungssituationen und je nach Unternehmen sogar für eine Vielzahl verschiedener Dienste anwendbar sein sollen. Folge sind oft zu großen Teilen schwammige[275] und letztlich aussagefreie „one fits all"-Datenschutzerklärungen:

Vordergründig erfüllen solche Datenschutzerklärungen die Anforderungen und vor allem die Informationspflichten der DSGVO. Die Unverbindlichkeit der gewählten Formulierungen führt aber gerade dazu, dass wesentliche DSGVO-Grundsätze der Artikel 5 und 12 DSGVO (etwa Transparenz, Verständlichkeit, Fairness) missachtet werden. Um dem App-Nutzer vor Augen zu führen, was mit seinen personenbezogenen Daten genau geschieht, müsste der Verantwortliche hingegen, auch um den Anforderungen der DSGVO an Transparenz und Fairness zu genügen, den Weg der einzelnen Daten kenntlich machen:

:

[275] Zu einschränkenden Floskeln s. *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679" (Fn. 204), Rn. 12 f.



pixabay/Clker-Free-Vector-Images, verändert

Abbildung 60: Legitimationskette für Datenverarbeitungen

Dass ein erheblicher Teil der App-Publisher ausschließlich englischsprachige Datenschutzerklärungen einsetzt, ist bemerkenswert. Jedenfalls bei großen Unternehmen, die mit dem Absatz ihrer Apps in Deutschland in nennenswertem Umfang Umsatz generieren, ist nicht einzusehen, weshalb diese keine Datenschutzerklärungen in deutscher Sprache anbieten sollten.[276] Zwar kann der Nutzer im Browser ggf. selbst eine maschinelle Übersetzung vornehmen. Dies ist jedoch nicht ausreichend, zumal solche Übersetzungen nach heutigem Stand naturgemäß nicht fehlerfrei sein können.

Um die leichte Zugänglichkeit von Datenschutzerklärungen zu gewährleisten, sollten diese jedenfalls in den zentralen App-Informationen ebenso wie in der App-Beschreibung gut sichtbar verlinkt werden. *Apple* zeigt mittlerweile auf der jeweiligen App-Seite in seinem App-Store einen eigenen Abschnitt „App-Datenschutz“ an, der eine Verlinkung zur einschlägigen Datenschutzerklärung enthält. Auch in den zentralen App-Informationen gibt es einen Link zu der jeweiligen Datenschutzerklärung. Dies stellt unter Zugänglichkeits- und Transparenzgesichtspunkten eine gute Lösung dar.[277]

Klickt der Nutzer auf einen Link zu einer Datenschutzerklärungs-Webseite, so sollte er den verlinkten Text lesen können, ohne dass seine Nutzerdaten erhoben werden. Entsprechende Seiten sollten daher völlig frei von jeglichen Nutzerverfolgungsmethoden sein. Wo dies nicht der Fall ist,

276 Auch kleinere App-Publisher sind grundsätzlich verpflichtet, deutschsprachige Datenschutzerklärungen anzubieten. Allerdings könnte eine zwangsweise Durchsetzung dieser Pflicht auch gegenüber kleinen Anbietern, die mitunter auch datenschutzfreundliche Apps in alternativen App-Stores anbieten, zu deren Rückzug vom Vertrieb in Deutschland führen und so geradezu kontraproduktiv wirken.

277 *Google* hat angekündigt, App-Publisher ab dem 2. Quartal 2022 zur Bereitstellung einer Datenschutzerklärung sowie der Angabe, welche personenbezogenen Daten zu welchen Zwecken verwendet werden, zu verpflichten, s.https://android-developers.googleblog.com/2021/05/new-safety-section-in-google-play-will.html. In welcher Form dies konkret geschehen wird und ob Verbraucher den entsprechenden Hinweisen die wesentlichen Informationen mit hinreichender Klarheit und Genauigkeit entnehmen können, bleibt abzuwarten.

muss die Nutzerverfolgung über eine unmissverständliche Abfrage mit eindeutig gekennzeichneten Schaltflächen (z. B. „Akzeptieren“/“Ablehnen“) mit einem Klick abstellbar sein, bevor personenbezogene daten erhoben werden.

Datenschutzerklärungen - Was sich ändern sollte

- Primäres Ziel von Datenschutzerklärungen muss die Verständlichkeit für den Verbraucher sein.
- Datenschutzerklärungen müssen präzise benennen, welche personenbezogenen Daten bei welcher Nutzung zu welchen Zwecken verarbeitet werden.
- Der Weg der einzelnen Daten von Erhebung über Speicherung und ggf. Weitergabe muss transparent offengelegt werden.
- Im App-Store sollte die Datenschutzerklärung zu einer App gut sichtbar platziert werden, etwa in einem eigenen Datenschutzabschnitt, in den zentralen App-Informationen und der App-Beschreibung. Auch aus der App selbst heraus sollte die Datenschutzerklärung stets abrufbar sein.
- Datenschutzerklärungs-Webseiten dürfen keine Instrumente zur Nutzerverfolgung einsetzen; tun sie dies doch, müssen diese Instrumente mit einem Klick abgestellt werden können, noch bevor sie Daten übermitteln.

2. Orientierungshilfen für Verbraucher

Dass Verbraucher Datenschutzerklärungen mehrheitlich nicht oder allenfalls flüchtig lesen, ist eine durch etliche Studien und Umfragen bestätigte Tatsache.[278] Es muss daher gewährleistet sein, dass selbst der flüchtige Verbraucher zumindest die wichtigsten Informationen schnell erfassen kann.

a) Symbolik und Kurzbeschreibungen verwenden

Insbesondere wenn der Verbraucher Datenverarbeitungen nicht verweigern kann, muss er über die mit einer Softwareverwendung einhergehenden Datenverarbeitungen bestmöglich aufgeklärt werden. Dies sollte durch ein leicht verständliches, geschichtetes Informationsmodell geschehen,

[278] S. dazu oben Fn. 65 auf S. 30.

das sich durch Symbolik und Kurzbeschreibungen auszeichnet, wie bereits im Sektorbericht Smart-TVs vorgeschlagen.[279]

Seit Einführung von *Apple iOS 14.5* verlangt *Apple* zwar von App-Publishern die Angabe, welche personenbezogenen Daten zu welchen Zwecken genutzt werden.[280] Diese Initiative bietet mehr Transparenz und ist daher im Sinne einer verbesserten Verbraucherinformation zu begrüßen. Der Informationsgehalt der Angaben ist jedoch bislang gering. So können dieselben Datenkategorien und sogar Einzeldaten wie die Werbe-ID sowohl in der Rubrik „Daten, die zum Tracking deiner Person verwendet werden“ als auch in der Rubrik „Nicht mit dir verknüpfte Daten“ auftauchen. Zudem handelt es sich bei den Datenschutzübersichten um reine Selbstveranlagungen der App-Publisher, die nicht kontrolliert werden.

Dem Bundeskartellamt liegt ferner eine Verbändebeschwerde aus der Werbe- und Medienbranche vor, die sich gegen *Apples* Tracking-Einschränkung von Nutzern im Zusammenhang mit der Einführung des Betriebssystems *iOS 14.5* unter anderem dahingehend wendet, dass *Apple* sich im Hinblick auf seinen eigenen Apps keinen unmittelbar vergleichbaren Verpflichtungen unterzieht (Verweis auf PM Einleitung Verfahren nach § 19a, Apple).

Es bleibt zu hoffen, dass *Apple* das ATT Framework im Sinne von mehr Verbrauchersouveränität weiter verbessert, widersprüchliche Angaben eliminiert und weitere wesentliche Informationen angezeigt oder leicht zugänglich verlinkt werden (etwa zu Speicherdauer und Datenweitergabe). Auch Google sollte entsprechende aussagekräftige Übersichten bzw. Symbole entwickeln.[281]

b) Prüfungen durch unabhängige Institutionen fördern

In der Verbraucherbefragung des Bundeskartellamts wurden die Teilnehmer u. a. danach befragt, wie sie den Informationsgehalt des folgenden Prüfergebnisses (mit Link zu einer ausführlichen Bewertung) finden würden:

---

279 S. zu den Möglichkeiten kompakter Informationsdarstellung den Abschlussbericht der Sektoruntersuchung Smart-TVs (Fn. 71) ab S. 106.

280 S. dazu oben Abbildung 55 auf S. 110.

281 Offensichtlich gibt es hierzu bereits konkrete Überlegungen, s. Fn. 277.

Abbildung 61: Bewertungsergebnis einer Spiele-App (jugendschutz.net)

Die Teilnehmer der Befragung bewerteten ein solches Testergebnis ganz überwiegend als eher oder sehr hilfreich:

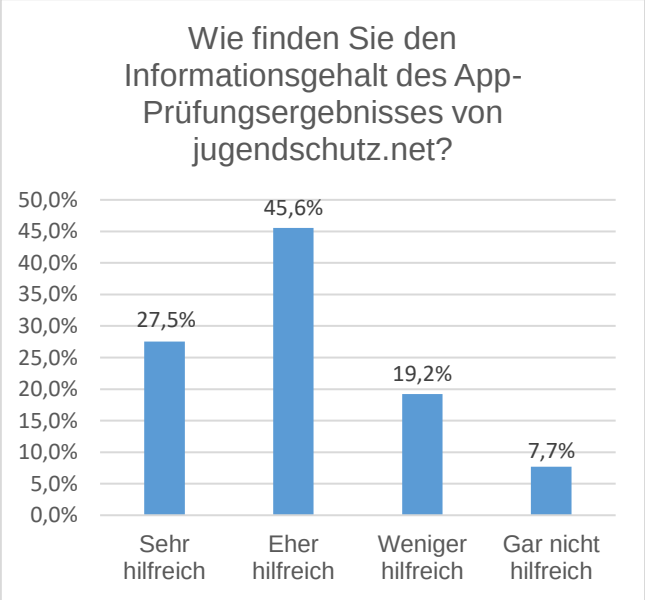


Abbildung 62: Verbrauchermeinung zu Bewertungsergebnis einer Spiele-App

Deutlich über 80 Prozent der Befragungsteilnehmer sprachen sich dafür aus, dass solche Bewertungsergebnisse generell für alle populären Apps zur Verfügung stehen sollten:

Abbildung 63: Verbrauchermeinung zur Verfügbarkeit von Prüfungsergebnissen für populäre Apps

Naturgemäß sind entsprechende App-Prüfungen jedoch recht aufwendig, insbesondere wenn der von einer App ausgehende Datenverkehr analysiert werden soll. Es sollte daher erwogen werden, entsprechende geeignete Projekte öffentlich zu fördern, soweit keine äquivalenten Beurteilungen durch öffentliche Stellen erfolgen.

Orientierungshilfen für den Verbraucher - Was sich ändern sollte

- Verbraucher sollten nicht gezwungen sein, lange Texte zu lesen, um zu verstehen, was mit ihren Daten geschieht. Unternehmen sollten die wichtigsten Informationen daher in kompakter Form bereitstellen, etwa in Form einer aussagekräftigen Übersicht oder eines sog. One-Pagers[282]. *Apple* geht für seinen App-Store mit der obligatorischen Anzeige wichtiger Datenschutzinformationen für jede App zwar den richtigen Weg; die aktuelle Umsetzung ist jedoch mangelhaft.

- Mithilfe von Bildsymbolen können Verbraucher wesentliche Informationen mit einem Blick wahrnehmen; eine aussagekräftige Symbolik könnte vom jeweiligen App-Store-Betreiber vorgegeben oder von (Branchen-)Verbänden vorgeschlagen werden. Die Europäische Kommission hat nach Art. 12 Abs. 8 DSGVO eine ausdrückliche Kompetenz, Bildsymbole verbindlich festzulegen.

[282] Beim One-Pager sollen die wesentlichen Informationen zum Umgang mit den personenbezogenen Daten der betroffenen Person verständlich auf höchstens einer A4-Seite dargestellt werden.

- Öffentliche Stellen sollten Initiativen zur Prüfung von Apps im Hinblick auf die Einhaltung datenschutz- und anderer verbraucherrechtlicher Vorschriften fördern. Auch sollten Projekte unterstützt werden, aus denen massentaugliche Anwendungen entstehen können, die den Verbraucher beim Verständnis komplexer Informationen effektiv unterstützen.

3. App-Informationen verbessern

Während bei Datenschutzerklärungen keineswegs gewährleistet ist, dass diese von der Mehrheit der Verbraucher gelesen werden, sind Angaben im unmittelbaren Umfeld eines App-Angebots zweifelsohne dazu geeignet, eine bessere Verbraucherinformation zu bewirken.

a) Transparente Information über Verantwortlichkeiten und Trackerverwendung

Bevor der Nutzer eine App aus dem App-Store herunterlädt, sollte diesem klar kommuniziert werden, wer bei Nutzung der App personenbezogene Daten erhält und wer für die Datenverarbeitung (allein oder gemeinsam) verantwortlich ist. In der Praxis dürften App-Publisher und Trackingunternehmen häufig gemeinsam Verantwortliche sein. In diesen Fällen wäre es sinnvoll, dass der App-Publisher die Information des App-Nutzers über den Einsatz von Trackern übernimmt. Dies könnte etwa durch eine detaillierte Auflistung aller wesentlichen Informationen zu den beteiligten Trackingunternehmen im Rahmen der Datenschutzerklärung des App-Publishers erfolgen. Ergänzend könnten die jeweiligen Vereinbarungen über die gemeinsame Verantwortlichkeit und die Datenschutzbestimmungen der Trackingunternehmen per Link zur Verfügung gestellt werden. Wo der App-Publisher sich ausschließlich solcher Links bedient, besteht die Gefahr einer Informationsüberflutung, jedenfalls wenn viele Tracker verwendet werden. Spätestens wenn auf den verlinkten Webseiten die wesentlichen Informationen nicht einfach aufzufinden sind und womöglich wiederum Tracking-Tools eingesetzt werden, die nicht einfach mit einem Klick abgeschaltet werden können, kann nicht mehr davon ausgegangen werden, dass der Verantwortliche die geforderten Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form“ übermittelt, wie es Art. 12 Abs. 1 S. 1 DSGVO verlangt.

Angesichts der Menge und Komplexität der zu erteilenden Informationen ist, jedenfalls ergänzend, eine vereinfachende Darstellung unter Verwendung aussagekräftiger Bildsymbolik erstrebenswert.[283]

[283] Siehe dazu unter Nr. 3, S. 119 ff. Ähnlich auch Abschlussbericht des BMJV, Verbraucherinformationen bei Apps (Fn. 35), S. 101, der für eine „Kompaktvariante“ plädiert.

b) Transparente Information über In-App-Käufe

Verbraucher sollten sich vor dem Herunterladen einer App ein realistisches Bild über mögliche künftige Kosten machen können, die mit der Nutzung der App verbunden sein können.[284] Daher sollten zum einen bereits vor dem Download detaillierte Preislisten abrufbar sein, die Gegenstand und Preis von Leistungserweiterungen der App präzise wiedergeben. Die jeweiligen Kaufgegenstände sollten dabei möglichst genau bezeichnet werden.[285]

Des Weiteren sollten durchschnittliche monatlich mit der App-Nutzung verbundene Kosten genannt werden. Dies kann insbesondere für Eltern ein hilfreiches Instrument sein, um abzusehen zu können, welche Kosten Apps verursachen können, die auf Geräten von Kindern installiert werden.

Aufgrund der glücksspielähnlichen Wirkungen von Lootboxen und gleichartigen Spieleelementen sollte zudem ein Hinweis im jeweiligen App-Store hierauf erfolgen, etwa „In-App-Käufe einschließlich zufallsabhängiger Inhalte“. Dies ließe sich auch symbolisch darstellen, etwa folgendermaßen:

Abbildung 64: Symbolvorschlag für In-App-Käufe von zufallsabhängigen Inhalten

c) Vertragspartner und Gewährleistungsregeln klarstellen

Wie gezeigt, sind die Gewährleistungsausschlüsse von *Google* und *Apple* in ihren jeweiligen Allgemeinen Geschäftsbedingungen unwirksam. Beide Unternehmen sollten daher sowohl in ihren AGB als auch bei der Präsentation von Apps in ihren App-Stores klar, konsistent und unzweifelhaft festlegen,

- wer bei einem App-Download Vertragspartner wird;

---

284 So auch Abschlussbericht des BMJV, Fn. 35, S. 74.

285 Falls dies eine Erläuterung erfordert, ließe sich dies über eine Einblendung bei Antippen des betreffenden Kaufgegenstands realisieren.

- dass gegen diesen Vertragspartner uneingeschränkt Gewährleistungsansprüche geltend gemacht werden können;
- wie die Abwicklung von Gewährleistungsansprüchen sowie ggf. auf Kulanz basierender Erstattungsmöglichkeiten vonstattengeht und welche Fristen hierfür gelten (wobei gesetzliche Fristen selbstverständlich nicht unterschritten werden dürfen).

Die Rechtsverhältnisse zwischen App-Store-Betreiber, Endabnehmer und App-Publisher sollten dabei einheitlich bezeichnet und festgelegt werden.[286]

Idealerweise sollten für In-App-Käufe und ggf. sonstige unter Beteiligung des App-Store-Betreibers zustande kommende Rechtsgeschäfte ebensolche Regelungen getroffen werden.

d) Vollständige Kontaktdaten angeben

Wie oben dargestellt, gilt die Impressumspflicht des § 5 TMG für die App-Stores sowie zumindest einen nicht unerheblichen Teil der angebotenen Apps. App-Store-Betreiber sollten daher ebenso wie App-Publisher jeweils zumindest detaillierte Kontaktdaten angeben. Für Apps sollten diese sowohl in den zentralen App-Übersichten im App-Store als auch in den Einstellungen bei der jeweiligen App-Info abrufbar sein[287].

App-Informationen verbessern - Was sich ändern sollte

- Für jede App sollte bereits vor dem Download klar und vollständig ausgewiesen werden, welche weiteren Unternehmen außer dem App-Publisher direkt oder durch Weitergabe durch den App-Publisher personenbezogene Daten bei Nutzung der App erhalten. Dies sollte nicht nur in der Datenschutzerklärung ausgewiesen werden, sondern bereits bei der Anzeige der zentralen App-Informationen.
- Jeder angebotene In-App-Kauf sollte sinntragend bezeichnet und mit Preisangabe aufgelistet werden.

---

286 Dies ist auch ein Punkt, den die niederländische *Autoriteit Consument & Markt (ACM)* gegenüber Google bemängelt hat, s. *ACM*, Google must better comply with consumer rights (Pressemeldung vom 23.07.2021), abrufbar unter https://www.acm.nl/en/publications/google-must-better-comply-consumer-rights.

287 Dies ist umso dringlicher, als bei bereits vorinstallierten Apps selbst die oftmals zu spärlichen im App-Store angezeigten Informationen fehlen. Als Voraussetzung für eine Anzeige notwendiger Angaben müsste indessen das Betriebssystem entsprechend angepasst werden.

- Auf In-App-Käufe mit Zufallsinhalt sollte, auch wenn kein Glücksspiel im rechtlichen Sinne vorliegt, aufgrund der Suchtgefahr gesondert hingewiesen werden.
- Es sollte für den App-Store-Nutzer völlig klar ersichtlich sein, von wem sie eine App beziehen; die entsprechenden Akteure sollten in allen Texten und Angaben einheitlich und aus Laiensicht zweifelsfrei bezeichnet werden (z. B. als App-Verkäufer oder eben als Vertreter oder Vermittler).
- Die Geltendmachung von Gewährleistungsansprüchen sollte automatisiert werden und innerhalb von 24 Monaten nach App-Kauf eine leicht zugängliche, einfache Kauf-Rückabwicklung mit wenigen Klicks erlauben.

II. Mehr Verbraucherkontrolle

Mehr Transparenz ist für die Souveränität von Verbraucherentscheidungen unabdingbar. Informationen sind aber wenig hilfreich, wenn der Verbraucher letztlich nur die Wahl zwischen unterschiedlichen Angeboten hat, die in ähnlichem Ausmaß dessen Recht auf informationelle Selbstbestimmung beeinträchtigen. Es ist daher wichtig, dem Verbraucher Instrumente an die Hand zu geben, um Datenflüsse selbst möglichst einfach und effektiv kontrollieren zu können.

1. Verbraucherhoheit über App-Auswahl

Je mehr Apps auf einem Smartphone oder Tablet installiert sind, desto größer ist auch die Gefahr unerwünschter Abflüsse personenbezogener Daten. Der Verbraucher sollte daher nicht gezwungen sein, Apps auf seinem Gerät zu akzeptieren, die er nicht benötigt. Ein völliger Verzicht auf nicht systemrelevante Software oder jedenfalls sämtliche sog. Bloatware wäre einerseits eine aus Verbrauchersicht hilfreiche Maßnahme. Andererseits können Vorinstallationen das Endgerät auch billiger machen, da App-Publisher bereit sind, den Gerätehersteller für die Vorinstallation zu bezahlen oder der Gerätehersteller sich künftige Einnahmen aus der Vorinstallation seiner eigenen Apps erhofft. Zudem sieht anscheinend ein erheblicher Teil der Verbraucher eine gewisse Minimalausstattung an Apps als positiv an[288]. Will man dem Gerätehersteller hier Freiräume belassen, so könnte man gesetzgeberisch darauf hinwirken, dass nicht systemrelevante Software stets deinstallierbar (und nicht nur deaktivierbar) sein sollte. Einwände von Herstellerseite, eine Deinstallierbarkeit führe zu Problemen bei einem Zurücksetzen des Geräts, sind bereits durch

[288] S. dazu Abbildung 15 auf S. 31.

die Praxis hinreichend widerlegt.[289] Wie im Bericht gezeigt[290], hat *Apple* in *iOS 14* bereits den größten Teil nicht systemrelevanter Apps deinstallierbar ausgestaltet.

Zwar sieht der Digital Markets Act auf europäischer Ebene vor, dass sog. Gatekeeper die Deinstallation von nicht systemrelevanten Software-Anwendungen nicht einschränken dürfen.[291] Aus Verbrauchersicht ist indessen nicht einsichtig, weshalb eine solche Deinstallierbarkeitsverpflichtung nur Gatekeeper und nicht generell auch alle Smartphone-Hersteller treffen sollte. Ein gesetzgeberisches Nachbessern in diesem Punkt, ggf. auch außerhalb des Digital Markets Act, wäre daher zu begrüßen.

2. Verbrauchereinwilligung bzgl. Drittempfängern einholen

Idealerweise sollten Apps die Einwilligung des Verbrauchers einholen, bevor sie den Datenzugriff durch Dritte erlauben. Es ist nicht auszuschließen, dass eine Einwilligung bzgl. jedes einzelnen Drittempfängers, die den strengen Vorgaben der DSGVO genügt, zu einer nicht unerheblichen Zahl von Einwilligungsersuchen führen könnte. Dies könnte jedoch auch zu einem Umdenken bei App-Publishern dahingehend führen, dass Apps weniger oder keinen Dritten Zugriff auf personenbezogene Daten einräumen. Auch könnten sog. Personal Information Management-Systeme (kurz „PIMS“) Abhilfe schaffen. Mit solchen Einwilligungsverwaltungsdiensten könnte der einzelne Nutzer seine Datenschutzpräferenzen festlegen, und Apps oder Websites könnten diese Präferenzen abfragen und umsetzen. Diesbezüglich stellen sich allerdings noch etliche technische und datenschutzrechtliche Fragen[292], so dass nicht zu erwarten ist, dass entsprechende Dienste in der Breite kurzfristig zur Verfügung stehen werden.

3. Einfache Einstellung von Datenschutzpräferenzen

Bereits bei der Erstinbetriebnahme eines neuen Smartphones oder Tablets wird der Verbraucher mit etlichen, teils sehr komplexen, Nutzungs-, Lizenz- und Datenschutzbestimmungen konfrontiert, die sich leicht auf mehr als 200 Bildschirmseiten addieren können. Auch beim Aufruf einzelner (vorinstallierter) Apps werden dem Nutzer mitunter sehr lange Texte angezeigt. Da bei rea-

---

289 Wie oben gezeigt ist es möglich, Apps deinstallierbar auszugestalten und diese bei einem Werksreset neu zu installieren bzw. aus dem Internet nachzuladen, s. dazu oben S. 32 bzw. 35.

290 S. insbesondere Abbildung 17 auf S. 32.

291 S. dazu oben S. 37 f.

292 S. dazu etwa *Blankertz/Specht*, Wie eine Regulierung für Datentreuhänder aussehen sollte (Juli 2021), S. 3, abrufbar unter https://www.stiftung-nv.de/sites/default/files/regulierung_fuer_datentreuhaender.pdf.

listischer Betrachtung kein Nutzer all diese Texte tatsächlich durchliest, wäre es aus Verbrauchersicht sinnvoll, dem Nutzer die Möglichkeit einzuräumen, wesentliche Vorkehrungen gegen mögliche Datenschutzverletzungen zentral vorzunehmen. Naturgemäß sind grundsätzlich nur die Betriebssystem-Betreiber in der Lage, entsprechende Anforderungen technisch zu realisieren.

So sollte es etwa möglich sein, den Zugriff von Apps auf bestimmte Gerätefunktionen vollständig zu verweigern und ggf. für einzelne Apps bei Bedarf wieder einzuräumen. *Apple* hat dies mittlerweile für Ortungsdienste und Werbetracking bereits umgesetzt.

Soweit nicht systemrelevante App-Funktionen betroffen sind, sollten sämtliche[293] Zugriffsberechtigungen jeder App auf Gerätefunktionen, die mit Verarbeitungen personenbezogener Daten einhergehen können, übersichtlich auf einer (scrollbaren) Displayseite dargestellt und ablehnbar ausgestaltet werden. Dass womöglich viele Verbraucher zumindest bei einem Teil der Berechtigungen nicht beurteilen könnten, ob ein Datenzugriff für das Funktionieren der App benötigt wird oder nicht, steht dem nicht entgegen. Zum einen existieren Berechtigungen (z. B. „Internetdaten erhalten“), deren Verständnis keine Fachkenntnisse erfordert; auch könnten etliche Berechtigungen bzw. Berechtigungskategorien benutzerfreundlicher ausgestaltet und verständlicher bezeichnet werden. Zum anderen wären entsprechende Hilfestellungen von dritter Seite denkbar, möglicherweise könnte jedenfalls mittelfristig auch eine eigenständige Gerätefunktion oder App die Berechtigungseinstellungen nach Nutzervorgaben (z. B. „minimale Berechtigungen“) übernehmen. Wie oben gezeigt, würden mehr als 80 Prozent der Nutzer eine solche Funktionalität hilfreich finden.[294]

Bei allen Informationen über Verarbeitungen personenbezogener Daten muss sichergestellt sein, dass der Nutzer trotz der begrenzten Anzeigefläche alle wesentlichen Angaben schnell und lückenlos erfassen kann. Einwilligungen müssen dabei insbesondere so ausgestaltet werden, dass die Ablehnung von Datenverarbeitungen nicht aufwendiger ausgestaltet wird als deren Annahme. Auch darüber hinaus dürfen Unternehmen keine sprachlichen oder designtechnischen Manipulationen verwenden, um die Entscheidung des Nutzers in eine gewünschte Richtung zu lenken. Zur

---

293 Sowohl bei *Android* als auch bei *iOS* wird dies bislang nur teilweise umgesetzt, so kann z. B. die Internetzugriffsberechtigung nicht vollständig gesperrt werden. Inwieweit das für *Android* 12 angekündigte Privacy-Dashboard (Datenschutz-Cockpit) hier bereits erste grundlegende Verbesserungen mit sich bringt, ist derzeit noch nicht absehbar.

294 Siehe Abbildung 48 auf S. 106.

Frage einer nicht-manipulativen[295] Einwilligungsgestaltung gibt es mittlerweile eine Vielzahl einschlägiger Publikationen.[296]

Das von *Apple* mit *iOS 14.5* eingeführte ATT-Framework lässt den Nutzer selbst über die Zulassung von Tracking durch Dritte entscheiden. Ungeachtet der Fragen, ob hier Umgehungsmöglichkeiten[297] bestehen, möglicherweise eine Selbstbevorzugung des Store-Betreibers vorliegt oder nicht auch exzessive Datenverarbeitungen durch die App-Publisher selbst verstärkt eingehegt werden sollte, stellt dies – jedenfalls unter Verbraucherschutzgesichtspunkten – einen deutlichen Schritt zu mehr Verbrauchersouveränität dar. Die gesetzlichen Informationspflichten sind zwar hilfreich, können in der Praxis aber mitunter nur begrenzt Wirkung entfalten. Selbst wenn die notwendigen Angaben auch in kompakter Darstellung erhältlich sein sollten, muss sich der Nutzer mit einer Fülle von Informationen auseinandersetzen. Die reine Information ist für den Nutzer aber nur begrenzt hilfreich, sofern er die Datenverarbeitungen nicht wünscht, sie aber auch nicht wirklich verhindern kann. Eine effektive Abschaltvorrichtung kommt dem Nutzer daher viel eher entgegen und sollte aus Verbrauchersicht grundsätzlich auch von anderen Betriebssystembetreibern angestrebt werden. Dabei sind naturgemäß nur die Betriebssystem- und App-Store-Betreiber in der Lage, Vorrichtungen wie Zugriffssperren für die Werbe-ID des Geräts effektiv umzusetzen.

4. App-Suche überarbeiten

Zum einen zeigen sich – wie oben dargestellt – sowohl bei *Google Play* als auch beim App-Store von *Apple* deutliche Mängel bei der Darstellung von Suchergebnislisten. Diese könnten bereits

---

295 *Weinzierl*, Vertane Chance – Die Cookie-Prüfung der deutschen Datenschutzbehörden lässt das Thema „Dark Patterns“ liegen, ZD-aktuell 2020, 04419, weist im Zusammenhang mit Cookie-Einwilligungen darauf hin, dass die Problematik der sog. Dark patterns (= manipulatives Verleiten des Nutzers zur Vornahme bestimmter Entscheidungen im Sinne des Fragestellers) bislang kaum thematisiert und sanktioniert wird.

296 S. z. B. die entsprechende Empfehlung bzw. Leitlinien der französischen Datenschutzbehörde *CNIL* (Fn. 211 bzw. 212); *Kettner/Thorun/Spindler*, Innovatives Datenschutz-Einwilligungsmanagement (07.09.2021), abrufbar unter https://www.bmjv.de/SharedDocs/Downloads/DE/Service/Fachpublikationen/090620_Datenschutz_Einwilligung.pdf;jsessionid=69E62FAA4519ED5B5B2099B0A8A2DA92.1_cid297?__blob=publicationFile&v=3; *Santos/Bielova/Matt,* Are cookie banners indeed compliant with the law?, Technology and Regulation, 2020, 91, abrufbar unter https://techreg.org/index.php/techreg/article/view/43/25; *Utz/Degeling/Fahl/Schaub/Holz*, (Un)informed Consent: Studying GDPR Consent Notices in the Field, in: 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS ’19), November 11–15, 2019, London, abrufbar unter https://doi.org/10.1145/3319535.3354212.

297 S. etwa *McGee*, *Apple* under pressure to close loopholes in new privacy rules (FT.com, 07.06.2021), abrufbar unter https://www.ft.com/content/9cb52394-f95f-4b07-a624-89c47439aa16.

jetzt oder jedenfalls nach Anpassung und Inkrafttreten der nationalen die Omnibus-Richtlinie umsetzenden Rechtsvorschriften Rechtsverstöße darstellen. Zum anderen wird der Verbraucherwunsch nach besseren Sortier- und Filtermöglichkeiten weitgehend bis vollständig ignoriert. *Google* und *Apple* sollten hier Maßnahmen für mehr Transparenz und individuelle Anpassbarkeit ergreifen.

Die Parameter, nach denen sich die Rangfolge von Apps in Suchergebnislisten bestimmt, sollten für die Verbraucher deutlich gemacht werden. Dies könnte beispielsweise über eine im unmittelbaren Zusammenhang mit den Suchergebnissen angezeigte Schaltfläche geschehen, bei deren Anklicken in einem Pop-up-Fenster zumindest die Hauptparameter sowie deren grobe Gewichtung angegeben werden. Die App-Store-Betreiber sind allerdings nicht gehalten, die Funktionsweise von Sortieralgorithmen konkret offenzulegen, zumal dies eine Manipulation seitens der App-Publisher erleichtern könnte. Realistischerweise kann durch die generalisierende Darstellung von Rankingparametern und deren Gewichtung daher nur ein rudimentäres Verständnis für die Suchreihung erreicht werden.

Eine deutlich höhere praktische Bedeutung kommt daher Sortier- und Filterparametern zu, mit denen Verbraucher selbst ihre App-Suche gestalten können.

Ergebnisse effektiv sortieren und filtern zu können, ist nicht nur aus Verbrauchersicht, sondern auch im Interesse der App-Publisher sinnvoll und dringend geboten. In der Verbraucherbefragung des Bundeskartellamts waren über 90 Prozent der Befragten nicht bereit, mehr als zehn Bildschirmseiten zu scrollen. Dies würde im Beispiel der Suche nach einer Sudoku-App bedeuten, dass der Großteil der Verbraucher bei *Google Play* weniger als ein Drittel und bei *Apples* App-Store sogar weniger als 10 Prozent der einschlägigen Suchergebnisse überhaupt zur Kenntnis nimmt. Apps, die sich durch bestimmte, vom Verbraucher erwünschte Eigenschaften auszeichnen (z. B. werbefrei, ohne In-App-Käufe)[298], sind daher über die App-Suche ggf. kaum auffindbar. Soweit ersichtlich sind Filterfunktionen auch bei anderen App-Stores als denen von *Google* und *Apple* nicht sonderlich ausgereift. Beim *Aurora*-App-Store lassen sich zumindest „Apps mit Werbung“ herausfiltern.

[298] Siehe dazu Abbildung 23 auf S. 40.

App-Stores sollten ihren Nutzern hier deutlich mehr Möglichkeiten anbieten. Entsprechende Parameter, die große Teile der Verbraucher als hilfreich ansehen, wurden oben bereits dargestellt[299]. Des Weiteren sollte der Nutzer auch solche Apps aus den Suchergebnissen ausschließen können, die eine Registrierung voraussetzen.[300] Außerdem wäre es aus Jugendschutzgesichtspunkten zu begrüßen, Apps aus einer Suche ausschließen zu können, die glücksspielähnliche Elemente wie z. B. sog. Lootboxen[301] enthalten.

Mehr Kontrolle an die Verbraucher übertragen - Was sich ändern sollte

- Sämtliche Anwendungen auf einem mobilen Endgerät sollten deinstallierbar sein, soweit sie nicht systemrelevant sind. Dies gilt auch für (Sprach-)Assistenten.
- Eröffnet eine App einen Zugriff auf Nutzerdaten durch Dritte, sollte hierfür grundsätzlich eine Einwilligung des Nutzers vorliegen.
- Nutzer sollten ihre Datenschutzpräferenzen einfach und zentral einstellen können. Nutzer sollten insbesondere Apps sämtliche Zugriffsrechte auf datenschutzrelevante Gerätefunktionen entziehen bzw. diese in eigener Regie verwalten können. Dabei sollte es möglich sein, solche Berechtigungen standardmäßig für alle Apps auf einmal zu deaktivieren und ggf. später Ausnahmen zuzulassen.
- Betriebssystem-Betreiber sollten den Nutzer in die Lage versetzen, Third-Party-Tracking durch Apps effektiv abzuschalten.[302]
- Die App-Suche muss so ausgestaltet sein, dass dem Nutzer bei Ausgabe der Suchergebnisliste alle wesentlichen Ranking-Kriterien und deren Gewichtung angezeigt werden. Noch wichtiger ist jedoch, dass dem Nutzer sinnvolle Filterkriterien an die Hand gegeben werden, die es insbesondere erlauben, nach Apps zu suchen, die Verbraucherinteressen wie Daten- oder Jugendschutz besser berücksichtigen (Offline-Apps, trackerfreie Apps, Apps ohne Registrierungszwang, Apps ohne In-App-Käufe…).

299 S. oben Abbildung 22 auf S. 39 und Abbildung 23 auf S. 40.

300 In Anbetracht der Tatsache, dass Third-party-tracking durch *Apple* bereits jetzt und für *Android*-Apps evtl. künftig erschwert wird, könnten womöglich Registrierungspflichten ausgeweitet werden, um so eine Zuordnung zu einem bestimmten Nutzer und dessen gezielte werbliche Ansprache zu ermöglichen.

301 S. dazu oben S. 95.

302 *Google* müsste diese Möglichkeit als Betriebssystem-Betreiber auch für Apps sicherstellen, die nicht von *Google Play* heruntergeladen wurden.

III. Mehr Rechtsdurchsetzung

Wie im vorliegenden Bericht ausgeführt, bestehen in einzelnen Punkten ernsthafte Zweifel, ob große App-Publisher, Werbenetzwerke sowie Betriebssystem- und App-Store-Betreiber sich stets an geltende datenschutzrechtliche Vorgaben halten.

Auch mehr als drei Jahre nach Inkrafttreten der DSGVO bleiben datenschutzrechtliche Verfahren gegen große Internetkonzerne dennoch Mangelware. Dabei stehen der jeweils zuständigen Behörde bei (drohenden) Verstößen gegen die DSGVO grundsätzlich effektive Sanktionsmittel zur Verfügung. Sie kann sich einerseits milder Mittel wie Hinweisen oder (Ver-)Warnungen bedienen. Andererseits kann sie auch Bußgelder verhängen, die bis zu 4 Prozent des Jahresumsatzes des Unternehmens betragen können.

Es stellt sich indessen die Frage, ob die prominente Rolle, die die DSGVO der federführenden Datenschutzaufsichtsbehörde zugedacht hat, einer effektiven Rechtsdurchsetzung stets förderlich ist. Anders als beispielsweise die Organisation der Durchsetzung des europäischen Wettbewerbsrechts setzt die DSGVO auf ein Prinzip exklusiver Federführung einer nationalen Behörde, die sich zudem am Sitz statt an den räumlichen Tätigkeitsbereichen bzw. Auswirkungen von Verhaltensweisen des Unternehmens orientiert. Die mutmaßlich größten datenverarbeitenden Unternehmen haben ihren EU-Hauptsitz in Irland, und es wird in der öffentlichen Diskussion immer häufiger die Frage gestellt, inwieweit die dortige federführende Aufsichtsbehörde willens und in der Lage ist, gegenüber den Internetgiganten ein höheres Datenschutzniveau zugunsten der Verbraucher in der EU durchzusetzen. Dass das Europäische Parlament die Europäische Kommission auffordert, ein Vertragsverletzungsverfahren gegen einen Mitgliedstaat wegen Untätigkeit einer Behörde anzustrengen, dürfte einen einmaligen Vorgang darstellen.[303] Mitunter wurden auch bereits Rufe nach einer zentralen EU-Datenschutzbehörde laut, die große, grenzüberschreitende Fälle übernehmen könnte.[304]

Auch die private Rechtsdurchsetzung tut sich bislang schwer. Das in Art. 80 Abs. 2 DSGVO vorgesehene Verbandsklagerecht bei Datenschutzverletzungen ist von einer optionalen Aktivierung durch die jeweiligen EU-Mitgliedstaaten abhängig. Privatklagen gegen große datensammelnde

---

303 S. dazu Entschließung des Europäischen Parlaments vom 20. Mai 2021 zu dem Urteil des Gerichtshofs der Europäischen Union vom 16. Juli 2020 – Data Protection Commissioner gegen Facebook Ireland Limited und Maximilian Schrems („Schrems II“) – Rechtssache C-311/18 (2020/2789(RSP)), Rn. 4 a. E., abrufbar unter https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_DE.pdf.

304 *Neuerer*, Datenschützer Kelber bringt neue EU-Behörde gegen Facebook & Co. ins Spiel (Handelsblatt.de, 28.01.2020), abrufbar unter https://www.handelsblatt.com/politik/deutschland/datenschutz-verstoesse-datenschuetzer-kelber-bringt-neue-eu-behoerde-gegen-facebook-und-co-ins-spiel/25479302.html?ticket=ST-819531-aeRBVIsIEpBtaAbHbyjw-ap2.

Unternehmen wie diejenige des *Irish Council for Civil Liberties* gegen *IAB Labtech*[305] bilden bislang die Ausnahme. Grund hierfür neben dem relativ hohen Prozesskostenrisiko auch die praktische Schwierigkeit sein, verschlüsselte und/oder unternehmensinterne Datenflüsse überhaupt nachvollziehen zu können. Einzelne betroffene Personen können bei Datenschutzverletzungen zwar ebenfalls klagen; die DSGVO erlaubt dies bereits jetzt; möglicherweise können bestimmte Ansprüche künftig auch auf Basis des Lauterkeitsrechts geltend gemacht werden. Allerdings dürfte der Einzelne im Regelfall mangels technischer Überwachungsmöglichkeiten und extrem vage formulierter Datenschutzerklärungen (und mutmaßlich häufig ebenfalls unzureichender individuell erteilter Auskünfte[306]) schon nicht ermessen können, welche personenbezogenen Daten überhaupt verarbeitet und ggf. weitergegeben wurden. Mangels greifbaren materiellen Schadens und Unklarheit über das Ausmaß der Datenverarbeitung dürften betroffene Personen daher in aller Regel den Aufwand rechtlicher Auseinandersetzungen mit großen Datenverarbeitern scheuen (rationale Apathie).

Die App-Stores selbst und vor allem die Betriebssysteme *iOS* und *Android* haben sich in Datenschutzbelangen zwar durchaus weiterentwickelt. So stehen dem Nutzer heute etwa deutlich mehr Kontrollmöglichkeiten zur Verfügung, um Datenzugriffe durch Apps zu unterbinden, als früher. Auch wenn *Apples ATT Privacy Framework* noch verbesserungsfähig sein mag, hat *Apple* Verbrauchern damit erstmals ein einfach handhabbares Mittel an die Hand gegeben, um bislang zumeist unbemerkte Datenabflüsse an Drittunternehmen zu unterbinden. Wünschenswert wäre darüber hinaus jedoch, dass die App-Store-Betreiber sich selbst stärker als bisher darum bemühen, Apps aus ihrem Angebot zu entfernen, die offensichtlich gegen Datenschutzrecht (evtl. auch gegen anderes Verbraucherrecht, z. B. betrügerische Fake-Shops oder Finanzdienstleister) verstoßen. App-Store-Betreiber könnten App-Publishern insoweit verbindliche Vorgaben zur Datenminimierung machen, diese auch überprüfen und Publisher bei Verstößen aus dem App-Store verbannen. Anhaltspunkte für Verstöße lassen sich auch Kundenrezensionen zu Apps entnehmen. Verbraucher sollten zudem eine – optional anonyme – Möglichkeit haben, Verbraucherrechtsverstöße bei den App-Store-Betreibern zu melden. Behörden und Verbänden könnte eine privilegierte Beschwerdemöglichkeit eingeräumt werden mit dem Ziel, entsprechende Meldungen unverzüglich und schnell zu prüfen. Spiegelbildich hierzu könnte man erwägen, eine (Mit-)Haftung von App-Stores für solche Fälle gesetzlich festzuschreiben, in denen App-Publisher trotz offensichtlicher und dem App-Store-Betreiber bekannter Rechtsverstöße ihre Apps weiterhin über

---

305 S. dazu *Nezik/Langemann*, Aktivist klagt vor Hamburger Landgericht gegen Onlinewerbung (Zeit Online, 16.06.2021), abrufbar unter https://www.zeit.de/digital/datenschutz/2021-06/datenschutz-internetwerbung-irish-council-civil-liberties-hamburg-klage.

306 S. hierzu Netflix, Spotify & YouTube: Eight Strategic Complaints filed on Right to Access (NOYB, 18.01.2019), abrufbar unter https://noyb.eu/en/netflix-spotify-youtube-eight-strategic-complaints-filed-right-access.

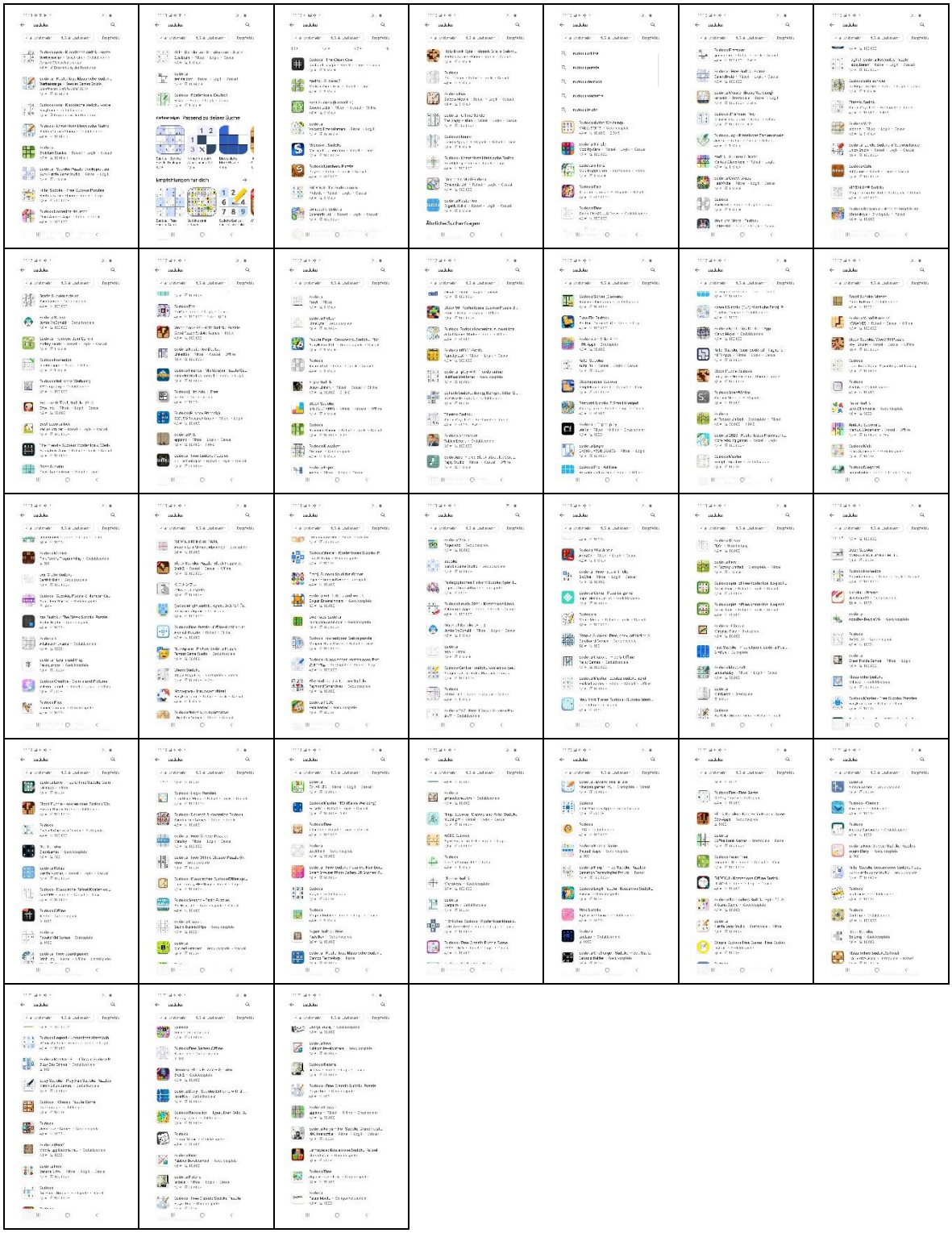
den App-Store vertreiben dürfen. Angesichts der Tatsache, dass viele App-Publisher außerhalb der EU ansässig sind und eine Rechtsdurchsetzung diesen gegenüber erhebliche praktische Schwierigkeiten bereiten kann, könnte schließlich erwogen werden, Aufsichtsbehörden als *utlima ratio* die Befugnis zu erteilen, App-Store-Betreibern den Vertrieb bestimmter Apps in dem Mitgliedstaat der betreffenden Aufsichtsbehörde zu untersagen.

Mehr Rechtsdurchsetzung - Was sich ändern sollte

- Das Durchsetzungsregime der DSGVO müsste grundlegend überdacht werden. Die Schaffung einer europäischen Institution zur Übernahme großer grenzüberschreitender Fälle – ähnlich dem Netz der europäischen Wettbewerbsbehörden – wäre eine mögliche Option.
- Um ihre jeweilige Schlagkraft zu verbessern und nötige Fachkenntnisse aufzubauen, sollten alle Behörden mit Aufsichtsbefugnissen in der Datenökonomie weitreichende Kooperationsbefugnisse erhalten.
- Zur Durchsetzung von verbraucherschützenden Rechtsnormen (insb. des Datenschutzrechts) sollte erwogen werden, Behörden gegen App-Store-Betreiber als ultima ratio einen Anspruch auf Sperrung von App-Publishern einzuräumen.

G. Anhang 1

Ergebnisliste für den Suchbegriff Sudoku auf *Google Play* (31 Displayseiten).



H. Anhang 2

Ergebnisliste für den Suchbegriff *Sudoku* im *Apple App Store* (137 Displayseiten):