Merle Freye

Die Datenschutzerklärungen von Gesundheits-Apps

Gesundheits-Apps[1] wie die Corona-Warn-App oder auch die Samsung Health App prägen den Alltag zahlreicher Smartphone-Nutzer/innen. Bereits 2016 stellten die Datenschutzbehörden insoweit aber erhebliche Mängel der Datenschutzerklärungen von Gesundheits-Apps fest.[2] Der vorliegende Beitrag veranschaulicht am Beispiel von zehn Gesundheits-Apps, dass viele Erklärungen auch sieben Jahre später immer noch unzureichend sind.

1 Einleitung

Spätestens mit der Einführung der appbasierten elektronischen Patientenakte und den Apps auf Rezept (Digitale Gesundheitsanwendungen, DiGA) sind Gesundheits-Apps in Deutschland massentauglich geworden. Zusätzlich hat auch die Covid-19-Pandemie die Verarbeitung von Gesundheitsdaten durch Apps vorangetrieben. Angesichts der Sensibilität der verarbeiteten Gesundheitsdaten besteht jedoch eine gewisse Skepsis[3] gegenüber der Nutzung von Gesundheits-Apps. Diese Skepsis wird auch dadurch genährt, dass abgesehen von Enthüllungen durch Hacker-Kollektive[4] in der Regel nicht transparent ist, was mit den Daten geschieht. Einen Einblick in die Funktionsweise der Apps sollte eigentlich die Datenschutzerklärung (DSE) ermöglichen. Diese wird von den Nutzer/innen jedoch bekannterweise selten konsultiert. Die vorliegende Untersuchung zeigt am Beispiel von zehn Gesundheits-Apps aus dem Google Play Store, dass die Erklärungen aus gutem Grund nicht gelesen werden. Vier[5] dieser Apps stammen aus dem kommerziellen Bereich und wurden ausgewählt, da sie von den Nutzer/innen des Google Play Stores am 1. Oktober 2022 am häufigsten heruntergeladen wurden.[6] Zusätzlich sind drei digitale Gesundheitsanwendungen (DiGA) Bestandteil der Untersuchung, die im 1. Oktober 2022 als App verfügbar und dauerhaft als DiGA angenommen waren.[7] Laut Statista waren zudem die Corona-Warn-App und die CovPass-App im Januar 2022 die beliebtesten Apps im Google Play Store,[8] sodass auch sie Prüfungsgegenstand sind. Die Erklärungen der zehn Apps werden im Hinblick auf die Informationspflichten der Art. 13, 14[9] DSGVO und die Vorgaben des Art. 12 DSGVO zur transparenten Information untersucht.

2 Form und Sprache, Art. 12 DSGVO

Nach Art. 12 Abs. 1 S. 1 DSGVO soll der Verantwortliche Maßnahmen treffen, um Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu vermitteln. Die Erklärungen der zehn Gesundheits-Apps werden anhand der Leitlinien[10] untersucht, die die Art.-29-Datenschutzgruppe (Datenschutzgruppe) für das Transparenzerfordernis aufstellte und die der EDSA 2018 ausdrücklich angenommen hat.[11] Auch die Empfehlungen zu Design-Mustern für den digitalen Kontext aus dem Jahr 2022 sind Maßstab der Untersuchung.[12] Zwar beziehen sich Letztere hauptsächlich auf Social Media, dennoch enthalten sie teilweise Vorgaben im Hinblick auf Art. 12 DSGVO, sodass zumindest einige Ausführungen als Kriterien für die folgende Untersuchung dienen.

1 Der Begriff der Gesundheits-Apps wird als Überbegriff für Medizin-Apps, Fitness-Apps und digitale Gesundheitsanwendungen (DiGA) verstanden.

2 BfDI: https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2016/19_Gesundheitsapps.html?nn=5217040.

3 Forsa-Umfrage: https://www.kkh.de/presse/pressemeldungen/app-auf-rezept-einfluss-von-aerzten-ist-bislang-gering.

4 Zerforschung: https://zerforschung.org/posts/datenabfluss-auf-rezept/.

5 Samsung Health (Samsung Electronics Co. Ltd.), Huawei Health (Huawei Internet Service), Menstruations-Kalender (Simple Design Ltd.), Workouts zuhause – ohne Geräte (Leap Fitness Group).

6 Berücksichtigt wurde nur die Kategorie Gesundheit & Fitness des Google Play Stores. Zur Grundlage der Downloadzahlen siehe: https://www.androidrank.org/.

7 Kalmeda (mynoise GmbH, Deutschland), Vivira (Vivira Health Lab GmbH, Deutschland), Somnio (mementor DE GmbH, Deutschland), Zanadio (aidhere GmbH, Deutschland).

8 https://de.statista.com/statistik/daten/studie/688733/umfrage/beliebteste-gesundheits-und-fitness-apps-im-google-play-store-nach-downloads-in-deutschland/.

9 Nicht berücksichtig werden Art. 14 Abs. 2 lit. f DSGVO und Art. 13 Abs. 3, 14 Abs. 4 DSGVO.

10 *Art.-29-DSG*, Leitlinien für Transparenz gemäß der Verordnung 2016/679.

11 *EDSA*, Endorsement 1/2018.

12 *EDSA*, Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them.

Merle Freye

Research Assistant and PhD Student at the Institute for Information, Health and Medical Law (IGMR), University of Bremen

E-Mail: mfreye@uni-bremen.de

2.1 Form der DSE

Nach den Leitlinien der Datenschutzgruppe soll die DSE vor dem Download bereitgestellt werden.[13] Dieses Kriterium wird anhand der Verfügbarkeit der DSE im Google Play Store nachvollzogen. Acht der zehn Apps erfüllen dieses Kriterium. In einem Fall ist eine DSE des Anbieters verlinkt, die allerdings nur die *Webseiten* des Anbieters betrifft, nicht jedoch die DiGA selbst.[14] Die DSE dieser App wird daher im Folgenden auch nicht mehr weiter untersucht. Eine andere App verlinkt keine DSE im Google Play Store. Im Folgenden wird daher die DSE analysiert, die nach der Installation in der App vorhanden ist.[15]

Der EDSA empfiehlt zudem ein (ausklappbares) Inhaltsverzeichnis am Anfang der DSE mit Überschriften und Unterüberschriften.[16] Diese Vorgabe wird nur teilweise erfüllt: Von den kommerziellen Gesundheits-Apps zeigen lediglich zwei Erklärungen ein Inhaltsverzeichnis mit Verlinkungen.[17] Während die Erklärungen der Covid19-Apps ein Inhaltsverzeichnis enthalten (jedoch ohne Verlinkung), besitzt keine DiGA-DSE ein Inhaltsverzeichnis. Weiterhin gibt die Datenschutzgruppe die klare Trennung der DSE von anderen Informationen wie z.B. Vertragsbestimmungen vor.[18] Diese Vorgabe setzen acht von neun Erklärungen um.[19] Die DSE soll außerdem innerhalb von zwei Klicks in der App aufrufbar sein.[20] Von den neun Apps erfüllen lediglich zwei dieses Kriterium.[21] Bei vier Apps war zusätzlich zu den Klicks ein Scrollen erforderlich, welches als weiterer Klick gezählt wurde, sodass diese vier Apps die Zwei-Klick-Vorgabe nicht erfüllen.[22] Mangels Testzugang zu den Apps aus dem DiGA-Bereich, konnte die Aufrufbarkeit in diesen Apps nicht untersucht werden.

Die Datenschutzgruppe stellt außerdem zahlreiche Empfehlungen zu einer sog. Mehrebenen-DSE auf.[23] Deren erste Ebene soll Einzelheiten zu den Verarbeitungszwecken, der Identität des Verantwortlichen sowie eine Beschreibung der Rechte der betroffenen Person beinhalten.[24] Allerdings erfüllt keine DSE diese Vorgabe. In Bezug auf die Änderung der DSE sieht die Datenschutzgruppe solche Verweise als unzureichend an, nach denen die betroffene Person die DSE regelmäßig auf Änderungen oder Aktualisierungen prüfen sollte.[25] Bis auf die Erklärungen der Covid19-Apps enthalten zwar alle Erklärungen einen Abschnitt zu Änderungen. Dennoch empfehlen drei Erklärungen, die jeweilige DSE regelmäßig zu prüfen und sind daher zu beanstanden.[26]

13 *Art.-29-DSG* (Fn. 10), S. 9 Rn. 11.
14 Somnio.
15 Huawei Health.
16 *EDSA* (Fn. 12), S. 22 Rn. 60.
17 Huawei Health, Workouts zuhause – ohne Geräte.
18 *Art.-29-DSG* (Fn. 10), S. 7 Rn. 8.
19 Die Vivira DSE beinhaltet zusätzlich die DSE für die entsprechende Webseite.
20 *Art.-29-DSG* (Fn. 10), S. 9 Rn. 11.
21 Menstruations-Kalender, CovPass. Berücksichtigt wurden jeweils nur die Klicks von dem Start/Home Bereich der jeweiligen App aus.
22 Huawei Health, Workouts zuhause – ohne Geräte, Samsung Health, Corona-Warn-App.
23 *Art.-29-DSG* (Fn. 10), S. 13 Rn. 17.
24 *Art.-29-DSG* (Fn. 10), S. 22 Rn. 36.
25 *Art.-29-DSG* (Fn. 10), S. 20 f. Rn. 29.
26 Huawei Health, Menstruations-Kalender, Workouts zuhause – ohne Geräte. Gleichzeitig wird angegeben, dass die Nutzer/innen per Mail oder einer Benachrichtigung in der App darüber informiert würden.

2.2 Sprache der DSE

Im Hinblick auf die Sprache empfiehlt der EDSA, dass die DSE in der Sprache verfügbar sein sollte, in der auch der Service verfügbar ist.[27] Für die Untersuchung ist Deutsch maßgeblich, allerdings sind lediglich sieben von neun Erklärungen auf Deutsch verfügbar.[28] Der EDSA befürwortet zudem eine einheitliche Wortwahl.[29] Bei der Untersuchung der Erklärungen fällt auf, dass fünf von neun Erklärungen keine einheitlichen Begriffe für die Einwilligung verwenden. Eine DSE enthält die Bezeichnungen „Zustimmung", „Genehmigung" und „Autorisierung", ohne den Begriff der Einwilligung zu erwähnen.[30] Andere Erklärungen verwenden neben der „Einwilligung" die „Zustimmung"[31] und das „Einverständnis"[32]. Zwei Erklärungen bezeichnen die Einwilligung als „agreement" und „consent".[33] Lediglich die DiGA-Erklärungen treffen eine einheitliche Wortwahl. Darüber hinaus empfiehlt der EDSA Definitionen für unbekannte oder technische Wörter oder Fachausdrücke, die als Glossar oder beim Klick auf das entsprechende Wort erscheinen.[34] Lediglich zwei von neun Erklärungen stellen einen Abschnitt mit Definitionen zur Verfügung.[35] Die Datenschutzgruppe empfiehlt weiterhin die Vermeidung von Modalverben und -wörtern wie „kann", „könnte", „manche", „oft" und „möglich".[36] Im Durchschnitt verwenden die Covid19-Apps diese Wörter am meisten,[37] gefolgt von den kommerziellen Apps[38]. Die DiGA-Erklärungen verzichten im Durchschnitt am ehesten auf die benannten Wörter.[39]

3 Informationspflichten mit Spielraum für die App-Anbieter

Die Art. 13, 14 DSGVO stellen einen umfangreichen Katalog von Informationspflichten auf. Allerdings sind nicht alle Kriterien für die vorliegende Untersuchung geeignet, da die Vorgaben teilweise zu unspezifisch sind und oft verschiedene Ansichten zum Informationsumfang vertreten werden. Dies betrifft die Information über eine verpflichtende Datenbereitstellung[40] und über eine automatisierte Entscheidung[41] sowie die Information über die Zwecke der Datenverarbeitung und über Kategorien von Empfängern und Daten.[42] Die Folge ist ein weiter Interpretations-

27 *EDSA* (Fn. 12), S. 25 Rn. 69.
28 Die Erklärungen von Workouts zuhause – ohne Geräte und Menstruations-Kalender waren ausschließlich in Englisch verlinkt.
29 *EDSA* (Fn. 12), S. 22 Rn. 60.
30 Huawei Health.
31 Samsung Health.
32 Corona-Warn-App.
33 Menstruations-Kalender, Workouts zuhause – ohne Geräte.
34 *EDSA* (Fn. 12), S. 22 Rn. 60.
35 Menstruations-Kalender, Workouts zuhause – ohne Geräte.
36 *Art.-29-DSG* (Fn. 10), S. 10 Rn. 13, in Englisch "may", "might", "some", "often" and "possible". Bei der Untersuchung wurden die Wörter „ermöglichen" und „Möglichkeit" nicht gezählt.
37 Durchschnittl. 116,5 dieser Wörter pro DSE.
38 Durchschnittl. 58 dieser Wörter pro DSE.
39 Durchschnittl. 34,33 dieser Wörter pro DSE.
40 Zur Angabe der gesetzl. Pflicht: *Franck* in Gola, DSGVO (2. Aufl. 2018), Art. 13 Rn. 25. Zur Angaben der Freiwilligkeit bei der Einwilligung *Mester* in Taeger/Gabel, DSGVO/BDSG/TTDSG (4. Aufl. 2022), Art. 13 Rn. 25; *Bäcker* in Kühling/Buchner, DSGVO/BDSG (3. Aufl. 2020), Art. 13 Rn. 49.
41 *Paal/Hennemann* in Paal/Pauly, DSGVO/BDSG (3. Aufl. 2021), Art. 13 Rn. 31a; *Schmidt-Wudy* in Wolff/Brink, BeckOK Datenschutzrecht (41. Ed. 2022), Art. 15 Rn. 78.
42 Art. 13 Abs. 1 lit. c, d,e; Abs. 2 lit. e, f DSGVO.

spielraum für die App-Anbieter, der eine Überprüfung erschwert. Ohne eine abschließende Aussage zur Umsetzung der Kriterien zu treffen, wird im Folgenden anhand der Zwecke der Datenverarbeitung und der Kategorien von Empfängern veranschaulicht, wie der Spielraum in der Praxis der DSE ausgefüllt wird.

3.1 Zwecke der Datenverarbeitung

Nach Art. 13 Abs. 1 lit. c DSGVO muss über die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, informiert werden. Vor dem Hintergrund des Verarbeitungszwecks gestaltet sich eine Form von Gesundheits-Apps besonders kontrovers: die kostenlos angebotene Gesundheits-App. Finanziert wird sie über das Anzeigen von Werbung. Oftmals ist diese Werbung auf die Interessen der Nutzer/innen angepasst und das scheinbar kostenlose Geschäftsmodell wird zum Inbegriff der Kommerzialisierung personenbezogener Daten. Im Hinblick auf die Information über diese Zwecke sollen Angaben, die unklar, generalisierend, zu allgemein oder oberflächlich formuliert sind, nicht genügen.[43] Unklar ist jedoch, wann eine Information zu allgemein oder oberflächlich ist. Dies spiegelt sich auch in den untersuchten Erklärungen wieder, die folgende Umschreibungen im Zusammenhang mit Werbung verwenden:

- „Werbung/ads/advertise(ment)“[44]
- „News, special offers and general information about other goods, services and events”[45]
- „Optimize the performance of the marketing campaigns“[46] und Teilnahme an „Marketingkampagnen“[47]
- „Marketing-Mitteilungen“[48]

Ob durchschnittliche Nutzer/innen diesen Beschreibungen entnehmen können, dass für die Werbung das eigene Verhalten ausgewertet wird, ist zweifelhaft. Eine interessenbasierte Werbung klingt lediglich versteckt an. So informiert eine DSE über die „Bereitstellung individueller Inhalte[…], die auf Ihre Interessen und die Art und Weise, wie Sie mit Samsung Health interagieren, abgestimmt sind“.[49] Zwei weitere Apps verweisen darauf, dass Produkte, Services und Werbung „of interest to you“ gezeigt würden und ein „interest-based advertising“ erfolge.[50]

Für eine DiGA ist die Datenverarbeitung zu Werbezwecken ausdrücklich verboten, § 4 Abs. 4 DiGAV, sodass eine Information über Werbung in der DSE einer DiGA eigentlich nicht vorliegen dürfte. Dennoch beinhaltet eine DSE den fragwürdigen Hinweis: „Verarbeitet die mynoise GmbH personenbezogene Daten, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht...“[51] Letztendlich verzichten lediglich vier von neun Apps auf Werbung – zumindest finden sich keine entsprechenden Informationen in den Erklärungen.

43 *Knyrim* in Ehmann/Selmayr, DSGVO (2. Aufl. 2018), Art. 13 Rn. 37.

44 Samsung Health, Menstruations-Kalender, Workouts zuhause – ohne Geräte.

45 Workouts zuhause – ohne Geräte.

46 Menstruations-Kalender, Workouts zuhause – ohne Geräte.

47 Huawei Health.

48 Samsung Health.

49 Samsung Health.

50 Menstruations-Kalender, Workouts zuhause – ohne Geräte.

51 Kalmeda.

3.2 Kategorien von Empfängern

Außerdem muss gegebenenfalls über die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten informiert werden, Art. 13 Abs. 1 lit. e DSGVO. Einigkeit besteht jedenfalls insoweit, dass der Begriff des Empfängers unstrittig auch Auftragsverarbeiter umfasst,[52] die weiteren Vorgaben zur Information sind jedoch unspezifisch. Die Datenschutzgruppe fordert „möglichst zweckdienliche“ Informationen und, dass die Angaben über die Empfängerart, die Industrie, den Sektor und Teilsektor sowie den Standort der Empfänger so genau wie möglich ausfallen sollen.[53] Zusätzlich diskutiert die Literatur, ob der Verantwortliche zwischen der Angabe einer Kategorie und der konkreten Benennung wählen darf.[54] Diese Diskussion spiegelt sich in den untersuchten Erklärungen wieder: Die Erklärungen der vier kommerziellen Apps verwenden Kategorien bzw. Überbegriffe und zwei Erklärungen geben alle Empfänger der Daten zusätzlich namentlich an.[55] Die gewählten Kategorien unterscheiden sich dabei stark.[56] Auch die Erklärungen der Covid19-Apps beschreiben die Empfänger abstrakt.[57] Im Gegensatz dazu enthalten die drei DiGA-Erklärungen keine Kategorien, sondern die Namen der Drittanbieter und eine kurze Beschreibung der Tätigkeit. Über Auftragsverarbeiter informieren drei Erklärungen abstrakt[58] und vier Erklärungen namentlich[59].

4 Informationspflichten ohne Spielraum für die App-Anbieter

Neben den Informationspflichten, die einen weitreichenden Spielraum für die App-Anbieter schaffen, sind für einige Informationspflichten hingegen konkrete Vorgaben vorhanden, anhand derer die Erklärungen untersucht werden können.

52 *Knyrim* (Fn. 43) Rn. 33; *Franck* (Fn. 40) Rn. 15; *Bäcker* (Fn. 40) Rn. 28; *Paal/Hennemann* (Fn. 41) Rn. 18.

53 Art.-29-DSG (Fn. 10), S. 47.

54 Der Streit knüpft an den Zusatz „gegebenfalls“ in Art. 13 Abs. 1 lit. b DSGVO an. Für ein eingeschränktes Wahlrecht nur bei Unkenntnis der Empfänger: *Bäcker* (Fn. 40) Rn. 30; *Mester* (Fn. 40) Rn. 15; *Schmidt-Wudy* (Fn. 41) Rn. 52; *Petri* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht (2019), Art. 13 Rn. 11; *Franck* (Fn. 40) Rn. 17; *Lorenz*, VuR 2019, 213, 216. Für ein unbeschränktes Wahlrecht: *Kamlah* in Plath, DSGVO/BDSG (3. Aufl. 2018), Art. 13 Rn. 13.

55 Menstruations-Kalender, Workouts zuhause – ohne Geräte. Dabei ist klar, dass die Aufzählung abschließend sein soll.

56 Samsung Health: Verbundene Unternehmen, Geschäftspartner, Dienstanbieter, Andere Parteien, Andere Parteien in Verbindung mit Unternehmenstransaktionen, Andere Parteien mit Ihrer Einwilligung oder auf Ihre Anweisung. Huawei Health: andere Gesundheits- und Fitness-Apps von Huawei und Drittanbietern, andere Gesundheits- und Fitness-Apps, Drittanbieter-Apps, Wetterserviceanbieter, Unsere Drittanbieter, die IT-Services (einschließlich cloudbasierter Services), Unternehmensdienstleistungen und Kundenservices bereitstellen, Unternehmen der Huawei-Gruppe oder ein anderes Unternehmen. Menstruations-Kalender: Analytics, Advertising, behavioural remarketing. Workouts zuhause – ohne Geräte: Payment, Advertising, Analytics.

57 Corona-Warn-App: Die jeweils verantwortlichen Gesundheitsbehörden, die Serversysteme der an den länderübergreifenden Warnungen teilnehmenden Corona-Apps, die jeweiligen eigenen Nutzer/innen der Serversysteme der nationalen Corona-Apps.

58 Vivira, Corona-Warn-App, Samsung Health.

59 Kalmeda, CovPass, Corona-Warn-App, Vivira.

4.1 Verantwortlicher

Gemäß Art. 13 Abs. 1 lit. a DSGVO müssen der Name und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters mitgeteilt werden. Die Datenschutzgruppe benennt beispielhaft Telefonnummer, E-Mail und Postanschrift und verweist auf das Ziel einer mühelosen Identifizierung.[60] In der Kommentarliteratur wird überwiegend die Angabe einer E-Mail-Adresse oder einer Telefonnummer gefordert.[61] Mit Blick auf Direktwerbung verlangt die Datenschutzkonferenz (DSK) eine ladungsfähige Anschrift einschließlich E-Mail-Adresse.[62] Zwar verweisen die vier Erklärungen der kommerziellen Apps ausdrücklich auf eine Datenverarbeitung zu Werbezwecken, sodass nach der DSK Anschrift und E-Mail-Adresse anzugeben sind. Dies geschieht jedoch nicht: Eine DSE nennt lediglich den Namen des Verantwortlichen[63], während eine andere DSE Namen und Adresse angibt.[64] In zwei Fällen ist lediglich eine E-Mail-Adresse zu finden.[65] Die Erklärungen der Covid19-Apps identifizieren allein das „Robert Koch-Institut (RKI)" ohne weitere Angaben als verantwortliche Stelle, was allerdings zur mühelosen Identifizierung aufgrund der Medienpräsenz des RKI während der Covid-19-Pandemie genügen dürfte. Lediglich die drei DiGA-Erklärungen stellen umfassend den Namen, die Anschrift, eine E-Mail-Adresse und in einem Fall auch eine Telefonnummer des Verantwortlichen zur Verfügung.

4.2 Rechtsgrundlage

Weiterhin muss die jeweilige Rechtsgrundlage der Datenverarbeitung benannt werden, Art. 13 Abs. 1 lit. c DSGVO. Ob es ausreicht, die Rechtsgrundlage zu wiederholen oder zu zitieren, wird unterschiedlich beantwortet.[66] Allerdings geht die Datenschutzgruppe davon aus, dass im Fall besonderer Kategorien von personenbezogenen Daten die Bestimmung des Art. 9 DSGVO und ggfs. das anwendbare Unionsrecht oder Recht des Mitgliedstaats, nach dem die Datenverarbeitung erfolgt, angegeben werden soll. Obwohl alle Erklärungen angeben, Gesundheitsdaten zu verarbeiten, nennen lediglich drei der neun Erklärungen Art. 9 DSGVO als Rechtsgrundlage.[67] Problematisch ist außerdem die Zulässigkeit der Datenverarbeitungen durch Analysedienstleister wie z.B. Google Analytics oder Matomo. An der Optimierung der Apps besteht naturgemäß ein großes Interesse seitens der App-Anbieter. Allerdings erfordert diese Optimierung eine umfangreiche Datenerhebung, deren Rechtsgrundlage nicht rechtssicher geklärt ist. Nach § 25 Abs. 1 TTDSG ist für die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder den Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, eine Einwilligung erforderlich. Auch die DSK ging 2019 davon aus, dass ein rechtmäßiger Einsatz von Google Analytics *in der Regel nur* aufgrund einer wirksamen Einwilligung der Webseitenbesuchenden möglich sei.[68] 2021 folgte der Hinweis, dass die DSK ausdrücklich keine Aussage zum Einwilligungserfordernis der sog. Reichweitenmessung treffe.[69] Selbst wenn die Einwilligung als erforderlich unterstellt wird, muss diese Einwilligung allerdings als opt-in erfolgen. Im Widerspruch dazu verweisen jedoch zwei App-Anbieter darauf, dass sie Google Analytics verwenden[70] und die Nutzer/innen diese „Google Analytics features" im Wege des opt-outs abwenden könnten.[71]

4.3 Interessenabwägung

Wenn die Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO beruht, sollen die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden, dargestellt werden. Wie detailliert die Darstellung erfolgen muss, wird aufgrund der zahlreichen individuellen Konstellationen nur abstrakt beantwortet. Die Kommentarliteratur lehnt den bloßen Verweis auf berechtigte Interessen überwiegend ab.[72] Die Datenschutzgruppe führt aus, dass aus der Unterrichtung der betroffenen Person die Möglichkeit, auf Anfrage Angaben zu der Abwägungsprüfung zu erhalten, klar hervorgehen sollte. Die Untersuchung zeigt, dass zwei Erklärungen pauschal ohne weitere Ausführungen auf „legitime interests" als Rechtsgrundlage verweisen.[73] Keine der Erklärungen, die eine Interessenabwägung beschreiben, informiert über die Möglichkeit, auf Anfrage Angaben zur Abwägungsprüfung zu erhalten.

4.4 Datenverarbeitung in Drittländern

Art. 13 Abs. 1 lit. f DSGVO enthält Informationspflichten im Zusammenhang mit der Datenübermittlung an ein Drittland. Nach der Datenschutzgruppe soll der entsprechende Artikel der DSGVO und das dazugehörige Verfahren, nach dem die Übermittlung zulässig ist, genau angegeben werden.[74] Informationen, wo und wie auf das entsprechende Dokument zugegriffen werden oder dieses erlangt werden kann, sollten ebenfalls erteilt werden.[75] „Normalerweise" sollen die Drittländer namentlich angegeben werden.[76] Gemessen an diesen Vorgaben enthalten vier Erklärungen unzureichende Informationen über die Verarbeitung im Ausland, da nicht alle Länder benannt werden.[77] Auch über die Rechtsgrundlage wird nicht[78] oder widersprüchlich[79] informiert.

60 Art.-29-DSG (Fn. 10), S. 43.

61 Zumindest wenn die E-Mail-Adresse als Kontaktmöglichkeit ohne Medienbruch gesehen wird: *Mester* (Fn. 40) Rn. 8; *Bäcker* (Fn. 40) Rn. 22; *Knyrim* (Fn. 43) Rn. 23. Alternativ zur E-Mail-Adresse verweisen auf eine Telefonnummer: *Schmidt-Wudy* (Fn. 41) Rn. 40; *Paal/Hennemann* (Fn. 41) Rn. 14.

62 *DSK*, Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO).

63 Samsung Health.

64 Huawei Health.

65 Menstruations-Kalender, Workouts zuhause – ohne Geräte.

66 *Mester* (Fn. 40) Rn. 11 fordert eine nähere Erläuterung bei komplexen Sachverhalten. Das Wiederholen bzw. Zitieren dieser Rechtsgrundlage halten folgende Autoren für ausreichend: *Paal/Hennemann* (Fn. 41) Rn. 16; *Knyrim* (Fn. 43) Rn. 38.

67 Vivira, Corona-Warn-App, CovPass.

68 *DSK*, Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich.

69 *DSK*, OH Telemedien 2021, S. 24.

70 Vivira und Zanadio verwenden u.a. den Anbieter Matomo.

71 Workouts zuhause – ohne Geräte, Menstruations-Kalender.

72 *Franck* (Fn. 40) Rn. 14; *Petri* (Fn. 54) Rn. 10; *Mester* (Fn. 40) Rn. 13; *Bäcker* (Fn. 40) Rn. 27; *Knyrim* (Fn. 43) Rn. 39.

73 Menstruations-Kalender, Workouts zuhause – ohne Geräte. Diese Erklärungen umschreiben ohne Anknüpfung an eine konkrete Datenverarbeitung die Rechtsgrundlagen des Art. 6 DSGVO. Alle anderen Apps nennen diesen Rechtfertigungsgrund entweder gar nicht (Samsung Health, Zanadio, Kalmeda, CovPass, Corona-Warn-App) oder fügen Erläuterungen bei (Huawei Health, Vivira).

74 Art.-29-DSG (Fn. 10), S. 47 f.

75 Art.-29-DSG (Fn. 10), S. 48.

76 Art.-29-DSG (Fn. 10), S. 48.

77 Samsung Health, Menstruations-Kalender, Workouts zuhause – ohne Geräte, Corona-Warn-App.

78 Samsung Health.

79 Huawei Health: „Zustimmung" der Nutzer/innen, „auch Artikel 49 (1)(b) DSGVO", „Standardvertragsklauseln der Europäischen Kommission (SCC) […]

Nach einer dieser vier Erklärungen ist die Einwilligung zur DSE die maßgebliche Rechtsgrundlage – nicht jedoch die Einwilligung in den Datentransfer.[80] Diese Angabe ist zudem bedenklich, da die App ausdrücklich Google Analytics verwendet und die Zulässigkeit der Datenverarbeitung durch Google Analytics in den USA kontrovers beurteilt wird.[81] Insbesondere der Ausnahmecharakter der in Art. 49 Abs. 1 DSGVO normierten Einwilligung ist Dreh- und Angelpunkt dieser Diskussion.[82] Selbst wenn die Einwilligung für umfangreiche Tracking Analysen durch Google Analytics zugelassen würde, liegt jedoch keine wirksame Einwilligung vor, wenn auf die unspezifische Zustimmung zur DSE abgestellt wird. Unabhängig davon informiert eine DSE als einzige DSE darüber, wie auf die unterschriebenen Standardvertragsklauseln zugegriffen werden kann. Während vier Erklärungen somit fehlerhaft sind, kommt die Untersuchung der DiGA-Erklärungen und Covid19-Apps zu einem anderen Ergebnis: Vier Apps genügen den Anforderungen.[83]

4.5 Speicherdauer

Nach Art. 13 Abs. 2 lit. a DSGVO umfasst die Information auch die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer. Die Datenschutzgruppe verweist darauf, dass eine allgemeine Aussage des Verantwortlichen, die personenbezogenen Daten würden solange wie nötig für die legitimen Zwecke der Verarbeitung gespeichert, hier nicht ausreicht.[84] Allerdings beinhalten drei Erklärungen diese unzulässige allgemeine Beschreibung.[85] Außerdem verweist eine DSE auf die gesetzliche Frist ohne nähere Angabe.[86] Es fällt auf, dass nur die Erklärungen der Covid19-Apps Kriterien und Fristen ausführlich beschreiben.

4.6 Betroffenenrechte

Der Verantwortliche muss zudem über zahlreiche Rechte der betroffenen Person informieren. Umfasst sind die Rechte auf Auskunft, Datenübertragbarkeit, Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung, Art. 13 Abs. 2 lit. b DSGVO. Außerdem soll eine Information über das Beschwerderecht bei einer Aufsichtsbehörde erfolgen, Art. 13 Abs. 2 lit. d DSGVO. Art. 13 Abs. 2 lit. c DSGVO enthält die Informationspflicht über das Bestehen des Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird. Die Datenschutzgruppe führt dazu aus, dass auch angegeben werden soll, wie die Einwilligung zurückgezogen werden kann. Fünf Erklärungen unterlaufen Fehler in der Darstellung der Betroffenenrechte.[87] In zwei Erklärungen erfolgt die Information über die Rechte, indem die jeweiligen Artikel der DSGVO angegeben wird, nicht aber indem die Rechte wörtlich beschrieben werden.[88]

5 Schlussbetrachtung

Die Untersuchung zeigt, dass keine DSE in Bezug auf alle untersuchten Merkmale überzeugt. Hinsichtlich der Pflichten der Art. 13, 14 DSGVO wurde die Information über die Betroffenenrechte insgesamt am schlechtesten umgesetzt. In einem relativen Vergleich der kommerziellen Apps zu den Apps aus dem DiGA-Bereich und den Covid19-Apps, bei dem alle geprüften Kriterien gleich stark gewichtet werden, schneiden die Erklärungen der Covid19-Apps am besten ab, gefolgt von den DiGA-Erklärungen. Die Erklärungen der kommerziellen Apps setzen die Vorgaben im Durchschnitt am schlechtesten um. Allerdings ist in Bezug auf die DiGA-Erklärungen zu erwarten, dass sich diese Wertung ändert, da ab April 2023 strengere Vorgaben für den DiGA-Bereich gelten. Einen entsprechenden Kriterienkatalog hat das BfArM im September 2022 veröffentlicht.[89]

In erster Linie müssen die App-Anbieter aktiv werden und ihre Erklärungen anpassen. Daneben sind jedoch auch spezifischere Vorgaben seitens der Aufsichtsbehörden erforderlich, da zurzeit ein großer Spielraum für die App-Anbieter besteht. Unklare Vorgaben betreffen vor allem die Informationen über die Zwecke der Datenverarbeitung, die Art der verarbeiteten Daten, die Empfänger, automatisierte Entscheidungsfindung und die Datenbereitstellungspflicht. Alarmierend ist, dass diese Aufzählung drei von sechs Informationen umfasst, die die Datenschutzgruppe[90] als Mindestinformation für eine informierte Einwilligung einordnet.[91] Wenn für die Informationen, die mindestens erforderlich sind, um eine informierte Einwilligung abgeben zu können, überwiegend keine klaren Vorgaben existieren, stellt sich die Frage, ob die Erklärungen einen wirklichen Mehrwert für die Nutzer/innen darstellen können. Letztendlich zeigt die Untersuchung aber auch, dass weder für den kommerziellen App-Bereich noch für den DiGA-Bereich ein überzeugendes Prüfverfahren existiert.

Allerdings muss jede DiGA ab dem April 2023 ein Datenschutzzertifikat vorlegen, § 139e Abs. 11 SGB V. Während das Konzept der Informationsvermittlung für den kommerziellen Bereich sowohl in Theorie und Praxis überdacht werden muss, besteht für den DiGA-Bereich somit zumindest Hoffnung auf (positive) Veränderungen.

oder die vorherige Zustimmung".

80 Workouts zuhause – ohne Geräte.

81 Für die Zulässigkeit der Einwilligung: ÖDSB m. Anm. *Messner/Mosing*, ZD 2022, 215, 219. Anders: *Stoklas*, ZD-Aktuell 2022, 01099.

82 Zum Ausnahmecharakter der Einwilligung EDSA, Leitlinien 2/2018 zu den Ausnahmen nach Art. 49 der VO 2016/679, S. 4.

83 Insbesondere die Corona-Warn-App verweist auf eine Datenverarbeitung in der Schweiz und informiert über das Vorliegen eines entsprechenden Angemessenheitsbeschlusses. Zur Datenverarbeitung im Ausland einer DiGA siehe § 4 Abs. 3 DiGAV und Nr. 38a der Anlage 1 zur DiGAV für die Datenverarbeitung ohne Angemessenheitsbeschluss.

84 *Art.-29-DSG* (Fn. 10), S. 49; zustimmend auch *Petri* (Fn. 54) Rn. 15; *Knyrim* (Fn. 43) Rn. 54.

85 Samsung Health, Menstruations-Kalender, Workouts zuhause – ohne Geräte.

86 Zanadio.

87 Samsung Health informiert lediglich über das Widerrufsrecht und die ex nunc Wirkung. Huawei Health informiert über das Beschwerderecht bei einer Aufsichtsbehörde nicht als Recht. Menstruations-Kalender und Workouts zuhause – ohne Geräte informieren weder über die ex nunc Wirksamkeit des Widerrufs noch darüber wie der Widerruf vorgenommen wird. Bei einer DiGA-Erklärung fehlt die Information über die ex nunc Wirkung des Widerrufs.

88 Nur das Beschwerderecht bei einer Aufsichtsbehörde ist in Worten beschrieben. CovPass, Corona-Warn-App.

89 *BfArM*, Prüfkriterien für die von digitalen Gesundheitsanwendungen (DiGA) und digitalen Pflegeanwendungen (DiPA) nachzuweisenden Anforderungen an den Datenschutz.

90 *Art.-29-DSG*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, S. 17 Rn. 64.

91 Zweck jedes Verarbeitungsvorgangs, die (Art der) Daten, automatisierte Entscheidungsfindung.