Mobile Apps im Gesundheitswesen: Anforderungen aus dem Datenschutz

Erarbeitet von

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.

Version 1.0

Stand der Bearbeitung: 07. November 2022

Autoren (Nennung in alphabetischer Reihenfolge)

Andrea Backer-Heuveldop	ds² Unternehmensberatung GmbH & Co. KG
Jamie Crookes	Compliant Digital GmbH & Co. KG
David Große Dütting	CURACON GmbH Wirtschaftsprüfungsgesellschaft
Mark Rüdlin	Datenschutzbeauftragter und Rechtsanwalt
Dr. Bernd Schütze	Deutsche Telekom Healthcare and Security Solutions GmbH
Gerald Spyra	Sozietät Ratajczak & Partner mbB

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

- Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Geschlechterneutrale Sprache muss im deutschen Umfeld drei Geschlechtern gerecht werden: Divers, Frauen und Männern.
- Im folgenden Text werden, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um juristische Fachbegriffe handelt, die sowohl natürliche als auch juristische Personen bezeichnen können, werden im folgenden Text nicht durch Paarformeln ersetzt. Dies gilt auch für technische Fachbegriffe, Definitionen und Zitate aus Normen (z. B. DIN EN ISO) und gesetzlichen Vorschriften. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren.
- Wo aus Gründen der leichteren Lesbarkeit bei personenbezogenen Substantiven und Pronomen nur ein Geschlecht dargestellt wurde, impliziert dies jedoch keine Benachteiligung der anderen beiden Geschlechter, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral verstanden werden.

Haftungsausschluss

- Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.
- Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.
- Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Copyright

Hinweis:

In dieser Praxishilfe wurden Texte von anderen Praxishilfen genutzt, welche ebenfalls unter der Creative Commons-Lizenz CC BY-SA 4.0 veröffentlicht wurden. Zur besseren Lesbarkeit erlaubten die Copyright-Inhaber die Nutzung der Texte mit einem zentralen Hinweis an dieser Stelle, sodass nicht an jeder Stelle darauf hingewiesen werden muss. Die genutzten Texte stammen aus den folgenden Praxishilfen:

- GMDS: Praxishilfe zur Beachtung des TTDSG im Bereich der Telemedizin. Stand: 23. April 2022. Online, zitiert am 2022-06-24; verfügbar unter https://gesundheitsdatenschutz.org/html/ttdsg.php
- GMDS, GDD: Datenschutz bei Klinischen Studien. Stand: 10. Dezember 2019. Online, zitiert am 2022-06-24; verfügbar unter https://gesundheitsdatenschutz.org/html/klin_studien.php
- GMDS, GDD, ZTG: Klinische Register und Datenschutz. Stand: 13. Dezember 2019. Online, zitiert am 2022-06-24; verfügbar unter https://gesundheitsdatenschutz.org/html/klin_register.php
- GMDS, GDD, ZTG: Leitfaden zur Erstellung eines IT-Sicherheitskonzeptes. Stand: 29. September 2017. Online, zitiert am 2022-06-24; verfügbar unter https://gesundheitsdatenschutz.org/html/itsicherheitskonzept.php

Inhaltsverzeichnis

1 Vorwort

Es werden immer mehr mobile Anwendungen („Apps“) auf dem App-Markt in den verschiedenen App-Stores angeboten, welche Gesundheitsdaten verarbeiten. Einige der angebotenen Apps dienen zur Steigerung des Wohlbefindens oder Stärkung der Resilienz (sog. „Wellness-Apps“), andere Apps dienen der Diagnostik, Therapie oder auch Vorbeugung von Krankheiten. Vielen Nutzern ist dabei oft nicht bewusst, welchen Risiken sie den dort erfassten personenbezogenen Daten aussetzen.

Untersuchungen[1] zeigten mehrfach, dass Apps grundlegende Aspekte von Datenschutz und IT-Sicherheit nicht erfüllen; dies gilt leider auch für Apps, die hochsensible Informationen wie die Gesundheitsdaten der Anwender verarbeiten.

Hersteller wie Google oder Apple bieten mit sogenannten „Software Development Kits“ (SDK) Möglichkeiten, dass man für die jeweiligen Android- oder Apple-Mobilgeräte auch ohne ausgesprochene Informatik-Kenntnisse mobile Anwendungen entwickeln kann, sodass auch hierdurch die Menge an Möglichkeiten zur Erstellung entsprechender Apps erhöht wird.

Die vorliegende Praxishilfe soll Entwicklern dabei helfen, sich in diese Thematik einzuarbeiten. Zugleich soll die Praxishilfe Datenschutzbeauftragte dabei unterstützen, Entwickler dieser Apps zu unterstützen, aber auch Apps, die in Gesundheitseinrichtungen eingesetzt werden sollen, zu prüfen[2].

Zielgruppe dieser Praxishilfe sind somit gleichermaßen

- Software-Entwickler von mobilen Apps,
- Verantwortliche, welche Apps im Gesundheitswesen einsetzen,
- Datenschutzbeauftragte, die Software-Entwickler beraten,
- Personen wie beispielsweise Auditoren, Datenschutzbeauftragte, Beschäftigte der Datenschutz-Aufsichtsbehörden oder auch des BfArM, welche für den Einsatz im Gesundheitswesen vorgesehene mobile Anwendungen auf die Einhaltung diverser Anforderungen aus dem Bereich Datenschutz und IT-Sicherheit prüfen wollen.

---

[1] So z. B.

- healthIT Answers: Healthcare Apps, Data Privacy and Security Risks. (2021-09-11) Online, zitiert am 2022-08-04; verfügbar unter https://www.healthitanswers.net/healthcare-apps-data-privacy-and-security-risks/
- tagesschau.de – Norddeutscher Rundfunk AöR: Sicherheitslücken bei Gesundheits-Apps. (2021-06-16) Online, zitiert am 2022-08-04; verfügbar unter https://www.tagesschau.de/inland/sicherheitsluecke-gesundheitsapps-101.html
  Ergänzend: Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Gesundheits-Apps (2021-06-16). Online, zitiert am 2022-08-04; verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/gesundheitsapps.html
- Heise Medien GmbH & Co. KG: IT-Sicherheit in der Medizin: 22 Krankenkassen-Apps im Sicherheits-Check. (2020-12-22). Online, zitiert am 2022-08-04; verfügbar unter https://www.heise.de/hintergrund/IT-Sicherheit-in-der-Medizin-22-Krankenkassen-Apps-im-Sicherheits-Check-4992896.html?seite=all
- Heise Medien GmbH & Co. KG: Warum Sie bei Medizin-Apps unbedingt das Kleingedruckte lesen sollten (2019-08-19). Online, zitiert am 2022-08-04; verfügbar unter https://www.heise.de/ct/artikel/Warum-Sie-bei-Medizin-Apps-unbedingt-das-Kleingedruckte-lesen-sollten-4483550.html?affiliateId=17957
- Health-Care-Com GmbH: Viele Medical Apps haben ein Datenschutzproblem (2019-03-26). Online, zitiert am 2022-08-04; verfügbar unter https://e-health-com.de/details-news/viele-medical-apps-haben-ein-datenschutzproblem/
- Arbeitsgemeinschaft der deutschen Ärztekammern – Arzneimittelkommission der deutschen Ärzteschaft (AkdÄ): Medizinische Apps: Vorsicht vor dem Einfluss kommerzieller Interessen der Hersteller (2019), in: Arzneiverordnung in der Praxis 46(1–2): 92-96. Online, zitiert am 2022-08-04; verfügbar unter https://www.akdae.de/fileadmin/user_upload/akdae/Arzneimitteltherapie/AVP/Artikel/201901-2/092.pdf

[2] Für Apps mit normalen Schutzbedarf siehe auch -BayLDA: Prüfkatalog für den technischen Datenschutz bei Apps mit normalem Schutzbedarf. Stand: 22.06.2016. Online, zitiert am 2022-06-24; verfügbar unter https://www.lda.bayern.de/media/baylda_pruefkatalog_apps.pdf

2 Einleitung

Mobile Apps stellen Softwareprodukte dar wie jegliche andere Software auch. Insbesondere gibt es keine Sonderregeln oder gar Ausnahmen für mobile Apps bzgl. Datenschutz und IT-Sicherheit, auch mobile Apps müssen allen rechtlichen und regulatorischen Anforderungen genügen. Insbesondere müssen bei der Entwicklung bzw. Programmierung von Software und somit auch von Apps die zwei in Art. 25 DS-GVO verankerten Grundsätze datenschutzkonformer Entwicklung (Datenschutz by Design) und datenschutzfreundlicher Grundeinstellung einer Anwendung (Datenschutz by Default) zwingend beachtet und umgesetzt werden: Die Werkseinstellung einer App muss den maximalen Grad von Datenschutz und IT-Sicherheit darstellen, den die App bieten kann.

Mobile Apps besitzen im Vergleich zu anderen Softwareprodukten besondere Herausforderungen, z. B.

- Regelhaft werden mobile Apps auf mobilen Endgeräten wie Tablets oder Smartphones mit dem Betriebssystem iOS oder Android betrieben. Die Hersteller dieser Betriebssysteme sind Apple bzw. Google – sofern eine Android-Version von Google auf dem Gerät eingesetzt wird, was in den meisten Fällen der Fall ist – haben weitreichenden Fernzugriff auf die Geräte, in weit höherem Ausmaß als in den Desktop-Betriebssystemen von Microsoft oder gar unter einer der Linux-Versionen. Daher müssen Softwareentwickler Mechanismen berücksichtigen, welche personenbezogene Daten ggf. auch vor Zugriff durch die Betriebssystemhersteller Apple und Google schützen.
- Insbesondere werden bei der Nutzung von Software Development Kits (SDK) der Betriebssystem-Hersteller häufig Daten wie IP-Adressen an die Hersteller der SDKs übertragen. Jedoch werden auch Daten wie IP-Adressen oftmals durch Gesundheitsdaten „infiziert“ und sind somit selbst auch als „Gesundheitsdaten“ anzusehen. Wird beispielsweise eine App zur Erinnerung an Medikamenteneinnahme eingesetzt, so ist auch die IP-Adresse als ein Gesundheitsdatum zu bewerten und entsprechend zu schützen. Insbesondere muss zur Übertragung von Daten an Hersteller der SDKs grundsätzlich ein Erlaubnistatbestand wie beispielsweise die informierte Einwilligung (im Rahmen von Gesundheitsdaten sogar die ausdrückliche informierte Einwilligung) oder eine andere gesetzliche Erlaubnisnorm vorhanden sein.
- Die Oberfläche zum Anzeigen von Informationen ist im Vergleich zu Desktop-Betriebssystemen deutlich kleiner. Daher muss dies beispielsweise hinsichtlich der Usability berücksichtigt werden, insbesondere hinsichtlich der Darstellung von Informationen, wie sie beispielsweise zur Abbildung der Informationspflichten nach Art. 13, 14 DS-GVO erforderlich sind oder die Informationen, welche bei der Einholung einer Einwilligung gegeben werden müssen.

Gesundheitsdaten gehören zu den in Art. 9 Abs. 1 DS-GVO genannten „besonderen Kategorien“ personenbezogener Daten. Eine Verarbeitung dieser Datenkategorien beinhaltet immer „erhebliche Risiken für die Grundrechte und Grundfreiheiten“ betroffener Personen (ErwGr. 51 DS-GVO), d. h. diese Daten haben immer einen hohen Schutzbedarf. Die Verarbeitung dieser besonderen Kategorien ist aufgrund des besonders hohen Schutzbedarfs in Art. 9 Abs. 1 DS-GVO grundsätzlich verboten. Nur wenn eine ausdrückliche Erlaubnis vorliegt, dürfen besondere Kategorien wie Gesundheitsdaten, genetische Daten oder auch biometrische Daten verarbeitet werden. D. h. es muss immer eine gesetzliche Erlaubnis zur Verarbeitung dieser Daten vorliegen. Dies kann beispielsweise auch die Einwilligung der betroffenen Person, deren personenbezogene Daten verarbeitet werden sollen, sein.

Werden besondere Kategorien wie Gesundheitsdaten, genetische Daten oder auch biometrische Daten aufgrund einer bestehenden Erlaubnisnorm verarbeitet, muss bei ihrer Verarbeitung dieser besonders hohe Schutzbedarf berücksichtigt und Maßnahmen zur Gewährleistung der Grundrechte

und Grundfreiheiten betroffener Personen getroffen werden, somit insbesondere die Sicherheit der Verarbeitung gewährleistet werden.

Der Begriff Gesundheitsdaten ist sehr weitreichend. In Art. 4 Ziff. 15 DS-GVO findet sich die Definition „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“. Somit werden alle entsprechenden Daten vom Begriff Gesundheitsdaten umfasst und fallen unter den hohen Schutzbedarf, also beispielsweise auch Daten, die bei Nutzung von Geräten wie Fitnesstrackern erhoben werden. Die Artikel-29-Datenschutzgruppe, die Vorgänger-Organisation des heutigen europäischen Datenschutzausschusses, unterschied schon 2015 in einem Antwortschreiben[3] an die Europäische Kommission „health data“ und „medical data“. „health data“ umfassen dabei den weiten Begriff der Gesundheitsdaten. Zu „medical data“ schrieb die Artikel-29-Datenschutzgruppe:

> „Dies ist die Kategorie der medizinischen Daten, die Kategorie der Daten über den physischen oder psychischen Gesundheitszustand einer betroffenen Person, die in einem professionellen, medizinischen Kontext erzeugt werden. Dazu gehören alle Daten im Zusammenhang mit Kontakten zu Personen und deren Diagnose und/oder Behandlung durch (professionelle) Anbieter von Gesundheitsdiensten sowie alle damit verbundenen Informationen über Krankheiten, Behinderungen, Krankengeschichte und klinische Behandlung. Dazu gehören auch alle Daten, die von Geräten oder Apps erzeugt werden, die in diesem Zusammenhang verwendet werden, unabhängig davon, ob die Geräte als "Medizinprodukte" gelten.“

Die Interpretation basiert natürlich noch auf den Begriff Gesundheitsdaten der Richtlinie 95/46/EG[4], der sich jedoch hinsichtlich der Weite der Begrifflichkeit „Gesundheitsdaten“ von der Definition in der DS-GVO nicht unterscheidet. „Medizinische Daten, wie sie beispielsweise bei Leistungserbringern wie niedergelassenen Arztpraxen, Krankenhäusern, Apotheken oder auch der häuslichen Krankenpflege anfallen, stellen somit eine Teilmenge des umfassenderen Begriffs „Gesundheitsdaten“ dar.

Entsprechend den Vorgaben der DS-GVO sind alle Gesundheitsdaten gleichermaßen vom hohen Schutzbedarf umfasst, d. h. die Datenschutzanforderungen gelten für alle „Health Apps“, insbesondere natürlich auch für „Medical Apps“. Bzgl. der IT-Sicherheit werden Daten, die bei Gesundheitsdienstleistern oder Angehörigen der Gesundheitsberufe im Sinne der Richtlinie 2011/24/EU[5] anfallen, anders behandelt, z. B. in der NIS-Richtlinie[6]. Daher können unterschiedliche Anforderungen für „Health Apps“ und „Medical Apps“ hinsichtlich IT-Sicherheit vorliegen.

---

[3] Article 29 Data Protection Working Party: Letter from the ART 29 WP to the European Commission, DG CONNECT on mHealth, 5. Februar 2015. Online, zitiert am 2022-06-24; verfügbar unter https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf
Begrifflichkeiten „health data“ und „medical data“ im Anhang „ANNEX - health data in apps and devices“ des Antwortscheibens. Online, zitiert am 2022-06-24; verfügbar unter https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

[4] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Online, zitiert am 2022-06-24; verfügbar unter, zitiert am 2022-05-25; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:31995L0046

[5] Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung. Online, zitiert am 2022-06-24; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32011L0024

[6] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der

Medizinische Apps werden in der Regel auch als Telemedien anzusehen sein. Hier ist zu beachten, dass entsprechend § 7d BSIG das Bundesamt für Sicherheit in der Informationstechnik (BSI) gegenüber Anbietern von Telemedien Anordnungen treffen können, nach denen Anbieter erforderliche technische und organisatorische Maßnahmen zur Gewährleistung der erforderlichen Sicherheit entsprechend den Vorgaben des BSI treffen müssen, wenn Telemedien aus Sicht des BSI keinen hinreichenden Schutz bieten vor

- unerlaubten Zugriffen auf die für diese Telemedienangebote genutzten technischen Einrichtungen oder
- Störungen, auch soweit sie durch äußere Angriffe bedingt sind.

Insofern muss neben den aus der DS-GVO resultierenden Anforderungen auch aus Sicht des BSIG die Implementierung einer dem Schutzbedarf entsprechenden angemessenen IT-Sicherheit jedem Hersteller und Anbieter von medizinischen Apps ein eigenes Anliegen sein.

Diese Praxishilfe soll dabei unterstützen, entsprechende Anforderungen aus Datenschutz und IT-Sicherheit bei der Anforderungsanalyse wie auch bei Implementierung und Betrieb aufzunehmen und zu berücksichtigen.

Union. Online, zitiert am 2022-06-24; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L1148

3 Abgrenzung

Für IT-Anwendungen aus dem Gesundheitsbereich gelten verschiedene Anforderungen, darunter beispielsweise:

- Ethik: Werden die Grundlagen ethischer Vorgaben entsprechend umgesetzt, insbesondere die Menschenwürde und die daraus resultierende Entscheidungsfreiheit von Menschen ausreichend berücksichtigt?
- Datenschutz: Behalten die Anwender die Hoheit über die Nutzung ihrer Gesundheitsdaten und werden die verarbeiteten Gesundheitsdaten vor einem Missbrauch geschützt?
- Nutzen[7] für den Patienten: Existiert mindestens ein konkreter gesundheitlicher oder medizinischer Nutzen für den Anwender, der das Risiko der Anwendung überwiegt?
- Evidenzbasierte Inhalte: Beruht das in die Anwendung eingeflossene Fachwissen auf empirische Belege wie beispielsweise den Leitlinien[8] der AWMF?
- Qualitätsgesichert: Wurde bei der Entwicklung qualitätsgesichert gearbeitet und entspricht die Anwendung höchsten Qualitätsansprüchen, sodass die Sicherheit der Anwender im Sinne des Produktsicherheitsgesetzes bzw. des Medizinprodukterechts bei der Anwendung gewährleistet ist?
- IT-Sicherheit: Entspricht die Anwendung dem Stand der Technik hinsichtlich der IT-Sicherheit und ist gewährleistet, dass eine Anpassung entsprechend ändernden Anforderungen des Stands der Technik über die gesamte Nutzungsdauer der Anwendung gewährleistet ist?
- Nachhaltigkeit: Ist die Pflege der Anwendung über einen entsprechend langen Zeitraum (= Dauer der Erkrankung/Therapie) auf einem dem medizinischen Anspruch entsprechendem qualitativ hohen Maß gewährleistet? Werden insbesondere ggf. neue Erkenntnisse der medizinischen Versorgung zeitnah eingepflegt?
- Zielgruppenorientiert: Wurde die Zielgruppe der Anwendung so genau beschrieben, sodass Anwender sicher entscheiden können, ob die Anwendung den eigenen Erwartungen, Fähigkeiten und möglicherweise bestehenden Einschränkungen entspricht?
- Werbung/Finanzierung: Wird klar beschrieben, wie die Anwendung finanziert wird, insbesondere ob die Anwendung Werbung als Finanzierungsquelle nutzt?

Die vorliegende Arbeit beschränkt sich auf die Beschreibung von Anforderungen aus dem Umfeld von Datenschutz und IT-Sicherheit, die bei der Entwicklung und Bereitstellung von „Medical Apps“ anzuwenden sind. Diese können, müssen aber nicht zwingend, auch für „Health Apps“ “ gelten.

Weiterhin erfolgt hier keine abschließende Darstellung. Sowohl im Umfeld der datenschutzrechtlichen Vorgaben als auch der Anforderungen aus der IT-Sicherheit wird ein risikobasierter Ansatz verfolgt. Daher sind konkrete Vorgaben nur für konkrete Verarbeitungen möglich; in dieser Praxishilfe können daher nur die wichtigsten Anforderungen vorgestellt und beispielhaft besprochen werden. Insbesondere wird in dieser Praxishilfe nicht auf datenschutzrechtliche Aspekte beim Einsatz von Software-Ökosystemen eingegangen, beispielsweise, was beim Einsatz von App-Stores zu beachten ist. Aber selbstverständlich müssen auch beim Einsatz von App-Stores ggfs. die datenschutzrechtlichen Anforderungen bzgl. Übermittlung in Drittstaaten auch zu beachten sind.

[7] Bzgl. Nutzen aus Sicht des Sozialrechts siehe z. B.

- Schweikard C.: Sozialrechtlicher Nutzen und medizinprodukterechtliche Konformität. Nomos Verlag, 2022. ISBN 978-3-8487-8171-3

[8] Arbeitsgemeinschaft der Wissenschaftlichen Medizinischen Fachgesellschaften e.V. (AWMF) e.V.: Leitlinie. Online, zitiert am 2022-09-01; verfügbar unter https://www.awmf.org/leitlinien/aktuelle-leitlinien.html

Hinsichtlich von digitalen Gesundheitsanwendungen i. S. v. § 33a SGB V existieren spezielle Vorgaben:

- Anforderungen an IT-Sicherheit sind entsprechend § 139e Abs. 10 SGB V[9] vom BSI im Einvernehmen mit dem BfArM und im Benehmen mit dem BfDI festgelegt.
- Das BfArM legt gemäß § 139e Abs. 11 SGB V[9] im Einvernehmen mit dem BfDI und im Benehmen mit dem BSI die Prüfkriterien für die nachzuweisenden Anforderungen an den Datenschutz fest.
- Anlage 1 „Fragebogen gemäß § 4 Abs. 6“ der DiGAV[10] enthält diverse Anforderungen an Datenschutz und IT-Sicherheit, deren Einhaltung rechtlich vorgeschrieben ist.

Auf Anforderungen für diese sogenannten DiGA wird in dieser Praxishilfe nicht eingegangen.

Gleiches gilt für digitale Pflegeanwendungen (DiPA) i. S. v. § 40a SGB XI, wo ebenfalls spezielle Vorgaben für Datenschutz und IT-Sicherheit vorgegeben werden:

- Entsprechend § 78a Abs. 7 SGB XI legt das BSI im Einvernehmen mit dem BfArM und im Benehmen mit dem BfDI die von DiPA zu gewährleistenden Anforderungen an die Datensicherheit fest.
- Das BfArM legt entsprechend § 78a Abs. 8 SGB XI im Einvernehmen mit dem BfDI und im Benehmen mit dem BSI die Prüfkriterien für die von DiPA-Herstellern nachzuweisenden Anforderungen an den Datenschutz fest.
- In der aktuell in Ausarbeitung befindlichen Verordnung zur Erstattungsfähigkeit digitaler Pflegeanwendungen (VdiPA), zu welcher das BMG in § 78a Abs. 6 SGB XI ermächtigt ist, werden weitergehende Anforderungen beschrieben, die voraussichtlich überwiegend den Vorgaben an eine DiGA entsprechen.[11]

D. h. die in dieser Praxishilfe dargestellten rechtlichen Anforderungen gelten zwar grundsätzlich für alle Medical Apps, speziell für DiGA und DiPA müssen Hersteller entsprechender Apps jedoch ergänzend die Erfüllung der entsprechenden Vorgaben von BfArM und BSI gewährleisten.

Auch weisen wir darauf hin, dass sich die Gesetzgebung ständig verändert. Sowohl der europäische Gesetzgeber wie auch der nationale Gesetzgeber plant jetzt schon Anpassungen oder auch neue Regelungen, die auch die Verarbeitung von Gesundheitsdaten betreffen (können). Daher muss diese Gesetzgebung im Blick behalten werden.

[9] § 139e SGB V: Verzeichnis für digitale Gesundheitsanwendungen; Verordnungsermächtigung. Online, zitiert am 2022-06-24; verfügbar unter https://www.gesetze-im-internet.de/sgb_5/__139e.html

[10] Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung - DiGAV): Anlage 1 Fragebogen gemäß § 4 Absatz 6. Online, zitiert am 2022-06-24; verfügbar unter https://www.gesetze-im-internet.de/digav/anlage_1.html

[11] Bundesministerium für Gesundheit: Referentenentwurf einer Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Pflegeanwendungen in der Sozialen Pflegeversicherung (VDiPA). Online, zitiert am 2022-07-07; verfügbar unter https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/detail/verordnung-ueber-das-verfahren-und-die-anforderungen-zur-pruefung-der-erstattungsfaehigkeit-digitaler-pflegeanwendungen-in-der-sozialen-pflegeversicherung-vdipa.html

4 Hinweise

4.1 Allgemeine Hinweise

In Art. 4 Ziff. 1 DS-GVO findet sich die Definition „eine identifizierte oder identifizierbare natürliche Person“ für die Begrifflichkeit „betroffene Personen“. Betroffene Personen sind somit beispielsweise Patienten oder auch Nutzer einer App, sodass man immer von betroffenen Personen sprechen könnte. Jedoch werden in verschiedenen Gesetzestexten ausdrücklich bestimmte Formulierungen genutzt, daher wird auch in dieser Praxishilfe nicht überall von „betroffener Person“ gesprochen, sondern im Kontext des TTDSG beispielsweise von Nutzern gesprochen. Leser dieser Praxishilfe sollten jedoch berücksichtigen, dass „betroffene Person“ der umfassendere Begriff ist und die DS-GVO für alle Betroffenenkreise (d. h. betroffener Personen jeglicher Art und Kategorie) die gleichen Rechte vorsieht.

4.2 Deutsches oder europäisches Recht?

Die DS-GVO ist grundsätzlich und vorrangig anzuwendendes Recht. Gerade im Bereich der Verarbeitung von Gesundheitsdaten, genetischen Daten und biometrischen Daten ist ergänzend jedoch das jeweilige geltende nationale Recht anzuwenden. § 1 Abs. 5 BDSG enthält die Regelung, dass das BDSG jeweils dort nicht anzuwenden ist, wenn Recht der Europäischen Union und insbesondere die DS-GVO unmittelbar gilt, was jedoch regelhaft bei der Verarbeitung von Daten von Personen, die sich in Deutschland aufhalten und somit die Verarbeitung der Daten in dem sich somit in Deutschland befindlichem Handy ebenfalls in Deutschland erfolgt, nicht gegeben sein wird. Daher gelten grundsätzlich die Vorgaben der DS-GVO, ergänzend die datenschutzrechtlichen Vorgaben aus dem deutschen Recht.

4.3 Hinweise bzgl. Anforderungsdarstellung

Bei der Darstellung der Anforderungen in dieser Praxishilfe werden sog. „Muss-, Soll-, Kann- und Darf-Vorschriften“[12] verwendet, wodurch die unterschiedlichen Grade an den Befolgungsanspruch der jeweiligen Anforderungen aus Sicht der Autoren dargestellt werden. Im Einzelnen gelten folgende Entsprechungen:

MUSS / MÜSSEN	Die Anforderung ist zwingend, d. h. in jedem Fall einzuhalten
SOLL / SOLLTEN	Die Anwendung muss eine bestimmte Funktion/Eigenschaft aufweisen, außer es wird dargelegt, dass durch ein Nicht-Umsetzen der Anforderung kein Risiko für den Nutzer der Anwendung sowie für den sicheren Betrieb der Anwendung besteht, bzw. eine Umsetzung, aufgrund von technischen Einschränkungen, derzeit nicht möglich ist.
KANN /KÖNNEN	Die Anwendung kann eine bestimmte Funktion/Eigenschaft aufweisen, wobei eine Implementierung der Funktion/Eigenschaft vom Hersteller bzw. Betreiber der Anwendung dem Nutzer anzuzeigen ist.
DARF / DÜRFEN NICHT	Die Anwendung darf die entsprechende Funktion/ Eigenschaft unter keinen Umständen aufweisen.

[12] angelehnt an RFC 2119: Key words for use in RFCs to Indicate Requirement Levels. Online, zitiert am 2022-09-29; verfügbar unter https://www.rfc-editor.org/rfc/rfc2119

Dabei gilt der Grundsatz: Nicht jede Anforderung muss immer erfüllt werden.

> Beispiel 1: Ein Vertrag zur Verarbeitung im Auftrag ist nur abzuschließen, wenn auch tatsächlich eine Auftragsverarbeitung vorliegt. Aber *wenn* eine Auftragsverarbeitung vorliegt und die Anforderung lautet „Vertrag MUSS vorliegen“, so muss die Anforderung erfüllt werden. Liegt hingegen keine Auftragsverarbeitung vor, sondern beispielsweise eine „gemeinsame Verantwortlichkeit“ entsprechend Art. 26 DS-GVO, so muss trotz entsprechender „Muss“-Anforderung selbstverständlich kein Vertrag zur Verarbeitung im Auftrag abgeschlossen werden.

5 Begriffsbestimmungen

Es gelten grundsätzlich die Begriffsbestimmungen der jeweiligen Gesetze bzw. Verordnungen, insbesondere die Vorgaben der DS-GVO. Einige Begrifflichkeiten sind jedoch nicht gesetzlich bestimmt, es existiert keine sogenannte „Legaldefinition“. Für einige dieser Begriffe wird nachfolgend dargestellt, wie diese Begriffe im Kontext dieser Praxishilfe verwendet werden.

Insbesondere für Gesundheit-Apps gibt es keine einheitliche Klassifikation. Juristisch kann man vier Kategorien darstellen:

1) Gesundheits-Apps als Medizinprodukte
2) Digitale Gesundheitsanwendungen i. S. d. § 33a SGB V, sogenannte „DiGA“, die immer auch ein Medizinprodukt der Medizinprodukte-Klasse I oder IIa sein müssen
3) Digitale Pflegeanwendungen i. S. d. § 40a SGB XI, sogenannte „DiPA“
4) Alle anderen Gesundheits-Apps.

Diese Unterteilung erscheint aus Sicht von Datenschutz und IT-Sicherheit nicht zielführend, da beispielsweise die Angabe „Medizinprodukt“ nichts über den Schutzbedarf der hierbei verarbeiteten personenbezogenen Daten aussagt. Auch ist die Sammelkategorie „Alle anderen“ unzureichend, da hier Apps, die personenbezogene Daten mit sehr unterschiedlichem Schutzbedarf verarbeiten wie beispielsweise Fitness- und Wellness-Apps und Apps zur Optimierung der Diabetes-Therapie z. B. in Form eines elektronischen Tagebuches, nicht differenziert werden.

Zielführender erscheint der Ansatz der Artikel-29-Datenschutzgupppe, der Vorgänger-Organisation des heutigen europäischen Datenschutz-Ausschusses, die zwischen „health data“ als Oberbegriff für alle Gesundheitsdaten und „medical data“ als Teilmenge von health data unterschieden, wobei medical data ausschließlich Daten der medizinischen Versorgung beinhalten, d. h. es handelt sich um Patientendaten, die von einem health professional verarbeitet werden. Entsprechend wird in dieser Arbeit zwischen „Health Apps“ als Oberbegriff und „Medical Apps“ als Untergruppe von Health Apps unterschieden.[13]

5.1 Apps

Der Begriff „App“ ist die Abkürzung des englischen Begriffs Application Software, also einer Anwendungssoftware. In der Rechtsprechung[14] wird unter einer App ein Anwendungsprogramm für Mobilgeräte verstanden, im Kontext dieser Praxishilfe wird der Begriff App für Software genutzt, welche auf Smartphones und Tablets eingesetzt wird.[15]

Bei Apps wird grundlegend zwischen drei Arten von Apps unterschieden:[16]

---

[13] Das Deutschen Netzwerkes Versorgungsforschung eV (DNVF) unterteilt in ihrem 2019 veröffentlichten Memorandum „Gesundheits- und Medizin-Apps (GuMAs)“ in die Kategorien „Gesundheits-Apps“, „Medizin-Apps“ und „Medizin-Apps als Medizinprodukte“. Online, zitiert am 2022-09-01; verfügbar unter https://www.thieme-connect.com/products/ejournals/abstract/10.1055/s-0038-1667451

[14] BGH, Urt. v. 28.01.2016 Az. I ZR 202/1, Rn. 19. Online, zitiert am 2022-09-01; verfügbar unter https://openjur.de/u/892184.html

[15] Siehe z. B. auch

- Ewald K.: Kap. 32.7 Erstellung und Vertrieb von Mobile Apps, Rn. 1: "Apps sind die kleinen Programme, mit denen insbesondere Smartphones und Tablets um zusätzliche Funktionen erweitert werden können. Mehr und mehr halten Apps auch auf weiteren Gerätetypen Einzug, darunter Wearables oder Smart Devices wie Uhren, Brillen, Armbänder." In: Taeger J. /Pohle J. (Hrsg.) Computerrechts-Handbuch. C. H. Beck Verlag, 36. Auflage 2021. ISBN 978-3-406-31830-6
- Schmidt M, Pruß M.: § 3 Technische Grundlagen des Internets, Rn. 238: "Obwohl sich der Begriff App auf jegliche Art von Anwendungssoftware bezieht, wird er im deutschen Sprachraum oft mit Anwendungssoftware für Smartphones und Tablets gleichgesetzt." In: Auer-Reinsdorff A. /Conrad I. Handbuch IT- und Datenschutzrecht. C. H. Beck Verlag, 3. Auflage 2019.ISBN 978-3-406-72177-9

[16] Steinmetz R.: Apps im Lauterkeitsrecht, S. 35ff. Nomos Verlag, 1. Auflage 2017. ISBN 978-3-8487-4635-4

a) Native-Apps: Hierbei handelt es sich um Apps, die speziell für eine Plattform entwickelt werden, also z. B. für Android. Die App wird direkt auf dem Gerät installiert und ist eng an das Betriebssystem gebunden.
b) Web-Apps: Web-Apps werden über einen Web-Browser des jeweiligen Gerätes aufgerufen und ausgeführt. I. d. R. erfolgt hierbei eine Darstellung der Webseite in der vollständigen Größe des Bildschirms in einer für das jeweilige Gerät optimierten Weise. Web-Apps sind nicht an eine bestimme Plattform gebunden, sondern können unter allen Betriebssystemen gleichermaßen verwendet werden.
c) Hybrid-Apps: Eine Hybrid-App zeigt die Inhalte einer Web-App innerhalb des Rahmens einer Native-App an, d. h. es sollen die Vorteile von Native-Apps und Web-Apps kombiniert werden, in dem über die Native-App auf die Hardware des Gerätes zugegriffen werden kann, der Großteil der Funktionalität jedoch plattformunabhängig entwickelt werden kann.

Hinsichtlich der Anforderungen von Datenschutz und IT-Sicherheit ist festzuhalten, dass die Art einer App für die Erfüllung der Anforderungen ist: Jede App muss alle auf sie zutreffenden Anforderungen erfüllen.

5.2 Health Apps

Unter Health Apps werden in dieser Praxishilfe alle Softwareanwendungen verstanden, bei denen Gesundheitsdaten im Sinne der Definition von Art. 4 Ziff. 15 DS-GVO in einer App verarbeitet werden.[17] Dies umfasst sowohl Apps, welche der Primärprävention dienen (z. B. Wellness- bzw. Fitness-Apps), wie auch alle im Rahmen der Patientenversorgung eingesetzten Apps.

5.3 Medical Apps

Medical Apps stellen im Rahmen der Verwendung in dieser Praxishilfe eine Untergruppe von Health Apps dar. Auch bei Medical Apps werden Gesundheitsdaten im Sinne der Definition von Art. 4 Ziff. 15 DS-GVO verarbeitet, aber nur Daten, welche in einem professionellen, medizinischen Kontext verarbeitet werden.

In diese Kategorie von Medical Apps gehören insbesondere auch die oben angesprochenen DiGA- und DiPA-Anwendungen[18] im Sinne der Regelung im jeweiligen Sozialgesetzbuch.

5.4 Gesundheitsdaten

Gesundheitsdaten werden in Art. 4 Ziff. 15 DS-GVO gesetzlich definiert: Gesundheitsdaten sind entsprechend der gesetzlichen Definition alle personenbezogenen Daten, die

- sich auf die körperliche oder geistige Gesundheit einer natürlichen Person,
- einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und
- aus denen Informationen über deren Gesundheitszustand hervorgehen.

Entsprechend ErwGr. 35 DS-GVO kann sich dies auf den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person beziehen.

Diese Definition ist sehr umfassend, da die Definition alle Informationen, die sich auf die Gesundheit einer Person unter allen Aspekten – körperlichen wie psychischen – beziehen, umfasst. Ist auf einem Foto beispielsweise eine Person mit Brille zu sehen, kann es sich bei diesem Foto bereits um ein

[17] So z. B. auch zu finden in: Kremer S.: § 28 Apps und Social Media, Rn. 67: "Health Apps sind Apps mit Bezug zur Gesundheit des Anwenders." In: Auer-Reinsdorff A. /Conrad I. Handbuch IT- und Datenschutzrecht. C. H. Beck Verlag, 3. Auflage 2019. ISBN 978-3-406-72177-9

[18] Zur Subsidiarität zwischen DiGA und DiPA siehe z. B.

- Kommentierung in Dittrich T. (2021) Digitalisierung in ambulanter und stationärer Pflege – Digitale Gesundheitsanwendungen und Pflegeanwendungen (Teil 1). SRa: 275-281, speziell Susidarität S. 279

Gesundheitsdatum handeln.[19] Auch Prognosen, Wahrscheinlichkeitsaussagen wie auch alle anderen Vermutungen können ein Gesundheitsdatum darstellen, z. B. wenn aufgrund familiärer Erkrankungen Aussagen über eine Person getroffen werden.[20] Ebenfalls sind Terminvereinbarungen mit einem Gesundheitsdienstleister wie beispielsweise Ärzten oder Physiotherapeuten als Gesundheitsdatum zu klassifizieren.[21]

Insbesondere handelt es sich auch bei Daten wie Puls, Blutdruck usw., welche von Fitness-Apps oder anderen Geräten gemessen, d. h. verarbeitet werden, um Gesundheitsdaten.

5.5 Stand der Technik

„Stand der Technik“ ist ein unbestimmter, abstrakt-genereller Begriff, der auf den jeweils aktuellen Erkenntnisstand der Technik und Wissenschaft verweist. Die Anforderung hinsichtlich „Stand der Technik“ beschreibt in allgemeiner Form Verfahren und Methoden, die es nach Einschätzung der Fachwelt als gesichert erscheinen lassen, ein vorgegebenes Ziel hinreichend sicher zu erreichen.

Um der Anforderung, eine Verarbeitung entsprechend dem Stand der Technik zu entwickeln und zu betreiben, zu genügen, müssen die verwendeten Maßnahmen die fortgeschrittenen Verfahren der technischen Entwicklung abbilden, jedoch nicht über den Stand erprobter Verfahren hinausgehen.

Stand der Technik ist dabei als dynamische Anforderung zu verstehen. D. h. es werden nicht einmal Maßnahmen ergriffen, sondern für die gesamte Zeitdauer der Verwendung einer App muss die Anforderung bzgl. Stand der Technik eingehalten werden. Somit muss von Zeit zu Zeit geprüft werden, ob Änderungen bei den fortgeschrittenen technischen Verfahren eine Anpassung der getroffenen (Schutz-)Maßnahmen erfordern.

In der Begründung zum IT-Sicherheitsgesetz[22] findet sich bezüglich des Terminus „Stand der Technik“:

> „Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden.“

Somit kann der Stand der Technik durch Normen und Richtlinien abgebildet werden, wenn diese die fortgeschrittenen Verfahren der technischen Entwicklung abbilden. Insbesondere Normen stellen nicht zwangsläufig den Stand der Technik dar. Vielmehr ist eine Norm dann anerkannt, wenn Fachleute diese anwenden und sich dabei sicher sind, dass sie dem Stand der Technik entspricht. Dies beinhaltet, dass die Norm „gepflegt“ wird, d. h. regelmäßig aktuell gehalten wird; eine deutlich ältere Norm wird gerade im Bereich der IT-Sicherheit eher selten den Stand der Technik abbilden, da innerhalb der IT in

[19] Ernst S.: Art. 4 DS-GVO XV. Gesundheitsdaten (Nr. 15), Rn. 109. In. Paal/Pauly (Hrsg.) Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG. C. H. Beck Verlag, 3. Auflage. 2021. ISBN 978-3-406-75374-9

[20] Ernst S.: Art. 4 DS-GVO XV. Gesundheitsdaten (Nr. 15), Rn. 119. In. Paal/Pauly (Hrsg.) Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG. C. H. Beck Verlag, 3. Auflage. 2021. ISBN 978-3-406-75374-9

[21] Schild H.: Art. 4 DS-GVO, Rn. 142. In: Wolff/Brink (Hrsg.) BeckOK Datenschutzrecht, 40. Edition, Stand: 01.05.2022

[22] Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). S. 14, 15. Online, zitiert am 2022-08-18; verfügbar unter https://dip21.bundestag.de/dip21/btd/18/040/1804096.pdf

relativ kurzen Abständen deutliche technische Veränderungen auftreten können. D. h. es obliegt denjenigen, die Apps entwickeln und auf dem Markt anbieten, sich entsprechend zu informieren und für die Einhaltung des Stands der Technik Sorge zu tragen.

Das BSI veröffentlichte speziell für Gesundheits-Apps[23] technische Richtlinien hinsichtlich zu erfüllender Sicherheitsanforderungen:[24]

- TR-03161 Anforderungen an Anwendungen im Gesundheitswesen - Teil 1: Mobile Anwendungen. Version 2.0, Stand 18. Mai 2922.
  URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03161/BSI-TR-03161-1.pdf?__blob=publicationFile&v=11
- TR-03161 Anforderungen an Anwendungen im Gesundheitswesen - Teil 2: Web-Anwendungen. Version 1.0, Stand 18. Mai 2022.
  URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03161/BSI-TR-03161-2.pdf?__blob=publicationFile&v=8
- TR-03161 Anforderungen an Anwendungen im Gesundheitswesen - Teil 3: Hintergrundsysteme. Version 1.0, Stand 18. Mai 2022
  URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03161/BSI-TR-03161-3.pdf?__blob=publicationFile&v=7

[23] Bundesamt für Sicherheit in der Informationstechnik: BSI veröffentlicht Sicherheitsanforderungen für Gesundheits-Apps, Presseerklärung vom 15. April 2020. Online, zitiert am 2022-08-18; verfügbar unter https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/TR-Gesundheitsapps_150420.html

[24] Bundesamt für Sicherheit in der Informationstechnik: BSI TR-03161 Anforderungen an Anwendungen im Gesundheitswesen. Online, zitiert am 2022-08-18; verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03161/tr03161_node.html

6 Digitale-Inhalte-Richtlinie und die daraus resultierende Update-Pflicht

Der deutsche Gesetzgeber setzte die europäische Digitale-Inhalte-Richtlinie[25] durch neu eingefügte Regelungen im BGB um. Die Richtlinie und ebenso die deutsche Umsetzung adressiert Verträge, auf deren Grundlage ein Unternehmer dem Verbraucher digitale Inhalte oder digitale Dienstleistungen bereitstellt oder deren Bereitstellung zusagt und der Unternehmer dafür eine Bezahlung erhält bzw. eine Bezahlung zugesagt wird.

Medical Apps sprechen Patienten an, es handelt sich daher bei Verträgen zwischen App-Anbietern und Patienten um entsprechende „Verbraucherverträge über digitale Produkte“ nach §§ 327ff BGB, sofern die digitale Dienstleistung gegen Zahlung eines Preises erfolgt; Letzteres kann beispielsweise auch in Form von digitalen Werten wie beispielsweise sog. „Likes“ bei Social-Media-Accounts[26] erfolgen. Dabei kann der Preis selbst auch von einem Dritten für den Verbraucher gezahlt werden, z. B. kann eine Krankenkasse für einen Patienten den Preis entrichten.

Gemäß § 327 Abs. 3 BGB sind die Vorgaben auch in den Fällen anzuwenden, wenn ein Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder sich zu deren Bereitstellung verpflichtet („sog. Handeln oder Zahlen mit Daten). Um in den Anwendungsbereich der rechtlichen Regelung zu kommen, reicht es ggf. bereits aus, dass der Verbraucher bei der Eröffnung eines Kontos seine Einwilligung zur Verwendung von personenbezogenen Daten erteilt, die er im Rahmen der Nutzung des digitalen Produkts möglicherweise später hochlädt oder erzeugt (siehe ErwGr. 24 RL (EU) 2019/770). Die Menge der bereitgestellten Daten ist für den Eintritt in den Geltungsbereich des Verbrauchervertrages über digitale Produkte unerheblich. Laut ErwGr. 24 RL (EU) 2019/770 kann es ausreichen, wenn ein Verbraucher einem Unternehmer Namen und E-Mail-Adresse bereitstellt, die „nicht ausschließlich zur Bereitstellung der digitalen Inhalte oder digitalen Dienstleistungen oder zur Erfüllung rechtlicher Anforderungen verwendet werden“.[25]

Zu beachten ist weiterhin, dass es dem Wortlaut von § 327 Abs. 3 BGB nach unerheblich ist, ob der Verbraucher sich zunächst nur zur Bereitstellung der Daten verpflichtet, diese Bereitstellung in der Folge jedoch unterbleibt, z. B. weil die Einwilligung widerrufen wird. Entsprechend § 327 Abs. 3 BGB genügt bereits die Verpflichtung, um den Anwendungsbereich eines Verbrauchervertrages über die Bereitstellung digitaler Produkte zu eröffnen und die daraus resultierenden Rechte und Pflichten in Wirkung zu bringen.[27] Ggf. sollte ein Unternehmer daher bei Verbraucherverträgen, welche eine Bereitstellung von Daten als Gegenleistung des Verbrauchers beinhalten, an eine Kündigungsklausel im Vertrag denken, wenn die Bereitstellung nicht mehr erfolgt bzw. nicht mehr möglich ist.

Ein Unternehmer, der sich gemäß den §§ 327, 327a BGB zur Bereitstellung eines digitalen Produkts wie eine Medical App verpflichtet hat, muss dieses Produkt entsprechend den Vorgaben von § 327d BGB frei von Produkt- und Rechtsmängeln bereitzustellen. Gemäß § 327e Abs. 3 Ziff. 3 BGB kann fehlende IT-Sicherheit einen Produktmangel darstellen. Der Begriff der Sicherheit ist weit zu verstehen. In Deutschland wird man den Begriff Sicherheit durch die Begriffsbestimmung in § 2 Abs. 2 BSI-Gesetz eingrenzen und unter Sicherheit die „Einhaltung bestimmter Sicherheitsstandards, die die

[25] 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. Online, zitiert am 2022-07-22; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32019L0770

[26] Fries M.: § 327 Rn. 16. In: Gsell/Krüger/Lorenz/Reymann (Hrsg.) beck-online.GROSSKOMMENTAR – BGB. Stand: 01.04.2022

[27] Metzger A.: § 327 Rn. 16. In: Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB, Band 3: Schuldrecht – Allgemeiner Teil II. C. H. Beck Verlag, 9. Auflage. 2022. ISBN 978-3-406-76673-2

Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen“ verstehen.

Der Aspekt der Sicherheit umfasst somit einerseits den Schutz des digitalen Produktes, also der App, vor einer unerwünschten Veränderung, andererseits aber auch den Schutz der personenbezogenen Daten der Verbraucher. Beides muss durch die Einhaltung entsprechender Sicherheitsstandards gewährleistet werden.[28] Dabei ist gerade im mobilen Umfeld zu beachten, dass Daten in verschiedenen Kontexten verarbeitet werden:[29]

- Data at Rest: Daten, die auf dem Mobilgerät oder Server gespeichert werden,
- Data in Transit: Daten, die übermittelt werden und
- Data in Use: Daten, die gerade von der App bearbeitet werden.

Die Sicherheit der Daten muss entsprechend § 327d BGB grundsätzlich in jedem der drei Zustände gewährleistet sein.

§ 327f Abs. 1 BGB schreibt vor, dass Verbrauchern für den vertragsgemäßen Nutzungszeitraum Aktualisierungen, welche „für den Erhalt der Vertragsmäßigkeit des digitalen Produkts erforderlich sind“, bereitgestellt und die Verbraucher über diese Aktualisierungen informiert werden. Unter einer Aktualisierung versteht der Gesetzgeber dabei eine Änderung des digitalen Produkts mit dem Ziel:[30]

a) einer Verbesserung gegenüber der bisherigen Version,
b) einer Verbesserung der Produktsicherheit,
c) einer Verbesserung der Kompatibilität und/oder
d) einer Verbesserung der Interoperabilität.

Grundsätzlich fallen also Updates, Patches, Bugfixes usw. unter den Begriff einer Aktualisierung i. S. d. § 327f BGB. Aber auch wenn eine Aktualisierung ausschließlich zusätzliche Funktionen beinhaltet, also das digitale Produkt über den Stand bei Vertragsschluss ergänzt, (sog. „Upgrade“), fällt dies unter den in § 327f BGB enthaltenen Begriff einer Aktualisierung.[31]

Hinweis 1: Eine Untersuchung der Queen’s University[32] aus dem Jahr 2017 fand heraus, dass heute oftmals bis zu 80% der Anwendungen aus externem Code bestehen, wobei diese Bibliotheken die gleichen Rechte wie die Anwendung, die sie verwendet, selbst haben (müssen), sodass diese externen Bibliotheken auf Daten zugreifen, diese verändern oder auch an Adressen im Internet senden können. Daher ist zu beachten: Diese Pflicht zur Aktualisierung besteht für die gesamte Anwendung. Beinhaltet die Anwendung von Dritten bereitgestellte Softwarebibliotheken, Frameworks oder ähnliche Softwareprodukte, so gilt diese Pflicht selbstverständlich auch für diese

[28] Fries M.: § 327e Rn. 28. In: Gsell/Krüger/Lorenz/Reymann (Hrsg.) beck-online. GROSSKOMMENTAR – BGB. Stand: 01.04.2022

[29] Barton T, Müller C, Seel C (Hrsg) (2016) Mobile Anwendungen in Unternehmen: Konzepte und betriebliche Einsatzszenarien, Kap. 10.1 „Sicherheit mobiler Anwendungen“. Springer Verlag, 2016. ISBN 978-3658120092

[30] Fries M.: § 327f Rn. 9. In: Gsell/Krüger/Lorenz/Reymann (Hrsg.) beck-online.GROSSKOMMENTAR – BGB. Stand: 01.04.2022

[31] So z. B.

- Metzger A.: § 327 Rn. 16. In: Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB, Band 3: Schuldrecht – Allgemeiner Teil II. C. H. Beck Verlag, 9. Auflage. 2022. ISBN 978-3-406-76673-2
- Fries M.: § 327f Rn. 15-17. In: Gsell/Krüger/Lorenz/Reymann (Hrsg.) beck-online.GROSSKOMMENTAR – BGB. Stand: 01.04.2022

[32] Queen's University Belfast: „Vulnerability Detection in Open Source Software: The Cure and the Cause“. Online, zitiert am 2022-09-15; verfügbar unter https://pure.qub.ac.uk/en/publications/vulnerability-detection-in-open-source-software-the-cure-and-the- bzw. pdf-Datei unter https://pureadmin.qub.ac.uk/ws/portalfiles/portal/128394396/SMillar_13616005_VulnerabilityDetectionInOSS.pdf

Bestandteile der App.[33] Insbesondere muss auch für diese Produktbestandteile bei bekannt gewordenen Sicherheitslücken Updates zur Behebung dieser Sicherheitslücken bereitgestellt werden. Daher ist zu raten, dass nur von Dritten bereitgestellte Softwarebibliotheken, Frameworks oder ähnliche Softwareprodukte eingesetzt werden, bei denen eine entsprechend zeitnahe Bereitstellung von Sicherheitsupdates sichergestellt ist – idealerweise eine vertragliche Zusicherung hinsichtlich der Bereitstellung von Sicherheitsupdates besteht.

Nach § 327f Abs. 1 S. 1 BGB muss eine Aktualisierung für den Erhalt der Vertragsmäßigkeit des Produkts erforderlich sein, damit die Pflicht zur Bereitstellung eintritt; bei einem Upgrade wird daher regelhaft keine Pflicht der Bereitstellung vorliegen. Anders sieht es bei Vorliegen von Schwachstellen im Bereich der IT-Sicherheit aus. Ist die Sicherheit der digitalen Anwendung oder sogar die personenbezogenen Daten gefährdet, besteht nach § 327f Abs. 1 BGB die Pflicht einer Aktualisierung in Form einer Sicherheitsaktualisierung, welche die Gefährdung beseitigt. Diese Pflicht besteht für den gesamten Bereitstellungszeitraum der App (§ 327f Abs. 1 Ziff. 1 BGB) bzw. für den Zeitraum, den der Verbraucher aufgrund der Art und des Zwecks des digitalen Produkts und unter Berücksichtigung der Umstände und der Art des Vertrags erwarten kann (§ 327f Abs. 1 Ziff. 1 BGB). Letzteres umfasst wohl den Zeitraum der Vertriebsdauer eines Produkts, aber insbesondere unter den Aspekten der Nachhaltigkeit und Klimaschutzes wird ein Verbraucher ggf. erwarten können, dass fehlende Updates nicht zu einer Ersetzung eines im Übrigen noch funktionstauglichen Produkts führen.[34]

ErwGr. 47 RL (EU) 2019/770 sieht insbesondere bei Sicherheitsaktualisierungen die Notwendigkeit einer großzügigen Auslegung des Zeitraums, in welchem Sicherheitsaktualisierungen bereitgestellt werden sollten, vor: [25]

„Während des Zeitraums, den der Verbraucher vernünftigerweise erwarten würde, sollte der Unternehmer dem Verbraucher Aktualisierungen, einschließlich Sicherheitsaktualisierungen, bereitstellen, damit die digitalen Inhalte oder digitalen Dienstleistungen in vertragsgemäßem Zustand bleiben und sicher bleiben.

So sollte beispielsweise in Bezug auf digitale Inhalte oder digitale Dienstleistungen,

deren Zweck zeitlich begrenzt ist, die Verpflichtung zur Bereitstellung von Aktualisierungen auf diesen begrenzten Zeitraum beschränkt sein,

während bei anderen Arten digitaler Inhalte oder digitaler Dienstleistungen der Zeitraum, in welchem dem Verbraucher Aktualisierungen bereitgestellt werden sollten, dem Gewährleistungszeitraum für Vertragswidrigkeit entsprechen könnte

oder über diesen Zeitraum hinausgehen könnte, was insbesondere bei Sicherheitsaktualisierungen der Fall sein könnte."

[33] Daher sollte, um eine Übersicht über die eingesetzten Fremd-Code-Anteile zu behalten, eine „Software Bill of Materials" (SBOM, siehe z. B. https://www.cisa.gov/sbom) genutzt und gepflegt werden, z. B. unter Nutzung der Open-Source Software CycloneDX von OWASP (https://cyclonedx.org/)

[34] Fries M.: § 327f Rn. 15-17. In: Gsell/Krüger/Lorenz/Reymann (Hrsg.) beck-online. GROSSKOMMENTAR – BGB. Stand: 01.04.2022

7 Medizinprodukt

Seit 26. Mai 2021 ist die europäische Medizinprodukteverordnung[35] in Wirkung, d. h. ihre Regelungen sind unmittelbar anwendbares Recht innerhalb der EU, natürlich auch in Deutschland. Art. 2 Ziff. 1 der Verordnung (EU) 2017/745 enthält die Begriffsbestimmung für Medizinprodukte:

> „Medizinprodukt“ bezeichnet ein Instrument, einen Apparat, ein Gerät, eine Software, ein Implantat, ein Reagenz, ein Material oder einen anderen Gegenstand, das dem Hersteller zufolge für Menschen bestimmt ist und allein oder in Kombination einen oder mehrere der folgenden spezifischen medizinischen Zwecke erfüllen soll:
>
> - Diagnose, Verhütung, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten,
> - Diagnose, Überwachung, Behandlung, Linderung von oder Kompensierung von Verletzungen oder Behinderungen,
> - Untersuchung, Ersatz oder Veränderung der Anatomie oder eines physiologischen oder pathologischen Vorgangs oder Zustands,
> - Gewinnung von Informationen durch die In-vitro-Untersuchung von aus dem menschlichen Körper — auch aus Organ-, Blut- und Gewebespenden — stammenden Proben
>
> und dessen bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische oder immunologische Mittel noch metabolisch erreicht wird, dessen Wirkungsweise aber durch solche Mittel unterstützt werden kann.
>
> Die folgenden Produkte gelten ebenfalls als Medizinprodukte:
>
> - Produkte zur Empfängnisverhütung oder -förderung,
> - Produkte, die speziell für die Reinigung, Desinfektion oder Sterilisation der in Artikel 1 Absatz 4 genannten Produkte und der in Absatz 1 dieses Spiegelstrichs genannten Produkte bestimmt sind.

Es liegt daher **nicht im Ermessen eines Herstellers oder Händlers**, ***ob*** ein **Softwareprodukt ein Medizinprodukt darstellt oder nicht**: Trifft die Begriffsdefinition zu, so handelt es sich bei der Anwendung bzw. der Mobile App um ein Medizinprodukt.

Die entsprechend Art. 103 Verordnung (EU) 2017/745 eingerichtete „Koordinierungsgruppe Medizinprodukte“ (Medical Device Coordination Group, MDCG) hat u. a. entsprechend Art. 105 lit. c Verordnung (EU) 2017/745 die Entwicklung von Leitlinien für die wirksame und harmonisierte Durchführung der Medizinprodukte-Verordnung zur Aufgabe. 2019 veröffentlichte die MDCG eine Leitlinie[36] zur Bestimmung, ob Software ein Medizinprodukt darstellt oder nicht, die leider ausschließlich in englischer Sprache verfügbar ist. Im Anhang I der Leitlinie finden sich verschiedene Beispiele, welche bei der Beurteilung, ob es sich bei der Software um ein Medizinprodukt handelt oder nicht, sehr hilfreich sein können.

---

[35] Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates. Online, zitiert am 2022-06-24; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32017R0745
Konsolidierte Text: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A02017R0745-20200424

[36] Medical Device Coordination Group (MDCG): Guidance MDCG 2019-11 - Qualification and classification of software. Online, zitiert am 2022-06-24; verfügbar unter https://ec.europa.eu/health/medical-devices-sector/new-regulations/guidance-mdcg-endorsed-documents-and-other-guidance_en bzw. pdf-Datei unter https://ec.europa.eu/health/document/download/b45335c5-1679-4c71-a91c-fc7a4d37f12b_en?filename=md_mdcg_2019_11_guidance_qualification_classification_software_en.pdf

Eine große Anzahl von Medical Apps wird ein vermutlich als Medizinprodukt klassifizierbar sein, aber auf einige wird es auch nicht zutreffen. Laut MDCG sind beispielsweise Software-Produkte, die ausschließlich der Dokumentation der Patientenbetreuung bzw. -behandlung dienen, nicht als Medizinprodukt anzusehen. So ist beispielsweise die Medical App „Onkologische S3-Leitlinien“ [37] der Deutschen Krebsgesellschaft eine reine App zum Nachschlagen, denn die App überträgt die Empfehlungen, Tabellen und Abbildungen diverser S3-Leitlinien lediglich digital ab; somit ist die App kein Medizinprodukt i. S. d. Verordnung (EU) 2017/745. Auch die Medical App „Arzneimittel pocket plus“[38] stellt ein reines Nachschlagewerk dar und ist somit laut MDCG kein Medizinprodukt. Hingegen ist die App „Mika“[39] ein Medizinprodukt, denn neben einem Patiententagebuch beinhaltet die Apps beispielsweise auch Hinweise bzgl. Ernährung bei Krebs sowie mentale Übungen, damit Patienten besser mit Gefühlen wie Angst und Kontrollverlust umgehen lernen; d. h., Mika unterstützt aktiv die Krebstherapie.

Die Einschätzung, ob es sich um ein Medizinprodukt handelt oder nicht, kann dabei schwierig sein.[40] Sogenannte „Lifestyle“-Produkte, die der Gesundheit im allgemeinen Dienen, müssen nicht zwangsläufig ein Medizinprodukt darstellen, wenn sie der Gesundheit im Allgemeinen dienen. Eine App, welche Anleitungen zu Trainingsübungen oder Tipps zur Ernährung gibt, kann der allgemeinen Gesundheit eines Menschen dienen und ist ggf. nicht als Medizinprodukt anzusehen. Eine App, welche beispielsweise Trainingsübungen für Adipositas-Patienten oder Ernährungs-Tipps für Diabetiker anbietet, weist einen Bezug zur „Verhütung, Behandlung oder Linderung von Krankheiten“ auf und wird wahrscheinlich als Medizinprodukt anzusehen sein. Daher kann nur im jeweiligen Einzelfall anhand der Zweckbestimmung der App entschieden werden, ob es sich um ein Medizinprodukt handelt oder nicht.

Aber auch wenn es sich bei der App um ein Medizinprodukt handeln sollte: Die Verordnung (EU) 2017/745 enthält keine speziellen datenschutzrechtlichen Anforderungen, welche von Herstellern oder Händlern im Kontext von Medizinprodukten zu berücksichtigen wären. Daher gilt unmittelbar die DS-GVO, ergänzend die nationalen datenschutzrechtlichen Vorgaben. In ErwGr. 43 der Verordnung (EU) 2017/745 findet sich jedoch eine Anforderung nach Transparenz und Informationen, die insbesondere in Hinblick auf Patientensicherheit (Safety[41]) auszulegen ist:

> „Transparenz und angemessener Zugang zu Informationen, die für den vorgesehenen Anwender entsprechend aufbereitet sind, sind im öffentlichen Interesse unerlässlich, um die öffentliche Gesundheit zu schützen, die Rolle der Patienten und Angehörigen der Gesundheitsberufe zu stärken und ihnen sachkundige Entscheidungen zu ermöglichen, ein solides Fundament für gesetzgeberische Entscheidungen zu schaffen und Vertrauen in das Rechtssystem aufzubauen.“

---

[37] Deutsche Krebsgesellschaft e.V.: Onkologische S3-Leitlinien – jetzt als App. Online, zitiert am 2022-08-18; verfügbar unter https://www.leitlinienprogramm-onkologie.de/app/

[38] Börm Bruckmeier Verlag GmbH: Arzneimittel pocket plus. Online, zitiert am 2022-08-18; verfügbar unter

- Android: https://play.google.com/store/apps/details?id=com.boerm.bruckmeier.arzneimittel_pocket&gl=DE
- Apple: https://apps.apple.com/de/app/arzneimittel-pocket-2018/id989086879

[39] Fosanis GmbH: Mündig, mutig, motiviert durch die Krebstherapie. Online, zitiert am 2022-08-18; verfügbar unter https://www.mitmika.de/

[40] Auf den Webseiten des BfArM findet sich eine Orientierungshilfe. Online, zitiert am 2022-09-01; verfügbar unter https://www.bfarm.de/DE/Medizinprodukte/Aufgaben/Abgrenzung-und-Klassifizierung/_artikel.html

[41] Grundsätzlich kann zwischen Informationstechnologie (IT) und Operationelle Technik (OT) unterschieden werden. Während IT-Security die Sicherheit informationstechnisch verarbeiteter Informationen gewährleisten soll, ist die Aufgabe von Safety, Umfeld und Menschen vor unerwünschten Wirkungen wie beispielsweise einem Stromschlag zu schützen. Zwischen beiden existiert mitunter ein Zusammenhang, die Schutzziele unterscheiden sich jedoch.

Nach Anhang I (Kap. II Ziff. 17.4, Kap. III lit. ab) der Verordnung (EU) 2017/745 müssen Hersteller insbesondere bei Softwareprodukten „Mindestanforderungen bezüglich Hardware, Eigenschaften von IT-Netzen und IT-Sicherheitsmaßnahmen einschließlich des Schutzes vor unbefugtem Zugriff, die für den bestimmungsgemäßen Einsatz der Software erforderlich sind“, festlegen; weitergehende Vorgaben sind jedoch nicht enthalten, sodass für die Umsetzung dieser Anforderung letztlich der Stand der Technik herangezogen werden muss. Jedoch veröffentlichte die MDCG 2019 eine englischsprachige Leitlinie zur Cybersicherheit[42], welche von Herstellern von Medizinprodukten beachtet werden muss. Die Leitlinie fordert, dass bei klinischen Prüfungen, die zum Nachweis der Konformität von Medizinprodukten mit der Verordnung (EU) 2017/745 durchgeführt werden müssen, Vorgaben aus dem Datenschutzrecht beachtet werden müssen. Die Leitlinie enthält jedoch bzgl. Datenschutz keinerlei weitergehende Anforderungen.

Auch enthält sowohl das deutsche Gesetz zur Durchführung unionsrechtlicher Vorschriften betreffend Medizinprodukte als auch die Medizinprodukte-Betreiberverordnung (MPBetreibV) für Betreiber ausschließlich Vorgaben, welche den sicheren Betrieb eines Medizinproduktes gewährleisten sollen, d. h. sicher in dem Sinne, dass Anwender und Patienten durch die Nutzung des Medizinproduktes keine gesundheitlichen Schäden erleiden sollen (Safety).[43]

Bzgl. Datenschutz enthalten weder die Verordnung (EU) 2017/745 noch die deutschen ergänzenden Regelungen Anforderungen bzgl. Datenschutz oder IT-Sicherheit für die Hersteller oder Betreiber von Medizinprodukten, sodass hier die allgemeinen Regelungen der DS-GVO sowie begleitende nationale Regelungen wie beispielsweise das BDSG oder das TTDSG anzuwenden sind.

Hinweis 2: Medizinprodukte werden häufig nicht nur für den europäischen Markt entwickelt, sondern Patienten globaler angeboten. Die amerikanische FDA veröffentlichte 2019 eine Leitlinie für mobile medizinische Softwareprodukte.[44]

[42] Medical Device Coordination Group (MDCG): Guidance MDCG 2019-16 rev.1 - Guidance on cybersecurity for medical devices. Online, zitiert am 2022-06-24; verfügbar unter https://ec.europa.eu/health/medical-devices-sector/new-regulations/guidance-mdcg-endorsed-documents-and-other-guidance_en bzw. pdf-Datei unter https://ec.europa.eu/health/document/download/b23b362f-8a56-434c-922a-5b3ca4d0a7a1_en?filename=md_cybersecurity_en.pdf

[43] Hinweis: Soll die App auch innerhalb U.S.A. vertrieben bzw. eingesetzt werden, so sind die Vorgaben der amerikanischen Behörden bzgl. Cybersicherheit zwingend auch zu beachten, insbesondere der U.S.-Behörden HHS und FDA (siehe Links in Literatur/Internet)

[44] FDA: Policy for Device Software Functions and Mobile Medical Applications. Guidance for Industry and Food and Drug Administration Staff. (Stand: 2019-09-27). Online, zitiert am 2022-08-02; verfügbar unter https://www.fda.gov/regulatory-information/search-fda-guidance-documents/policy-device-software-functions-and-mobile-medical-applications bzw. pdf-Datei unter https://www.fda.gov/media/80958/download

8 Mobile Apps: In der Regel ein Telemedium

Entsprechend § 1 TMG sind alle elektronischen Informations- und Kommunikationsdienste Telemedien, soweit sie nicht „reine“[45]

a) Telekommunikationsdienste nach § 3 Nr. 61 Telekommunikationsgesetz (TKG),
b) telekommunikationsgestützte Dienste nach § 3 Nr. 63 TKG oder
c) Rundfunk nach § 2 Rundfunkstaatsvertrag (RStV)

sind. Diese Negativdefinition des Begriffs „Telemedien“ beinhaltet eine Ausschlussdefinition, die als Oberbegriff für alle denkbaren Arten multimedialer Angebote anzusehen ist, auch solche, die erst zukünftig entstehen oder zukünftig an Bedeutung gewinnen werden. Es gibt keinen elektronischen Informations- und Kommunikationsdienst, den man nicht zuordnen kann oder der aus dem Raster fallen würde.

Ist eine App daher kein Telekommunikationsdienst i. S. v. § 3 Ziff. 61 TKG, so handelt es sich um einen Telemediendienst. Aber: Entsprechend § 3 Nr. 40 TKG zählen auch nummernunabhängige interpersonelle Kommunikationsdienste zu den Telekommunikationsdiensten[46], sodass auch sogenannte „Over-the-top-(OTT)“-Kommunikationsdienste wie webgestützte E-Mail-Dienste oder Instant-Messenger Telekommunikationsdienste darstellen. Das Gremium europäischer Regulierungsstellen für elektronische Kommunikation[47] (GEREK, englisch Body of European Regulators for Electronic Communications, BEREC) führte eine Taxometrie für OTT-Dienste ein, sodass verschiedene Klassen unterschieden werden sollten[48]:

- OTT-0: Ein OTT-Dienst, der als elektronischer Kommunikationsdienst („electronic communications service“, ECS) eingestuft wird. Dies sind Dienste, die z. B. Internet-Telefonie (VoIP) anbieten.
- OTT-1: Ein OTT-Dienst, der kein elektronischer Kommunikationsdienst ist, aber potenziell mit einem elektronischen Kommunikationsdienst konkurriert. Darunter fallen Dienste, welche Kommunikationsmöglichkeiten unter Einsatz des Internets anbieten, selbst aber keine inhaltlichen Angebote beinhalten. Beispiele sind Webmail-Dienste oder Instant-Messenger.
- OTT-2: Alle anderen OTT-Dienste. Diese Dienste haben gemeinsam, dass sie auch inhaltliche Elemente beinhalten. Typische Beispiele hierfür sind On-Demand-Plattformen wie Netflix® oder Amazon Prime Video®.

OTT-0 und OTT-1 sind als Telekommunikationsdienste i. S. d. TKG anzusehen, OTT-2 als Inhalteanbieter werden eher regelhaft als Telemedien anzusehen sein.

[45] Ricke T.: § 1 TMG, Rn. 2. In: Spindler/Schuster (Hrsg.) Recht der elektronischen Medien. C. H. Beck Verlag, 4. Auflage 2019. ISBN 9783406730122

[46] Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts (Telekommunikationsmodernisierungsgesetz). Drucksache 19/26108, S. 234. Online, zitiert am 2022-06-24; verfügbar unter https://dserver.bundestag.de/btd/19/261/1926108.pdf

[47] Verordnung (EU) 2018/1971 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 zur Einrichtung des Gremiums europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) und der Agentur zur Unterstützung des GEREK (GEREK-Büro), zur Änderung der Verordnung (EU) 2015/2120 und zur Aufhebung der Verordnung (EG) Nr. 1211/2009. Online, zitiert am 2022-06-24; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32018R1971

[48] BEREC Report on OTT services. Stand 2016-02-26. Online, zitiert am 2022-06-24; verfügbar unter https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services bzw. pdf-Datei des Reports unter https://www.berec.europa.eu/sites/default/files/files/document_register_store/2016/2/BoR_%2816%29_35_Report_on_OTT_services.pdf

Somit müssen Mobile Apps, welche keinen Telekommunikationsdienst darstellen, den Vorgaben für Telemedien genügen, d. h. insbesondere auch den Regelungen im TMG und TTDSG.

8.1 Ausgewählte Anforderungen aus dem TMG

Entsprechend § 5 TMG sowie § 55 RStV müssen Diensteanbieter Informationen bereitstellen.[49] Diese Anforderung ist allgemein auch als „Impressumspflicht" für Webseiten bekannt, gilt aber für alle Anbieter von Telemedien, die nicht ausschließlich persönlichen oder familiären Zwecken dienen. Daher müssen auch entsprechend einzustufende Apps entsprechende Informationen bereitstellen. Aus Sicht des Datenschutzrechts ist diese Pflicht von Bedeutung, weil bei einem Verstoß gegen datenschutzrechtliche Vorgaben eine betroffene Person den Hersteller bzw. den Anbietern der App als Verursacher des Datenschutzverstoßes nur über diese Angaben aus dem Impressum identifizieren und so gegen diesen vorgehen kann.

8.2 Ausgewählte Anforderungen aus dem TTDSG[50]

8.2.1 Vorgaben TTDSG: Eine Ergänzung der Anforderungen der DS-GVO

In Art. 4 Abs. 1a RL 2002/58/EG heißt es: „Unbeschadet der Richtlinie 95/46/EG ist durch die in Absatz 1 genannten Maßnahmen zumindest Folgendes zu erreichen". D. h., bei den Anforderungen hinsichtlich technischer und organisatorischer Vorkehrungen im TTDSG handelt es sich um die RL 95/46/EG *ergänzende* Maßnahmen, es erfolgt insbesondere keine Verdrängung der Anforderungen der Datenschutz-Richtlinie 95/46/EG, bzw. der DS-GVO als Fortsetzung der Datenschutz-Richtlinie.

Damit muss allen Anforderungen der DS-GVO genügt werden, insbesondere auch den Anforderungen aus

- Art. 25 DS-GVO Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen („Privacy by Design/Default"),
- Art. 32 DS-GVO Sicherheit der Verarbeitung und
- Art. 35 DS-GVO Datenschutz-Folgenabschätzung.

8.2.2 Standortdaten

Speziell im Umfeld von Mobile Apps werden des Öfteren Standortdaten verarbeitet. Entsprechend § 3 Ziff. 56 TKG werden unter „Standortdaten" Daten verstanden, welche „in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst verarbeitet werden und die den Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben", also Standortkoordinaten wie GPS-Informationen, welche mit mobilen Geräten wie Smartphones oder Tablets empfangen und verarbeitet werden können.

Hier gilt es vor allem auch dem Grundsatz der datenschutzfreundlichen Voreinstellungen Rechnung zu tragen (vgl. Kapitel 9.5.2). Demnach darf die Verarbeitung von Standortdaten durch eine App nur erfolgen, wenn der Nutzer der Verarbeitung zuvor ausdrücklich zugestimmt hat. Die Genauigkeit der Standortlokalisierung sollte sich zudem eng am jeweiligen Zweck der App orientieren. So könnte eine App für die Verarbeitung des eRezepts für die Darstellung der nächstgelegenen Apotheke entweder die Standortdaten verwenden oder der Nutzer gibt seinen Standort (z. B. die Postleitzahl) händisch ein.

[49] Siehe z. B. OLG Hamm, Urt. v. 20.05.2010, Az. I-4 U 225/09. Online, zitiert am 2022-07-08; verfügbar unter https://dejure.org/2010,622, Volltext Urteil unter https://openjur.de/u/51869.html

[50] Für eine umfassendere Einführung in die Bedeutung des TTDSG für telemedizinische Versorgungsmöglichkeiten siehe „Praxishilfe zur Beachtung des TTDSG im Bereich der Telemedizin" der GMDS, Stand: 23. April 2022. Online, zitiert am 2022-06-24; verfügbar unter https://gesundheitsdatenschutz.org/html/ttdsg.php

Anforderung 1: Ist die Nutzung von Standortdaten wie beispielsweise Daten des „Global Positioning System“ (GPS) oder „Location Based Services“ (LBS) für bestimmte Funktionen der App erforderlich, **MUSS** der Nutzer der Verarbeitung der Standortdaten durch die App ausdrücklich zustimmen.

Anforderung 2: Die Genauigkeit der Lokalisierung **MUSS** sich am Zweck des Service orientieren.

Anforderung 3: Die Verarbeitung von Standortdaten **MUSS** in den Datenschutzhinweisen dargestellt werden.

Anforderung 4: Die Zustimmung **KANN** einmalig erfolgen und permanent gespeichert werden, **MUSS** aber jederzeit vom Nutzer für die Zukunft widerrufen werden können. Bei Abgabe der Einwilligung **MUSS** der Nutzer über sein Widerrufsrecht informiert werden. Der Widerruf der Einwilligung **MUSS** so einfach wie die Erteilung der Einwilligung sein.

Anforderung 5: Erteilte Einwilligungen für die Lokalisierung des Nutzerstandortes **MÜSSEN** jederzeit temporär oder permanent für die Zukunft widerrufen werden können.

8.2.3 Schutz der Daten

Entsprechend § 19 Abs. 1 TTDSG müssen Anbieter von Telemedien sicherzustellen, dass Nutzer von Telemedien

- die Nutzung des Dienstes jederzeit beenden können und
- diese Dienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen können.

Die Regelung basiert auf Art. 5 Abs. 1 Richtlinie 2002/58/EG und schützt die Vertraulichkeit der Kommunikation. Die Regelung ist weit formuliert, sodass schon der Umstand einer Nutzung von Telemedien geschützt ist, d. h. einem etwaigen Dritten darf eine Nutzung nicht bekannt werden.

Anforderung 6: Die personenbezogenen Daten **MÜSSEN** gegen die Kenntnisnahme unberechtigter Dritter geschützt werden.

Anforderung 7: Das System **MUSS** es Benutzern ermöglichen, sich von ihrer laufenden Sitzung abzumelden.

Auch der Einsatz von sogenannten Third-Party-Cookies kann beispielsweise dazu führen, dass bekannt wird, wer einen Telemediendienst nutzt. Ein Telemediendienst muss daher einen Schutz vor dieser (unbefugten) Kenntnisnahme beinhalten. Analog gilt die Aussage für alle anderen Technologien, mit denen ein Dritter Kenntnis von der Nutzung des Telemediendienstes erhalten kann. Und natürlich müssen die bei der Nutzung des Telemediendienstes anfallenden Daten erst recht entsprechend geschützt werden.

Diese Anforderung aus dem TTDSG impliziert, dass insbesondere auch eine sichere Identifikation des Nutzers erfolgen muss, damit ein unberechtigter Zugriff auf die personenbezogenen bzw. personenbeziehbaren Daten verhindert wird. Dabei ist zu beachten, dass gerade im mobilen Bereich eingesetzte biometrische Methoden der Authentifizierung wie Nutzung von Fingerabdruck- oder Gesichtserkennung schon des Öfteren erfolgreich angegriffen wurden, weswegen diese Authentifizierungsmethoden nicht zur alleinigen Identifizierung geeignet sind, wenn sensible Daten zu schützen sind. Insbesondere wenn die in Art. 9 Abs. 1 DS-GVO genannten Datenkategorien verarbeitet werden, sollten biometrische Authentifizierungsmethoden nur als Add-on, z. B. im Rahmen einer Zwei-Faktor-Authentifizierung, genutzt werden, jedoch nie als einzige Authentifizierungsmethode eingesetzt werden.

Anforderung 8: Benutzerkonten **MÜSSEN** mit mindestens einem geeigneten Authentisierungsmerkmal geschützt werden.

Anforderung 9: Falls die App Passwörter zur Authentisierung des jeweiligen Benutzers verwendet, **MUSS** die App diese bei der Speicherung schützen, indem ausschließlich Passwort-Hashes gespeichert werden. Das Hashing der Passwörter **MUSS** dem Stand der Technik entsprechen und vom BSI empfohlene Algorithmen verwenden[51].

Anforderung 10: Falls Passwörter als Authentisierungsmerkmal genutzt werden, **DARF** die Darstellung **NICHT** im Klartext erfolgen, ausgenommen der Benutzer schaltet die Funktion ausdrücklich zur Prüfung des eingegebenen Passwortes an.

Anforderung 11: Falls Passwörter als Authentisierungsmerkmal genutzt werden, **MUSS** eine Änderung des eigenen Passwortes jederzeit durch den Anwender möglich sein.

Anforderung 12: Falls Passwörter als Authentisierungsmerkmal genutzt werden, **MUSS** ein Schutz gegen Online-Angriffe wie Wörterbuch- und Brute-Force-Attacken vorhanden sein, der das Erraten von Passwörtern stark erschwert.

Anforderung 13: Die App **MUSS** insbesondere Maßnahmen implementiert haben, welche ein Ausprobieren von Login-Parametern wirksam behindern.[52] Dies **SOLLTE** eine Verzögerung zur Neueingabe von Login Credentials nach Falscheingabe beinhalten, wobei sich die Dauer der Verzögerung an der Anzahl Fehlversuche orientiert.[53]

Anforderung 14: Falls Passwörter als Authentisierungsmerkmal genutzt werden, MUSS die Eingabe von Passwörtern mit Einsatz von Textelementen/-feldern erfolgen, die die eingegebenen Zeichen verschleiern.

Anforderung 15: Für die Authentisierung an einer App **KÖNNEN** biometrische Möglichkeiten des Betriebssystems (z. B. Fingerprint, Gesichtserkennung) mit Zustimmung des jeweiligen Benutzers genutzt werden. Es **MUSS** immer auch eine eigene[54] Authentisierung angeboten werden.

---

[51] BSI: Technische Richtlinie 02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“. Stand: 2022-02-11. Online, zitiert am 2022-07-22; verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html

[52] Siehe auch NIST Password Guidelines, insbesondere NIST Special Publication 800-63 „Digital Identity Guidelines“ Online, zitiert am 2022-08-18; verfügbar unter https://pages.nist.gov/800-63-3/sp800-63-3.html

[53] Z. B. nach insgesamt 3 Fehlversuchen Verzögerung 1 Minute, nach insgesamt 5 Fehlversuchen 10 Minuten, usw. Dadurch wird das Ausprobieren so zeitintensiv, dass die Zeit, die ein Angreifer zum einzudringen benötigt, drastisch erhöht, bis hin zu dem Punkt, an dem der Versuch für den Angreifer faktisch sinnlos ist.

[54] D. h. es muss eine vom Hersteller der App implementierte Authentisierungsmethode vorhanden sein, die unabhängig von den Methoden ist, welche der Hersteller des Mobilgerätes anbietet.
Vorsicht ist bei der Nutzung von Authentisierungsdiensten von amerikanischen Anbietern wie Google, Apple usw. geboten. Einerseits stellen einige dieser Anbieter auch das Betriebssystem zur Verfügung, sodass die Sicherheit bei Nutzung dieser Dienste im Vergleich zur Verwendung der in den mobilen Geräten enthaltenen Authentisierungswerkzeugen kaum erhöht wird, andererseits findet bei diesen Diensten i. d. R. immer ein Transfer personenbezogener Daten in ein Drittland statt, sodass sich hier die ganze Spannbreite der Drittlandübermittlung eröffnet.
Besser ist die von Herstellern mobiler Geräte unabhängige Verwendung bekannter Authentifizierungsmethoden wie bspw. Benutzername/Passwort oder die Zusendung einer PIN über SMS an eine hinterlegte Mobiltelefonnummer. Auch die Nutzung von Security-Token mit Authentisierungsfunktion ist möglich, wobei der benutzte Security-Token vom Hersteller des Betriebssystems des mobilen Gerätes unabhängig sein muss. Dies kann ein virtuelles Security-Token sein (ähnlich des von der gematik geplanten virtuellen Konnektors) oder auch ein Hardware-Token, wie beispielsweise ein FIDO2-Token. FIDO2 Security Token mit NFC-Funktionalität sind i. d. R. auch bei aktuell auf dem Markt erhältlichen Smartphones gut einsetzbar.
Hinweis: Wer sich für die Implementierung von Benutzername/Passwort entscheidet, sollte „Appendix A—Strength of Memorized Secrets“ der NIST Special Publication 800-63B „Digital Identity Guidelines: Authentication and Lifecycle Management“ berücksichtigen. Online, zitiert am 2022-08-04; verfügbar unter https://csrc.nist.gov/publications/detail/sp/800-63b/final

Anforderung 16: Die Verwendung biometrischer Systeme wie z. B. Fingerabdruck oder Gesichtserkennung **DARF** jedoch **NICHT** als alleiniger Authentifizierungsmechanismus eingesetzt werden, sondern mur als Teil einer Zwei-Faktor-Authentifizierung verwendet werden.

Anforderung 17: Für die Verwendung von biometrischen Identifizierungsmethoden wie Fingerprints **MUSS** eine Einwilligung des jeweiligen Benutzers zur Nutzung dieser Daten vorhanden sein. Der Einsatz von biometrischen Identifizierungsmethoden **MUSS** in den Datenschutzhinweisen erläutert werden.

Grundsätzlich besitzen die Hersteller von mobilen Betriebssystemen wie Apple oder Google, aber auch Hersteller von mobilen Geräten wie Smartphones oder Tablets, weitreichenden Zugriff auf die Geräte und damit ggfs. auch auf die entsprechenden Daten und somit die entsprechenden Informationen. Hier sind, ebenso wie bei der Übertragung der Informationen, Schutzvorkehrungen hinsichtlich unberechtigter Kenntnisnahme zu treffen.[55]

Anforderung 18: Schutzbedürftige Daten **MÜSSEN** bei der Übertragung sowie Speicherung gegen unberechtigte Einsichtnahme und Veränderung geschützt werden.

Anforderung 19: Für die verschlüsselte Speicherung vertraulicher Informationen **MÜSSEN** individuelle Krypto-Schlüssel verwendet werden. Es **SOLLTEN** vom Benutzer der App gebildete und kontrollierte Schlüssel verwendet werden.

Anforderung 20: Für kryptographische Operationen **MÜSSEN** geprüfte Standardbibliotheken verwendet werden.

Anforderung 21: Krypto-Schlüssel **KÖNNEN** auf dem Gerät nur dann gespeichert werden, wenn die Laufzeitumgebung dafür einen sicheren Datenspeicher zur Verfügung stellt. Andernfalls **MÜSSEN** Krypto-Schlüssel jeweils zur Laufzeit deterministisch berechnet werden und dabei einen beim ersten Start oder der Installation der App hinterlegten Faktor verwenden.

Anforderung 22: Vor der Übertragung vertraulicher Informationen an Backend-Server oder andere Empfänger **MÜSSEN** diese authentisiert werden.

Anforderung 23: Falls TLS-Server-Zertifikate verwendet werden, **MÜSSEN** diese von einer App auf Gültigkeit und Revocation-Status überprüft werden.[56] Bei Ungültigkeit oder Verbindungs-Timeout zum Revocation- oder OCSP-Server **MUSS** der Verbindungsaufbau abgebrochen und der Benutzer informiert werden.

Anforderung 24: Falls ein TLS-Server-Zertifikat verwendet wird und dieses Zertifikat als ungültig erkannt wurde, **MUSS** die Verbindung unterbrochen werden.

Es sollten nur unbedingt notwendige Kommunikations-Protokolle eingesetzt werden, da jedes implementierte Protokoll grundsätzlich die Möglichkeit eines Missbrauchs durch einen Angreifer beinhaltet. Die Dokumentation der Software muss daher die von der App genutzten

[55] Bzgl. TLS-Verschlüsselung sollten die Mindeststandards des BSI beachtet werden:
- Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG zur Verwendung von Transport Layer Security (TLS) Version 2.2 (Stand 2021-05-03) Online, zitiert am 2022-07-07; verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_2.html
- IT-Grundschutz-Referenztabelle zum Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG zur Verwendung von Transport Layer Security (TLS) (Stand 2021-05-03) Online, zitiert am 2022-07-07; verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Referenztabelle_Mindeststandard_TLS_V2_2-Grundschutz2021.html

[56] Hinweis: Für Behörden stellte das BSI Testfälle zur Prüfung des TLS-Protokolls, die sich ebenfalls gut zur Prüfung der eigenen Anwendung eignen. Online, zitiert am 2022-07-21; verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03116/TR-03116_node.html

Kommunikationsprotokolle sowie die Ports beinhalten, damit bei der Risikobetrachtung alle Protokolle und Ports berücksichtigt werden. Dies kann z. B. in Form einer Tabelle erfolgen:

Protokoll	Protokollname	Port-Nr. / Art	Verschlüsselt	Bemerkung
http	Hypertext Transfer Protocol	80 / TCP	Nein	Aus Gründen der Abwärtskompatibilität erforderlich
https	Hypertext Transfer Protocol Secure	443 / TCP	Ja (TLS)	TLS v. 1.2
FTPS	File Transfer Protocol über TLS	989/TCP; 990/TCP	Ja (TLS)	TLS v. 1.2
SFTP	SSH File Transfer Protocol	22/TCP	Ja (SSH-2)	
SSH	Secure Shell	22/TCP	Ja (SSH-2)	

Tabelle 1: Beispiel für eine Dokumentation der in einer mobilen App implementierten Kommunikations-Protokolle

Anforderung 25: Alle in der App implementierten Kommunikations-Protokolle **MÜSSEN** einschließlich genutzter Ports und eingesetzter Verschlüsselung dokumentiert werden.

Anforderung 26: Kommunikations-Protokolle ohne Verschlüsselung **DÜRFEN NICHT** eingesetzt werden, wenn kein zwingendes Erfordernis für den Einsatz besteht. Bei Einsatz eines unverschlüsselten Protokolls **MUSS** die Begründung, warum keine verschlüsselte Kommunikation möglich ist, dokumentiert werden.

Da insbesondere mobile Geräte wie Smartphones oder Tablets auch von Dritten genutzt werden können, ist dafür Sorge zu tragen, dass diese Dritte bei Nutzung des Endgerätes keinen Zugriff auf schutzwürdige Informationen erhalten.

Anforderung 27: Dateien, Ausgaben und Meldungen, die unautorisierten Benutzern zugänglich sind, **DÜRFEN NICHT** schutzbedürftige Informationen enthalten.

8.2.4 Anonyme oder pseudonyme Nutzung/Bezahlung

Gemäß § 19 Abs. 2 TTDSG müssen Anbieter von Telemedien

- den Nutzern die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist.
- Die Nutzer von Telemedien sind über diese Möglichkeit einer anonymen oder pseudonymen Nutzung bzw. Bezahlung zu informieren.

Im Bereich der Gesundheitsversorgung kann eine anonyme oder pseudonyme Bezahlung beispielsweise bei einer Abrechnung mit einer Krankenkasse technisch vielleicht möglich sein, jedoch müssen einer Krankenkasse zur Abrechnung die Versichertendaten übermittelt werden – was letztlich eine anonyme Abrechnung verhindert.

Gerade im Bereich der Gesundheitsversorgung können Vorgaben aus den Sozialgesetzbüchern oder anderen Gesetzen bestehen, welche diese Regelung des TTDSG einschränken.

Zu beachten: Abweichungen von den Vorgaben des TTDSG können nur gesetzlich geregelt sein, Abweichungen von den Vorgaben des TTDSG müssen inklusive der Gründe für die Abweichungen immer nachgewiesen werden, d. h. auch hier gilt eine entsprechende Dokumentationspflicht.

Anforderung 28: Personenbezogene Dienstleistungen innerhalb einer App **SOLLTEN** unter Verwendung von Pseudonymen (d. h. ohne Verwendung von Klarnamen oder anderen einer Person direkt zuordenbaren Informationen) nutzbar sein.

Anforderung 29: Nicht abrechnungsrelevante und nicht personenbezogene Dienstleistungen **MÜSSEN** anonym oder pseudonym nutzbar sein.

Anforderung 30: Vollständige IP-Adressen **DÜRFEN NICHT** als Pseudonym verwendet werden, sondern gelten grundsätzlich als direkt personenbeziehbar.

8.2.5 Weitervermittlung ist anzuzeigen

Gemäß § 19 Abs. 3 TTDSG ist die Weitervermittlung zu einem anderen Anbieter von Telemedien dem Nutzer anzuzeigen. Bei internetbasierten Diensten ist dies beispielsweise regelmäßig der Fall, wenn ein Nutzer mittels eines Hyperlinks zu einem anderen Dienst, also einer anderen Internetpräsenz geführt wird.[57] Keine Anwendung findet die Regelung jedoch, wenn ein Telemedium aus verschiedenen Inhalten besteht, welche ggf. auch von unterschiedlichen Servern abgerufen und im Browser des Nutzers als ein Dienst dargestellt werden[58]; die Transparenzpflicht verpflichtet aber zu einer entsprechenden Information des Nutzers.

Anforderung 31: Links oder Weiterleitungen aus der App auf Webportale von Dritten (externe Seitenanbieter) **MÜSSEN** mit einem Abgrenzungshinweis versehen werden. Der Nutzer **MUSS** erkennen können, dass ein Link zu einem Dritten führt, oder, dass er an einen Dritten weitergeleitet wird.

8.2.6 Technische und organisatorische Maßnahmen

Anbieter von geschäftsmäßig angebotenen Telemedien müssen gemäß § 19 Abs. 4 TTDSG

- soweit dies technisch möglich und wirtschaftlich zumutbar ist
- unter Berücksichtigung des Stands der Technik
- durch technische und organisatorische Vorkehrungen sicherstellen, dass
    - kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und
    - diese gesichert sind gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind.

§ 19 Abs. 4 TTDSG verpflichtet den Anbieter von Telemedien somit:

1) Zur Sicherstellung, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist. Wie der Anbieter dies gewährleistet, ist dem Anbieter überlassen. Aus technischer Sicht wird regelmäßig eine sog. „Härtung“ des Systems erforderlich sein, d. h. durch entsprechende Systemkonfigurationen Betriebssystem, Datenbank usw. entsprechend dem Stand der Technik abzusichern. Desgleichen müssen Richtlinien für Zugriffe existieren sowie technische Vorkehrungen, welche eine wirksame Umsetzung der Richtlinien gewährleisten. Nicht zuletzt gehört dazu auch ein Monitoring wie beispielsweise Intrusion Detection and Prevention Systeme, welche unbefugte Zugriffsversuche erkennen lassen. Wird der Telemediendienst selbst entwickelt, so gehört eine sicherheitsorientierte Entwicklung selbstverständlich auch dazu, dies beinhaltet ggf. auch externe Code-Reviews von auf IT-Sicherheit spezialisiertem Fachpersonal (welches sich selbstverständlich auch mit der Entwicklungsumgebung und -sprache auskennen muss).

[57] So wird beispielsweise ein Webseitenbesucher im Downloadbereich von „heise online“ (Heise Medien GmbH & Co. KG) eine Weiterleitung zur Webseite des Herstellers angezeigt, z. B. beim Download einer App wie den „DB Navigator“ unter https://www.heise.de/download/product/db-navigator-55739/download?affiliateId=17957 (URL zitiert am 2022-07-21)

[58] Moos F.: § 19, Rn. 26. In: Taeger / Gabel (Hrsg.) DS-GVO - BDSG – TTDSG. Deutscher Fachverlag GmbH, 4. Auflage 2022. ISBN 978-3-8005-1760-2

2) Die Gewährleistung der Sicherung gegen Störungen beinhaltet insbesondere, dass Vorkehrungen für möglichst wenig Ausfälle getroffen werden, was insbesondere natürlich auch ein entsprechendes Patchmanagement beinhaltet. Dazu gehört auch die Fähigkeit, die Verfügbarkeit des Telemediendienstes bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.
3) Die Gewährleistung der Sicherheit auch bei äußeren Angriffen wird letztlich durch die Erfüllung der beiden erstgenannten Punkte erfüllt, insbesondere dem ersten Punkt. Aber hierzu gehört ggf. auch, dass regelmäßige Penetrationstest erfolgen, damit Schwachstellen frühzeitig erkannt und beseitigt werden.

Anforderung 32: Anmeldeinformationen, wie Benutzername/Passwort bzw. Authentisierungstoken, **KÖNNEN** für die Session auf dem Endgerät gespeichert werden. Wenn der Nutzer eingewilligt hat (Opt-In), **KÖNNEN** die Informationen dauerhaft gespeichert werden (in der Anwendung angemeldet bleiben). Diese LogIn-Informationen **MÜSSEN** verschlüsselt gespeichert werden. Der Nutzer **MUSS** über die Speicherung informiert werden und, im Falle der Nutzung einer „Angemeldet bleiben"-Funktion, die Möglichkeit haben, dieser zu widersprechen.

Anforderung 33: Wenn in der App persönliche oder personenbezogene Informationen zugänglich sind, **MUSS** der Nutzer bei der Verwendung einer „Angemeldet bleiben"-Funktion die Möglichkeit haben eine PIN zu vergeben, die beim Starten der App oder beim Aufwecken der App aus dem Hintergrund abgefragt werden **MUSS**.

Bei der Interpretation der Vorgaben von § 19 Abs. 4 TTDSG ist zu beachten: Art. 4 Abs. 1 RL 2002/58/EG verlangt unter Berücksichtigung Stand der Technik und Kosten „geeignete technische und organisatorische Maßnahmen [zu] ergreifen, um die Sicherheit seiner Dienste zu gewährleisten", kennt aber keine „Unzumutbarkeit". Bei richtlinienkonformer Auslegung spielt die Zumutbarkeit daher keine Rolle. Gleichwohl beinhaltet die in Art. 4 Abs. 1 RL 2002/58/EG enthaltene „Berücksichtigung Stand der Technik und Kosten" sicherlich, dass die Kosten zur Gewährleistung der Sicherheit der Dienste analog Art. 32 DS-GVO angemessen im Sinne des Risikos auszulegen sind, jedoch grundsätzlich ein „um ein dem Risiko angemessenes Schutzniveau zu gewährleisten" ist.

Anforderung 34: Werden Betriebssystemfunktionen oder Funktionen, die von anderen Apps bereitgestellt werden, von der App zur Verarbeitung von Daten genutzt, so **MUSS** diese Nutzung in den Datenschutzhinweisen beschrieben werden. Der Nutzer **MUSS** vor oder spätestens bei der ersten Nutzung der Funktion darauf hingewiesen werden.

8.2.7 Erlaubnistatbestände zur Verarbeitung bei Telemedien

§ 25 TTDSG ist in Teil 3 des TTDSG verortet, adressiert also den Schutz der Privatsphäre bei Endeinrichtungen bei der Nutzung von Telemedien. Entsprechend § 25 TTDSG ist

- die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder
- der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind,

nur zulässig, wenn

a) der **Endnutzer** auf der Grundlage von klaren und umfassenden Informationen **eingewilligt hat** (§ 25 Abs. 1 TTDSG)
b) oder wenn
    1. der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder
    2. der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen

die Durchführung der **Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz** ist (§ 25 Abs. 2 Ziff. 1 TTDSG)

c) oder wenn
   1. die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder
   2. der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen

   unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen **vom Nutzer ausdrücklich gewünschten Telemediendienst** zur Verfügung stellen kann (§ 25 Abs. 2 Ziff. 2 TTDSG).

Die Regelung von § 25 TTDSG entspricht fast wortgleich Art. 5 Abs. 3 ePrivacy-Richtlinie und stellt eine Verbotsnorm mit Erlaubnisvorbehalt dar.

Hinweis 3: Auch wenn die ePrivacy-Richtlinie häufig als „Cookie"-Richtlinie bezeichnet wird, betrifft diese Regelung natürlich nicht nur Cookies, sondern alle Verarbeitungen, wenn Daten auf einem Endgerät gespeichert werden oder Informationen vom Endgerät abgerufen werden. Insbesondere sind somit auch andere Tracking-Maßnahmen als Cookies von dieser Regelung umfasst, wenn „in der Endeinrichtung gespeicherte Informationen" wie beispielsweise Betriebssystem, Bildschirmauflösung, in Browser installierte Plug-ins usw. abgerufen werden.

Anforderung 35: Zugriffe auf personenbezogene Daten, die bereits auf dem Gerät gespeichert sind (z. B. Kontakte, Nachrichten, Fotos, GPS) **MÜSSEN** im Datenschutzhinweis beschrieben und begründet werden. Wenn das Betriebssystem die Einwilligung nicht verwaltet, **MUSS** die Verwaltung der Einwilligung durch die App selbst erfolgen.

Anforderung 36: In die Verarbeitung von Unique Identifier des Endgerätes bzw. des Betriebssystems **MUSS** der Nutzer einwilligen (Opt-In), ansonsten dürfen die Daten nicht verarbeitet werden. Die Verarbeitung **MUSS** in den Datenschutzhinweisen erläutert werden.

Anforderung 37: Die Verarbeitung von Unique Identifier, die einen Nutzer App-übergreifend identifizieren (z. B. in App 1 - Nutzer = abcd und in App 2 - Nutzer = abcd), **MUSS** mit ausdrücklicher Einwilligung (Opt-In) erfolgen. Die Verarbeitung **MUSS** in den Datenschutzhinweisen erläutert werden.

Anforderung 38: Werden personenbezogene Daten für zusätzliche Funktionen, die dem Funktionsumfang der App zuzurechnen sind, erhoben und verarbeitet, **MUSS** dem Nutzer die Möglichkeit des Widerspruchs (Opt-Out) angeboten werden. Die optionalen Funktionen sowie die Freiwilligkeit der Verwendung **MUSS**, inklusive der Opt-Out-Möglichkeit, in den Datenschutzhinweisen beschrieben werden.

9 Datenschutzrechtliche Anforderungen

9.1 Einhaltung der „Grundsätze für die Verarbeitung personenbezogener Daten“

Art. 5 Abs. 1 DS-GVO beinhaltet Grundsätze, die bei jeder Verarbeitung personenbezogener Daten immer gewährleistet sein müssen. Diese Grundsätze beinhalten:

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz** (Art. 5 Abs. 1 lit. a DS-GVO):

  Personenbezogene Daten dürfen ausschließlich auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Dies beinhaltet:

  1. Die Verarbeitung muss einem legitimen Zweck dienen und ein Erlaubnistatbestand zur Verarbeitung der Daten liegt vor. Desgleichen müssen im Falle der Verarbeitung der personenbezogenen Daten in einem Drittstaat die Vorgaben von Kapitel V DS-GVO erfüllt sein. Werden Auftragsverarbeiter eingesetzt, sind die Vorgaben zur Auftragsverarbeitung einzuhalten, bei Zusammenarbeit mit Partnern muss ggf. ein Vertrag zur gemeinsamen Verarbeitung abgeschlossen werden.
  2. Was genau der Verordnungsgeber unter der Regelung einer „Verarbeitung nach Treu und Glauben“ versteht, wird an keiner Stelle in der DS-GVO präzisiert. Jedoch findet sich in ErwGr. 38 RL 95/46[59] hierzu Folgendes:

     > „Datenverarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden.“

     D. h. die Verarbeitung muss „fair“ erfolgen.
  3. Die Verarbeitung der Daten muss für die betroffenen Personen transparent erfolgen. Dies erfordert insbesondere die Gewährleistung der in Kapitel II DS-GVO dargestellten Betroffenenrechte.

Anforderung 39: Die Verarbeitung **MUSS** einem legitimen Zweck dienen.

Anforderung 40: Eine Verarbeitung von Daten, die überraschend oder unerwartet für die betroffenen Personen ist, **DARF NICHT** durchgeführt werden.

Anforderung 41: Über jede Verarbeitung **MÜSSEN** betroffene Personen alle Informationen erhalten, damit eine für die betroffenen Personen transparente Verarbeitung gewährleistet wird.

Anforderung 42: Eine Verarbeitung, welche das Machtungleichgewicht[60] zwischen Verantwortlichem und betroffenen Personen missachtet, **DARF NICHT** erfolgen.

Hinweis 4: Man spricht von einem „Machtungleichgewicht“ zwischen Verantwortlichem und betroffener Person, wenn eine Abhängigkeit der betroffenen Person vom Verantwortlichen besteht, z. B. Arbeitgeber und Arbeitnehmer oder Arzt und Patient. Ein gewisses Ungleichgewicht zwischen Verantwortlichem und betroffenen Personen besteht natürlich immer, da nur der Verantwortliche über Zwecke und Mittel der Verarbeitung entscheidet. ErwGr. 43 DS-GVO hebt aber hervor, dass bei besonders klaren Ungleichgewichten ggf. eine Einwilligung keine Rechtsgrundlage darstellen kann,

[59] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Online, zitiert am 2022-06-24; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri= CELEX%3A31995L0046

[60]

da die Einwilligung nicht als „freiwillig gegeben“ angesehen werden kann. Als Beispiel nennt ErwGr. 43 eine Behörde als Verantwortlichen. Aber auch im medizinischen Kontext kann dies eine Rolle spielen, da beispielsweise eine angebotene Heilung einer Krankheit (z. B. Krebs) immer eine starke Abhängigkeit des Patienten als betroffene Person erzeugt. Wird das Machtungleichgewicht missachtet, ist eine Einwilligung als Rechtsgrundlage der Verarbeitung daher ggf. nicht wirksam, eine darauf erfolgende Verarbeitung würde dann rechtswidrig erfolgen. Daher muss immer beachtet werden, wie dem Ungleichgewicht zwischen Verantwortlichem und betroffener Person begegnet werden kann, insbesondere durch eine transparente Verarbeitung, der Wahrung der Betroffenenrechte sowie der Gewährleistung der Sicherheit der Verarbeitung.

- **Zweckbindung** (Art. 5 Abs. 1 lit. b DS-GVO):
  Die Verarbeitung personenbezogener Daten darf nur im Rahmen von festgelegten, eindeutigen und legitimen Zwecken erfolgen. Somit scheidet insbesondere eine Verarbeitung für noch unbekannte Zwecke aus, eine „Vorratsdatenspeicherung“ ist nicht mit den Vorgaben der DS-GVO vereinbar.
  Eine Änderung des Zweckes bedarf wiederum eines eigenen Erlaubnistatbestandes. Dabei gilt eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke nicht als unvereinbar mit dem ursprünglichen Zweck, was ggf. für andere Zweckänderungen nachgewiesen werden muss.

Anforderung 43: Die Zwecke der Verarbeitung personenbezogener Daten **MUSS** dokumentiert sein. Die Zwecke **MÜSSEN** in der App durch betroffene Personen jederzeit einsehbar sein.
Anforderung 44: Wird eine Zweckänderung der Verarbeitung der personenbezogenen Daten angestrebt, **MUSS** hierfür eine Erlaubnisnorm (Einwilligung des Betroffenen oder gesetzlicher Erlaubnistatbestand) existieren.
Anforderung 45: Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, **DÜRFEN NICHT** einer Zweckänderung unterzogen werden.
Anforderung 46: Personenbezogene oder personenbeziehbare Daten, die zu unterschiedlichen Zwecken erhoben wurden, **MÜSSEN** getrennt verarbeitet werden.
Anforderung 47: Betroffene Personen **MÜSSEN** bei einer Zweckänderung vor Beginn der Verarbeitung informiert werden.

- **Datenminimierung** (Art. 5 Abs. 1 lit. c DS-GVO):
  Die Verarbeitung personenbezogener Daten muss für den verfolgten Zweck *erforderlich* und *angemessen* sein. Erforderlich ist die Verarbeitung personenbezogener Daten nur dann, wenn ohne diese Datenverarbeitung der verfolgte Zweck nicht erreicht werden kann. D. h. die Daten sind für die Erreichung der verfolgten Zwecke unverzichtbar.
  Angemessenheit liegt vor, wenn es zu der Verarbeitung kein „milderes“ Mittel gibt, welches weniger in die Rechte und Freiheiten natürlicher Personen eingreift.
  Datenminimierung beinhaltet daher keine Beschränkung der absoluten Datenmenge, es kann durchaus die Verarbeitung einer sehr großen Menge personenbezogener Daten erforderlich und angemessen sein. Andererseits müssen ggf. Daten entfernt werden, wenn diese nicht benötigt werden wie beispielsweise GPS-Koordinaten aus Aufnahmen mit der Kamera eines mobilen Gerätes.

Anforderung 48: Die Erhebung und Verarbeitung von personenbezogenen Daten **MUSS** sich an den Prinzipien der Datenvermeidung und Datensparsamkeit orientieren.

Anforderung 49: Um die Sparsamkeit der Datenerhebung bzw.- verarbeitung durch Aufsichtsbehörden, betroffene Personen oder andere überprüfen zu können, **MUSS** der Verwendungszweck jedes Datums bzw. jeder Datenkategorie beschrieben sein.

Anforderung 50: Daten, die keinen zur Erfüllung der Aufgabe definierten Verwendungszweck haben, **DÜRFEN NICHT** verarbeitet werden.

Anforderung 51: Werden durch Verwendung von im mobilen Gerät eingebauten Aufnahmegeräten, wie beispielsweise einer Kamera, oder mit dem mobilen Gerät verbundenen Aufnahmegeräten wie beispielsweise eine Waage oder einem Blutdruckmessgerät Daten erhoben, **MÜSSEN** für die Verarbeitung nicht erforderliche Daten bzw. Metadaten wie beispielsweise GPS-Daten gelöscht werden.

- **Richtigkeit** (Art. 5 Abs. 1 lit. d DS-GVO):
  Die Daten müssen für die Dauer der Verarbeitung, die von der Erhebung der Daten bis zu deren Löschung andauert („Lebenszyklus“ der Daten), sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.
  Es müssen alle „angemessenen“ Maßnahmen getroffen werden, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.
  Während eine Berichtigung falscher Daten immer erfolgen muss, ist eine Aktualisierung der Daten nur erforderlich, wenn die Aktualisierung für die Verarbeitung der Daten erforderlich ist. Wenn ein Patient vor zwei Jahren in Behandlung war und dieser Patient heute nach zwei Jahren umzieht, so liegt kein falsches Datum vor, denn zum Zeitpunkt der Behandlung stimmte die Adresse. Daher ist eine Korrektur nicht erforderlich. Kommt dieser Patient jedoch zur erneuten Behandlung ins Krankenhaus, so muss die neue Adresse erfasst werden.

Anforderung 52: Es **MUSS** gewährleistet sein, dass nur richtige Daten verarbeitet werden. Soweit erforderlich **MÜSSEN** Daten aktuell gehalten werden. Änderungen **SOLLTEN** nachvollziehbar sein.

Anforderung 53: Eine App **MUSS** Daten bei Eingabe auf Validität wie auch Konsistenz prüfen. Ungültige Werte **MÜSSEN** erkannt und eine Verarbeitung verhindert werden.

Anforderung 54: Die App **MUSS** betroffenen Personen die Möglichkeit bieten, gespeicherte Daten zu korrigieren und zu aktualisieren.

- **Speicherbegrenzung** (Art. 5 Abs. 1 lit. e DS-GVO):
  Personenbezogene Daten dürfen nur so lange in einer die Identifizierung der betroffenen Personen erlaubenden Form gespeichert werden, wie es für die erfolgten Zwecke erforderlich ist.
  Dabei erlauben auch pseudonymisierte Daten die Identifizierung einer Person. Art. 5 Abs. 1 lit. e DS-GVO verlangt also, dass personenbezogene Daten schnellstmöglich gelöscht oder anonymisiert werden. D. h. entweder direkt nach Zweckerreichung oder nach Ablauf der gesetzlichen Aufbewahrungspflichten, wenn diese für die Verarbeitung bestehen, muss die Anonymisierung oder Löschung erfolgen.
  Erfolgt die Verarbeitung ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke, so dürfen diese Daten länger gespeichert werden, wenn geeignete technische und organisatorische Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen durchgeführt werden. Dies beinhaltet insbesondere, dass das Verarbeitungsverfahren gemäß den Vorgaben von Art. 25 DS-GVO (s. Kap. 9.5.2.1) entwickelt und durchgeführt wird.

Dies setzt voraus, dass die Speicherdauer differenziert nach Zwecken festgelegt wird, damit der betroffenen Person gegenüber transparent dargestellt werden kann, wann welche Daten gelöscht werden.

Anforderung 55: Die Dauer der Speicherung personenbezogener Daten **MUSS** anhand der gesetzlichen Vorgaben festgelegt werden. Im Falle einer Einwilligung als Rechtsgrundlage richtet sich die Speicherdauer nach dem Verwendungszweck, Daten **MÜSSEN** spätestens beim Widerruf der Einwilligung gelöscht werden.

Anforderung 56: Die Speicherdauer **MUSS** dem Benutzer mitgeteilt werden.

Anforderung 57: Ist die Angabe eines Datums bzgl. der Speicherdauer nicht möglich, so **MÜSSEN** die Kriterien für die Festlegung dieser Dauer dem Benutzer in einer verständlichen Form mitgeteilt werden.

Anforderung 58: Daten, deren Speicherfrist abgelaufen ist, **MÜSSEN** schnellstmöglich gelöscht werden.

Beispiel 1: Bei einer App, bei welcher die Rechtsgrundlage der Verarbeitung personenbezogener Daten auf der Einwilligung einer betroffenen Person beruht, sind Daten nach Erreichen des Zweckes zu löschen, ebenso, wenn die Einwilligung widerrufen wird. (Siehe Abbildung 1)

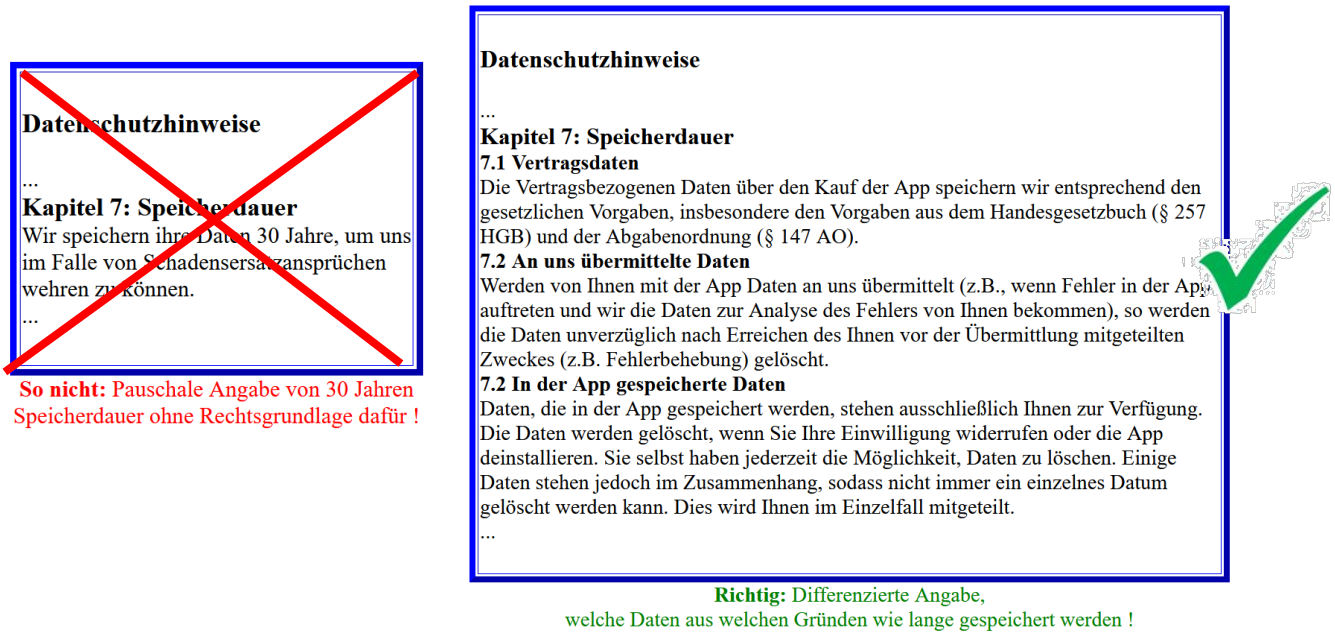

Abbildung 1: Information des Benutzers über Speicherdauer

- **Integrität und Vertraulichkeit** (Art. 5 Abs. 1 lit. f DS-GVO):
  Bei jeder Verarbeitung muss die Integrität der Daten sowie der Schutz vor unbefugter Kenntnisnahme und Verarbeitung gewährleistet werden. Dies wird insbesondere durch die Umsetzung der Anforderungen von Art. 32 DS-GVO („Sicherheit personenbezogener Daten“) gewährleistet.

Anforderung 59: Der Verantwortliche **MUSS** den Schutzbedarf der zu verarbeitenden Daten festlegen. Die Festlegung **MUSS** dokumentiert werden.

Anforderung 60: Alle Personen[61], welche auf die gespeicherten Gesundheitsdaten zugreifen können, **MÜSSEN** vor dem erstmaligen Zugriff auf die Wahrung des Datengeheimnisses verpflichtet worden sein.

Anforderung 61: Alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten tätigen Personen **MÜSSEN** vor Verarbeitungsbeginn dazu verpflichtet worden sein, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren.[62] Weiterhin **MÜSSEN** sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt worden sein.

Art. 5 Abs. 2 DS-GVO verlangt, dass die Einhaltung dieser Grundsätze nachgewiesen werden muss. D. h. bei jeder Verarbeitung besteht eine Rechenschaftspflicht, welche die Erfüllung aller Anforderungen der DS-GVO umfasst. In jeder App muss dementsprechend eine entsprechende Dokumentation möglich sein, idealerweise unterstützt durch eine entsprechende Protokollierung. Damit Protokolle Aussagen bzgl. eines zeitlichen Zusammenhangs abbilden können, muss die Zeitangabe im Protokoll auch die tatsächliche Zeit widerspiegeln, was nur durch eine regelmäßige Synchronisation auf Basis der koordinierten Weltzeit[63] (UTC) gewährleistet werden kann.

Anforderung 62: Es **SOLLTE** ein Protokollierungskonzept existieren.[64]

Anforderung 63: Die Systemzeit **MUSS** regelmäßig mit einer zuverlässigen externen Zeitnormale-Quelle auf Basis der UTC synchronisiert werden.

Anforderung 64: Es **MUSS** protokolliert werden, wer wann auf welche personenbezogenen oder personenbeziehbaren Daten mit welcher Berechtigung zugegriffen hat.

Anforderung 65: Es **MUSS** protokolliert werden, wer wann welche personenbezogenen oder personenbeziehbaren Daten mit welcher Berechtigung exportiert oder ausgedruckt hat. Zu jedem Datenexport oder Ausdruck **MUSS** die Eingabe einer Begründung möglich sein, damit nachvollziehbar und überprüfbar ist, zu welchem Zweck ein Datenexport oder ein Ausdruck erfolgte.

Anforderung 66: Enthalten Protokolle personenbezogene oder personenbeziehbare Daten, so **MÜSSEN** diese Protokolle vor jeglicher Verarbeitung außer zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes durch technische und organisatorische Mittel geschützt werden.

[61] Die betroffene Person, also z. B. Patient/-in, selbst ist von einer Pflicht zur Verschwiegenheit natürlich ausgenommen; betroffene Personen dürfen im Rahmen gesetzlicher Vorgaben insbesondere Einschränkungen ihre persönlichen Geheimnisse jederzeit offenbaren – oder halt auch nicht.

[62] Hierzu kann beispielsweise das Muster aus dem Anhang des Papiers der Verbände bitkom, DKG, bvitg, Bundeszahnärztekammer und Hartmannbund verwendet werden. Online, zitiert am 2022-09-02; verfügbar unter https://www.bitkom.org/Bitkom/Publikationen/Muster-zur-Umsetzung-des-Gesetzes-zur-Neuregelung-des-Schutzes-von-Geheimnissen-bei-der-Mitwirkung-Dritter-an-der-Berufsausuebung-schweigepflichtiger-Personen.html bzw. pdf-Datei unter https://www.bitkom.org/sites/main/files/file/import/20180718-Muster-203StGB-final.pdf

[63] Siehe auch entsprechende Informationsseite der Physikalisch-Technische Bundesanstalt. Online, zitiert am 2022-07-20; verfügbar unter https://www.ptb.de/cms/ptb/fachabteilungen/abt4/fb-44/ag-441/darstellung-der-gesetzlichen-zeit/koordinierte-weltzeitskala-utc.html

[64] Bzgl. Erstellung siehe z. B. GMDS, GDD, bvitg: Leitfaden für die Erstellung von Löschkonzepten im Gesundheitswesen. Stand: 20. Juni 2020. Online, zitiert am 2022-06-24; verfügbar unter https://gesundheitsdatenschutz.org/html/loeschkonzept.php

Anforderung 67: Protokolle **MÜSSEN** eine zeitliche Zuordnung gewährleisten. Dies **SOLLTE** über Zeitstempel oder über eine Versionierung, welche eine zeitliche Zuordnung ermöglicht, erfolgen.

Anforderung 68: Änderungen am Protokoll **MÜSSEN** jederzeit nachvollziehbar sein. D. h. es **MUSS** neben dem ursprünglichen Inhalt erkennbar sein, wann Änderungen erfolgten.

Anforderung 69: Die Aufbewahrungsdauer für Protokolldaten **MUSS** schriftlich festgelegt werden.

Anforderung 70: Die Begründung für die Festlegung der Aufbewahrungsdauer **MUSS** schriftlich festgehalten werden, sodass Dritte die Begründung nachvollziehen können.

9.2 Rechtsgrundlage der Verarbeitung

Die DS-GVO unterscheidet zwischen „normalen" Daten sowie Daten, die zu den in Art. 9 Abs. 1 DS-GVO genannten besonderen Kategorien gehören. Zu diesen Daten der besonderen Kategorien gehören:

- Rassische und ethnische Herkunft,
- Politische Meinungen,
- Religiöse oder weltanschauliche Überzeugungen,
- Gewerkschaftszugehörigkeit,
- **Genetische Daten,**
- **Biometrische Daten zur eindeutigen Identifizierung** einer natürlichen Person,
- **Gesundheitsdaten**,
- **Daten zum Sexualleben** oder der **sexuellen Orientierung** einer natürlichen Person.

Neben medizinischen Informationen gehören zu den besonderen Kategorien von Daten also auch biometrische Informationen wie Fingerprint oder Fotografien, wenn Letztere zur eindeutigen Identifikation genutzt werden können, wie es beispielsweise bei der Gesichtserkennung erfolgt.

Die Verarbeitung der besonderen Kategorien von Daten ist laut Art. 9 Abs. 1 DS-GVO grundsätzlich verboten! Die Verarbeitung ist nur statthaft, wenn ein gesetzlicher Erlaubnistatbestand vorhanden ist.

Anforderung 71: Für die Verarbeitung **MUSS** ein Erlaubnistatbestand zur Verarbeitung der personenbezogenen bzw. personenbeziehbaren Daten vorliegen.

Auch die Einwilligung einer betroffenen Person ist ein entsprechender gesetzlicher Erlaubnistatbestand, im Rahmen von mobilen Apps in der Regel auch der einzige mögliche Erlaubnistatbestand.

9.2.1 Einwilligung

Gemäß Art. 9 Abs. 2 lit. a DS-GVO ist eine Verarbeitung besonderer Kategorien personenbezogener Daten gestattet, wenn

a) die betroffene Person ausdrücklich für einen oder mehrere Zwecke einwilligt und
b) Unionsrecht oder das Recht von Mitgliedstaaten die Verarbeitung nicht verbieten.

Für eine wirksame Einwilligung müssen die Vorgaben der DS-GVO eingehalten werden. Näheres zur rechtskonformen Einwilligung findet sich z. B. in der Praxishilfe „Die datenschutzrechtliche Einwilligung: Freund (nicht nur) des Forschers[65].

Auch für eine Einwilligung gilt die in Art. 5 Abs. 1 lit. a DS-GVO verankerte Transparenzpflicht. Wird innerhalb einer App mehr als eine Einwilligung eingeholt, sollte in der App daher in den Datenschutz-

[65] GMDS, GDD: Die datenschutzrechtliche Einwilligung: Freund (nicht nur) des Forschers. Stand der Bearbeitung: 30. April 2021. Online, zitiert am 2022-06-24; verfügbar unter https://gesundheitsdatenschutz.org/html/einwilligung.php

Einstellungen auch eine Auflistung aller gegebenen Einwilligungen vorhanden sein, inklusive der Möglichkeit, jede der einzeln abgegebenen Einwilligungen auch einzeln widerrufen zu können.

Anforderung 72: Beim ersten Aufruf einer App **MUSS** zuerst der Status der Einwilligung geprüft werden.

Anforderung 73: Liegt eine Information zu Einwilligungen, z. B. in Form eines Cookies, vor, **MUSS** diese beachtet werden. Liegt keine Information zu Einwilligungen vor, **MUSS** die informierte, ausdrückliche Einwilligung eingeholt werden. Wird eine Einwilligung abgefragt **MUSS** gleichzeitig die Möglichkeit der Ablehnung angeboten werden. Die Sichtbarkeit und die Möglichkeit der Auswahl **MÜSSEN** für beide Optionen (Zustimmen / Ablehnen) gleichwertig sein.

Anforderung 74: Ist eine Nutzung der App für nicht einwilligungsfähige Kinder und/oder Jugendliche (i. d. R, also jünger als 16 Jahre) nicht ausgeschlossen, **MUSS** für diese eine Nutzung nur mit Einwilligung der jeweiligen Erziehungsberechtigten möglich sein.

Anforderung 75: Die Aufklärung vor Abgabe einer Einwilligung **MUSS** die Möglichkeit eines jederzeitigen Widerrufs der Einwilligung beinhalten und **MUSS** ebenfalls auf die möglichen Folgen eines Widerrufs hinweisen.

Anforderung 76: Eine App **MUSS** in den Datenschutz-Einstellungen anzeigen, welche Einwilligungen für welche Zwecke erteilt wurden. Bei Abgabe mehrerer Einwilligungen **MUSS** jede Einwilligung in den Datenschutz-Einstellungen auch einzeln widerrufbar sein.

Anforderung 77: Bei der Einbettung von zusätzlichen Funktionen Dritter (wie z. B. Karten) **MUSS** sichergestellt sein, dass durch die Einbettung der Funktionen in die eigene App erst dann Daten übertragen oder abgerufen werden, wenn eine Einwilligung vorliegt.

Die Beweislast, dass für die Verarbeitung der personenbezogenen Daten eine Einwilligung vorgelegen hat bzw. immer noch vorliegt, liegt beim Verantwortlichen. Ebenfalls muss nachgewiesen werden, dass alle Anforderungen an eine Einwilligung vorgelegen haben, insbesondere natürlich:

- Freiwilligkeit
  D. h., die Einwilligung wurde ohne Zwang abgegeben, es existierte mindestens eine „echte“ Alternativmöglichkeit (ErwGr. 42 beachten: „[…] wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“)

Beispiel 2: Existieren keine Alternativen, so ist eine Einwilligung niemals freiwillig. Bieten Sie den Download nur an, wenn Anwender ihre Daten an Google weitergeben, so ist dies niemals als rechtlich gültige Einwilligung aufzufassen. Damit hier eine Einwilligung angenommen werden kann, sind Alternativen erforderlich. (Siehe auch Abbildung 2)

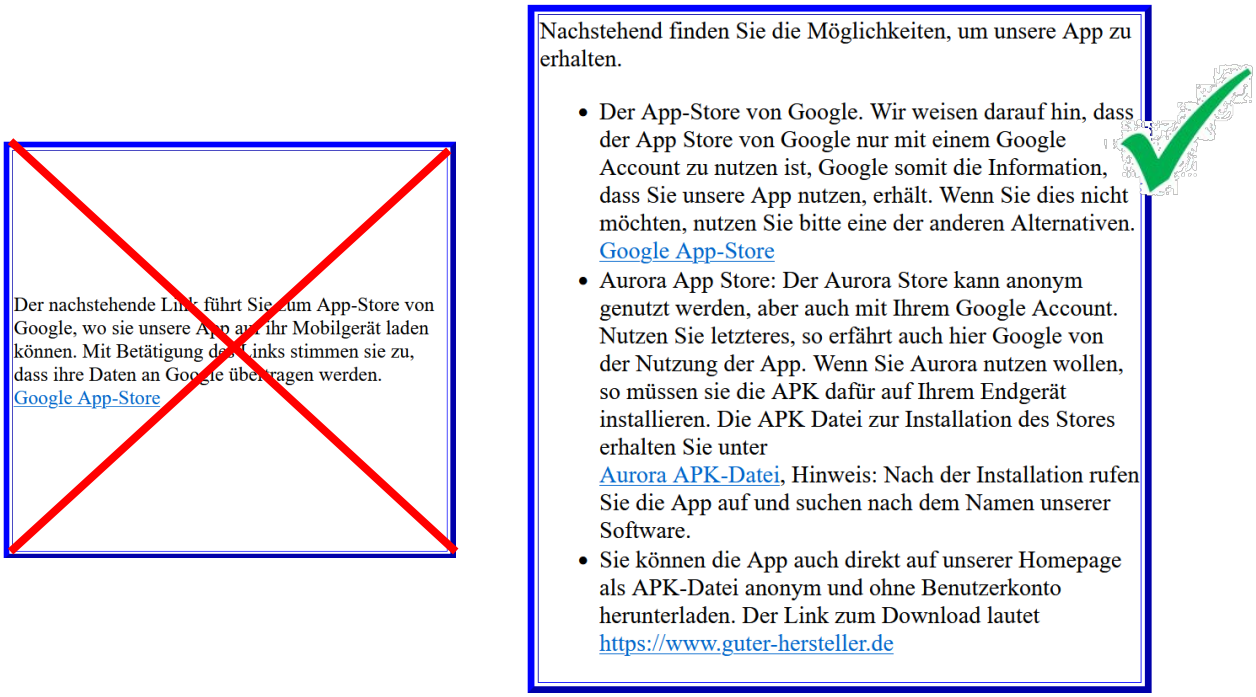

Abbildung 2: Beispiel für ein Alternativangebot zur Gewährleistung der Freiwilligkeit der Einwilligung

- Für <u>den</u> bestimmten Fall (= Zweckbindung)
  Entsprechend Art. 4 Nr. 11 DS-GVO muss eine Einwilligung für den bestimmten Fall abgegeben werden, was immer beinhaltet, dass der betroffenen Person der Zweck der Verarbeitung ihrer Daten vor Abgabe der Einwilligung bekannt sein muss.

  Beispiel 3: Eine App, welche einem Benutzer die nächstgelegene Arztpraxis anzeigt, braucht hierfür i. d. R. Zugriff auf die Geolokalisierung des mobilen Gerätes, dies muss dem Anwender entsprechend erklärt werden. Auch der Zweck für die Nutzung von Kontakt- und Bankdaten muss erläutert werden (Siehe Abbildung 3)

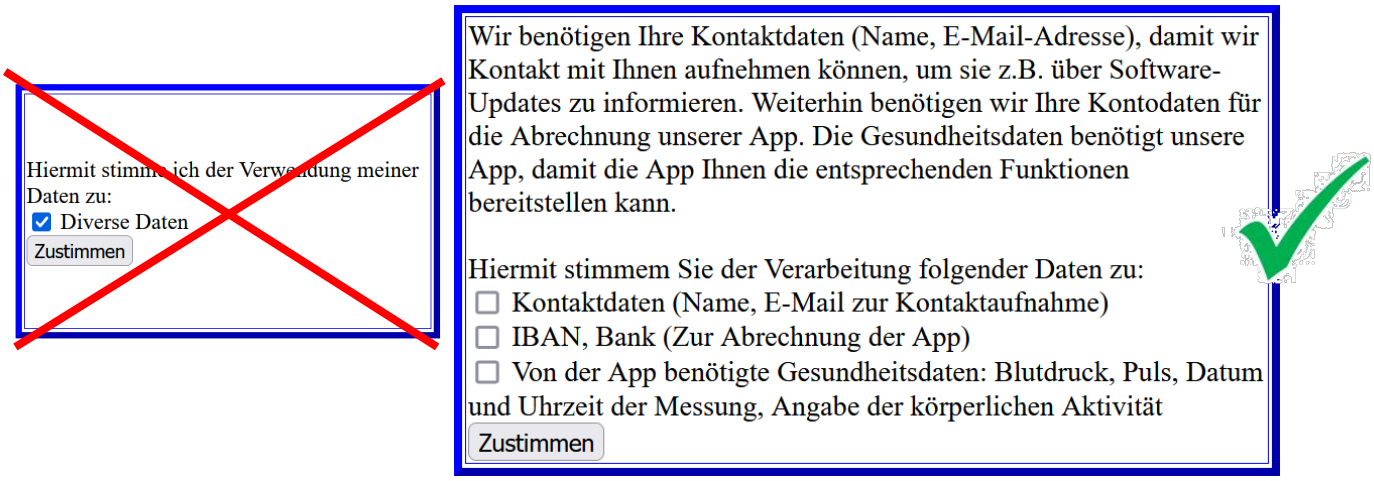

Abbildung 3: Beispiel für die Informierung des Verarbeitungszweckes von Daten bei der Einholung einer Einwilligung

- Informiertheit
  Die Einwilligung muss in Kenntnis der Sachlage erteilt werden. Dies beinhaltet natürlich auch alle Informationen nach Art. 13 bzw. Art. 14 DS-GVO.

Beispiel 4: Vor einer Einwilligung muss es für den Nutzer möglich sein, alle benötigten Informationen einsehen zu können. Dies schließt insbesondere Datenschutzhinweise und Allgemeine Geschäftsbedingungen mit ein. Dabei muss der ggf. kleine Bildschirm eines mobilen Gerätes bedacht werden, der evtl. eine tatsächliche Kenntnisnahme insbesondere von umfangreicheren Dokumenten mit mehreren Seiten verhindert. (Siehe Abbildung 4)

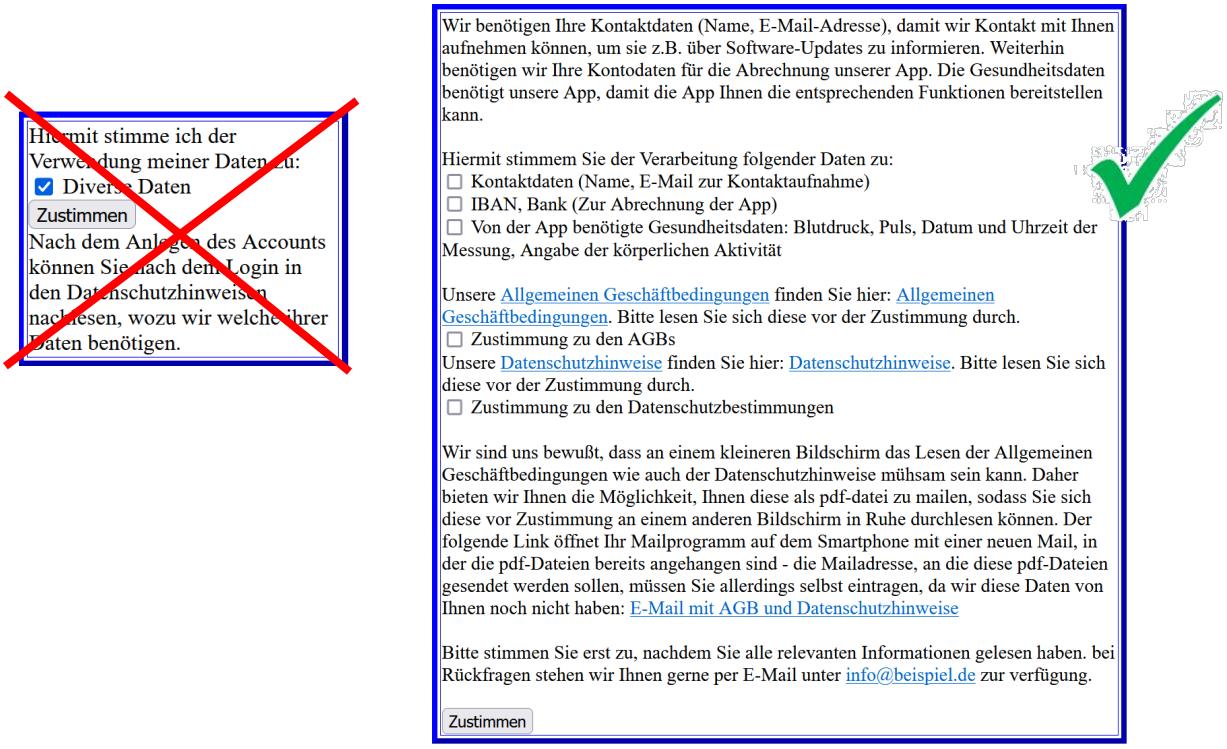

Abbildung 4: Beispiel für die Möglichkeit, Informationen vor Abgabe der Einwilligung zur Verfügung zu stellen

- Es muss sich um eine unmissverständlich abgegebene Willensbekundung handeln, also in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung geschehen.
- Bei Gesundheitsdaten zu beachten: Es ist eine ausdrückliche Willenserklärung erforderlich.

Beispiel 5: In einem Einwilligungsformular sind vorausgefüllte Felder grundsätzlich nicht rechtswirksam. Jede Einwilligung bedarf einer bestätigenden Handlung, d. h. die betroffene Person muss immer selbst ein Kreuz setzen oder eben nicht. (Siehe Abbildung 5)

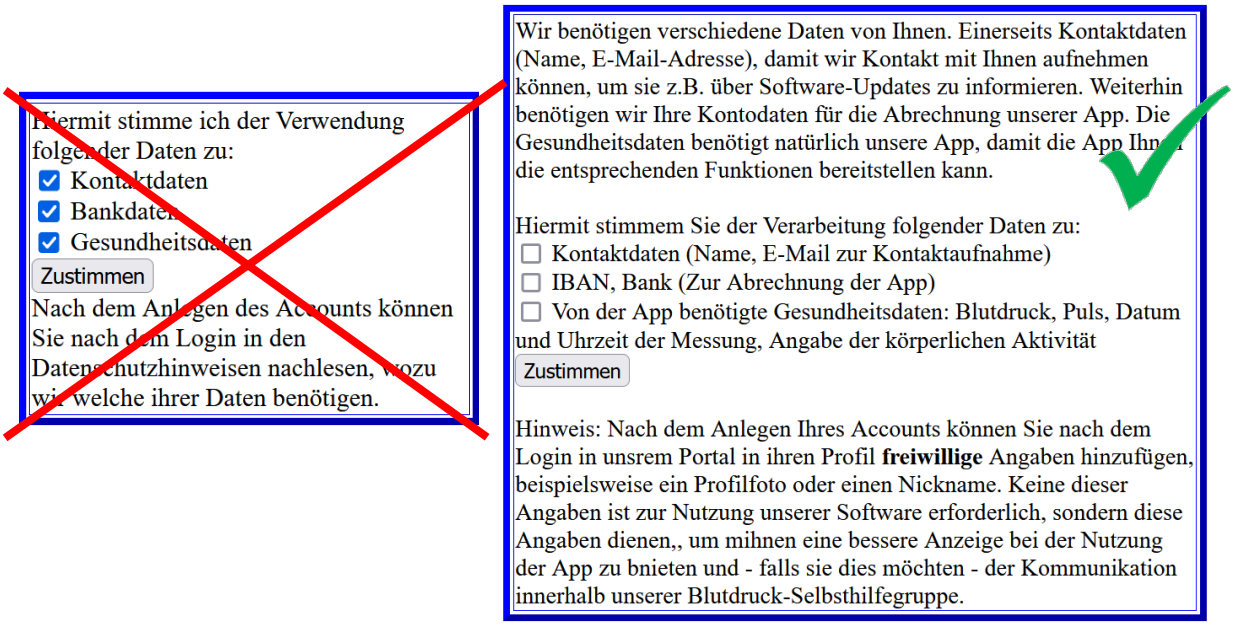

Abbildung 5: Beispiel für Ausdrücklichkeit bei Einholung einer Einwilligung

Der Verantwortliche muss gemäß Art. 7 Abs. 1 DS-GVO dabei nachweisen können, dass für die Verarbeitung eine rechtsgültige Einwilligung vorgelegen hat bzw. immer noch vorliegt.

Anforderung 78: Wird die Einwilligung des Betroffenen elektronisch eingeholt, so **MUSS** der Vorgang protokolliert werden und der Inhalt der Einwilligung für den Betroffenen jederzeit abrufbar sein.

Hinweis 5: Grundsätzlich ist zu beachten: Auch eine Einwilligung kann keine übermäßige oder unverhältnismäßige Datenverarbeitung legitimieren.[66]

Da die Einwilligung in der Regel die Rechtsgrundlage für eine Verarbeitung in medizinischen mobilen Apps darstellt, findet sich in Anhang 1: eine Checkliste zur Einwilligung, welche aus der Praxishilfe „EU DS-GVO: Anforderungen an eine Einwilligung“[65] stammt.

9.2.1.1 Die datenschutzrechtliche Aufklärung

Eine datenschutzrechtlich wirksame Einwilligung erfordert eine entsprechende Aufklärung, d. h. bedarf einer vollständigen Information, wer zu welchem Zweck wann und wo welche Daten zu verarbeiten beabsichtigt. Auch die an der Datenverarbeitung Beteiligten und die Speicherdauer sind von Bedeutung. Erst nach einer umfassenden Aufklärung kann der Patient um die Einwilligung gebeten werden, diesem Verfahren zuzustimmen.

Anforderung 79: Vor der Erteilung der Einwilligung zur Verarbeitung der personenbezogenen Daten **MÜSSEN** den betroffenen Personen alle erforderlichen Informationen bereitgestellt werden. Dazu gehören insbesondere auch alle Informationen nach Art. 13 bzw. Art. 14 DS-GVO.

[66] Artikel-29-Datenschutzgruppe: Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten vom 27. Februar 2013. Online, zitiert am 2022-06-24; verfügbar unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_de.pdf

9.2.1.2 *Möglichkeit eines Widerrufes*

Betroffenen Personen muss bekannt gemacht werden, dass jederzeit das Recht auf Widerruf einer gegebenen Einwilligung besteht. Diesbezüglich gilt es der betroffenen Person auch aufzuzeigen, welche Konsequenzen ein Widerruf hat. Mögliche Konsequenzen im Rahmen medizinischer Apps könnten beispielsweise sein, dass bestimmte Funktionen nicht oder nur eingeschränkt zur Verfügung stehen oder die Ergebnisse oder Auswertungen aus den Apps eine geringere Aussagekraft erhalten bzw. sogar völlig falsche Ergebnisse resultieren können.

Weiterhin muss der Widerruf so einfach wie die Einwilligung selbst sein. D. h. in einer App muss ein einfacher Vorgang zum Widerruf integriert sein, sodass der Widerruf entsprechend einfach gestaltet wird. Eine gute Möglichkeit ist hier eine prominente Position im Dialog „Einstellungen der App“.

Anforderung 80: Eine Einwilligung **MUSS** für den Betroffenen jederzeit mit Wirkung für die Zukunft temporär oder permanent widerrufbar sein.

Anforderung 81: Der Widerruf **MUSS** mindestens so einfach sein wie die Erteilung der Einwilligung. Dies bedeutet insbesondere, es **MUSS** möglich sein, auch in der App die erteilte Einwilligung zu widerrufen, wenn die Einwilligung über die App erteilt wurde.

Beispiel 6: Wird die Einwilligung über die App eingeholt, so muss auch der Widerruf über die App möglich sein und der Nutzer darauf hingewiesen werden. Aber parallel zum Widerruf in der App kann man auch andere Möglichkeiten anbieten. (Siehe)

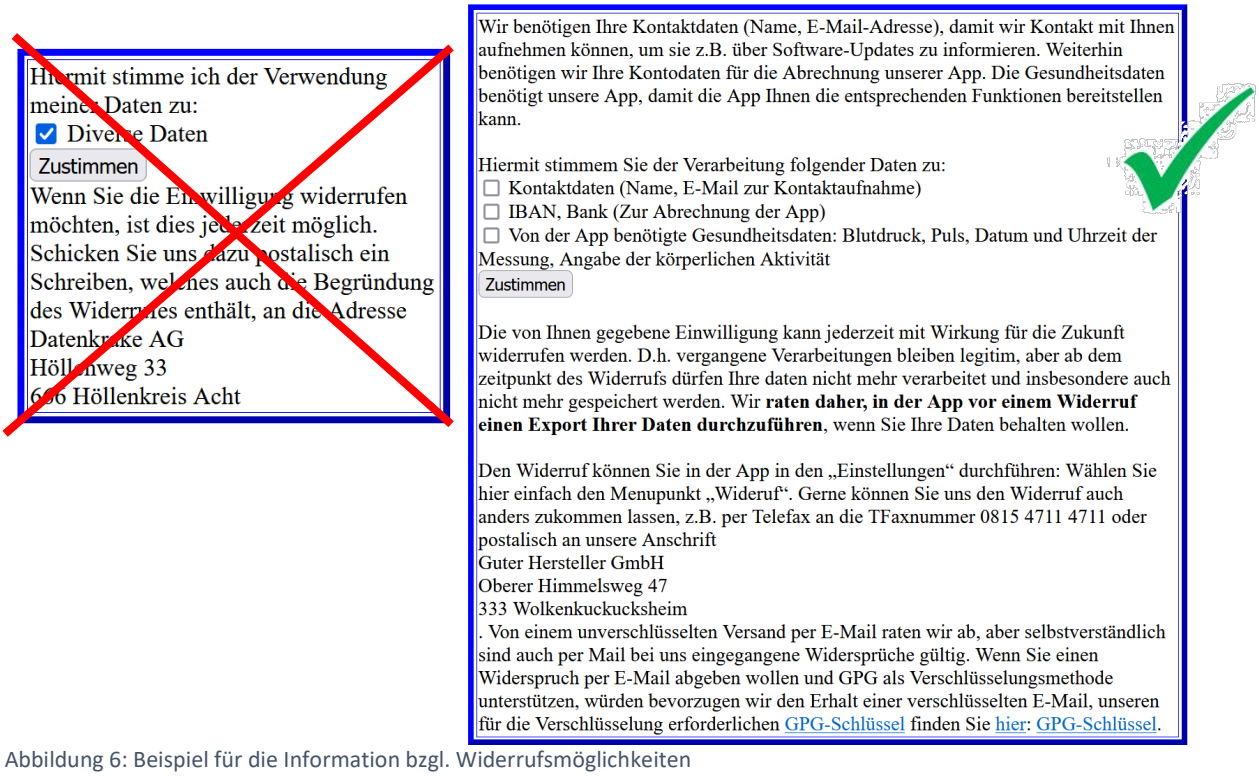

Abbildung 6: Beispiel für die Information bzgl. Widerrufsmöglichkeiten

9.2.2 Zweckänderung aufgrund einer Interessensabwägung

Art. 6 Abs. 1 lit. f DS-GVO erlaubt eine Verarbeitung personenbezogener Daten, wenn

a) dies „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich“ ist, und
b) die überwiegenden „Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person“ stehen einer Verarbeitung nicht entgegen.

Grundsätzlich darf gemäß Art. 6 Abs. 1 lit. f DS-GVO also ein Verantwortlicher, ein Auftragsverarbeiter oder ein Dritter personenbezogene Daten verarbeiten, wenn ein überwiegendes Interesse an der Verarbeitung nachgewiesen werden kann.

Aber: Die Verarbeitung der in Art. 9 Abs. 1 DS-GVO genannten besonderen Datenkategorien wie Gesundheitsdaten, biometrischen oder genetischen Daten ist grundsätzlich verboten, außer ein in Art. 9 Abs. 2 DS-GVO genannter Erlaubnistatbestand liegt vor. Somit **stellt Art. 6 Abs. 1 lit. f DS-GVO keinen Erlaubnistatbestand zur Verarbeitung** der in Art. 9 Abs. 1 DS-GVO genannten Datenkategorien **dar**, eine zweckändernde Verarbeitung wie beispielsweise die Nutzung der personenbezogenen Daten von App-Anwendern zu Werbezwecken kann somit nicht durch Art. 6 Abs. 1 lit. f DS-GVO legitimiert werden.

Entsprechend Art. 9 Abs. 4 DS-GVO können Mitgliedstaaten der EU zusätzliche Bedingungen für die Verarbeitung besonderer Kategorien von Daten betroffener Personen einführen oder aufrechterhalten, jedoch nur, „soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist“. Deutschland führte zusätzliche Regelungen für die Verarbeitung zu anderen Zwecken ein:

1) § 24 Abs. 1 Ziff. 1 BDSG erlaubt die Verarbeitung personenbezogener Daten zu anderen Zwecken, wenn diese Verarbeitung zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist; dies wird regelhaft für keine Verarbeitung durch Hersteller einer App oder andere Personen, welche keine staatlichen Aufgaben wie beispielsweise die Bundeswehr oder Polizei wahrnehmen, anwendbar sein.
2) § 24 Abs. 1 Ziff. 2 BDSG erlaubt die Verarbeitung personenbezogener Daten zu anderen Zwecken, wenn diese zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen. Somit können ggf. personenbezogene Daten in Gerichtsprozessen, wenn Ansprüche gegenüber einer betroffenen Person durchgesetzt werden sollen, genutzt werden.
3) § 27 Abs. 1 BDSG erlaubt die Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken sowie zu statistischen Zwecken, wenn die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung *erheblich* überwiegen.

Eine **Nutzung personenbezogener Daten der besonderen Kategorie** von App-Anwendern **aufgrund einer Interessensabwägung ist** somit – ein nachgewiesenes **erhebliches überwiegendes Interesse vorausgesetzt** – **ausschließlich zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken** sowie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche **möglich**. Jegliche Verarbeitung personenbezogener genetischer, biometrischer oder Gesundheitsdaten zu anderen Zwecken, insbesondere zu Zwecken der Werbung, bedarf einer anderen Rechtsgrundlage als einer Interessensabwägung. In der Regel wird hierfür die ausdrückliche Einwilligung der jeweils betroffenen Person erforderlich sein.

Anforderung 82: Genetische, biometrische oder Gesundheitsdaten aus medizinischen Apps **DÜRFEN NICHT** aufgrund einer Interessensabwägung zu anderen Zwecken wie beispielsweise Werbung genutzt werden.

Anforderung 83: Genetische, biometrische oder Gesundheitsdaten **KÖNNEN** bei *erheblich* überwiegendem Interesse des datenschutzrechtlich Verantwortlichen gegenüber dem Interesse betroffener Personen an der Nicht-Verarbeitung dieser Daten zu Zwecken der wissenschaftlichen Forschung verarbeitet werden.

Hinweis 6: Bzgl. Werbung ist insbesondere zu beachten, dass auch Medizinprodukte vom Heilmittelwerbegesetz[67] erfasst werden.

9.3 Erlaubnistatbestände abseits der Einwilligung

Art. 9 Abs. 2 DS-GVO kennt neben der Einwilligung noch weitere Erlaubnistatbestände, dazu gehören insbesondere:

- Ausübung von aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte durch einen Verantwortlichen oder einer betroffenen Person (Art. 9 Abs. 2 lit. b DS-GVO)
- Verarbeitung ist zum Schutz lebenswichtiger Interessen einer natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben (Art. 9 Abs. 2 lit. c DS-GVO)
- Verarbeitung erfolgt durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten, wobei
    1. geeigneter Garantien zur Wahrung der Rechte und Freiheiten betroffener Personen sind vorhanden,
    2. es sind ausschließlich Informationen von Mitgliedern oder ehemaligen Mitgliedern der Organisation oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, betroffen
    3. und die personenbezogenen Daten werden nicht ohne Einwilligung nach außen offengelegt

  (Art. 9 Abs. 2 lit. d DS-GVO)
- Es werden ausschließlich Daten verarbeitet, welche die betroffene Person offensichtlich öffentlich gemacht hat (Art. 9 Abs. 22 lit. e DS-GVO)
- Die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich (Art. 9 Abs. 2 lit. f DS-GVO)
- Verarbeitung ist für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich erforderlich und
    1. Die Verarbeitung beruht auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats
    2. oder erfolgt aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs

  (Art. 9 Abs. 2 lit. h DS-GVO)
- Die Verarbeitung ist für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich und
    1. die Verarbeitung erfolgt auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, welches
        a) in angemessenem Verhältnis zu dem verfolgten Ziel steht,
        b) den Wesensgehalt des Rechts auf Datenschutz wahrt und
        c) angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht

  (Art. 9 Abs. 2 lit. j DS-GVO)

[67] Gesetz über die Werbung auf dem Gebiet des Heilwesens (Heilmittelwerbegesetz - HWG). Online, zitiert am 2022-08-02; verfügbar unter https://www.gesetze-im-internet.de/heilmwerbg/index.html

Grundsätzlich besteht zwischen App-Anbieter und betroffener Person zwar ein Vertrag, jedoch ist dies in der Regel kein Behandlungsvertrag, sodass bzgl. der Argumentation hinsichtlich Vertragserfüllung Art. 9 Abs. 2 lit. h DS-GVO nicht angewendet werden kann. In **seltenen Ausnahmen**, wo eine App die Behandlung durch einen professionellen Anbieter von Gesundheitsdienstleistern wie beispielsweise Ärzten unterstützt, kann der Behandlungsvertrag auch die Verarbeitung von Patientendaten in einer App legitimieren.

Auch im Rahmen der medizinischen Forschung kann eine App bzw. die Verarbeitung personenbezogener Daten von Probanden ggf. durch ein nationales deutsches Recht, welches den Anforderungen von Art. 9 Abs. 2 lit. j DS-GVO genügt, legitimiert werden.

In den allermeisten Fällen wird eine Einwilligung aber die einzige Möglichkeit zur Legitimierung der Verarbeitung personenbezogener Daten in einer App, insbesondere der in Art. 9 Abs. 1 DS-GVO genannten besonderen Kategorien von Daten darstellen.

9.4 Gewährleistung der Betroffenenrechte

Die Betroffenenrechte sind datenschutzrechtlich im Kapitel III der DS-GVO (Artikel 12 bis 22) festgelegt. Im Überblick handelt es sich um folgende Rechte des Betroffenen bzw. Pflichten gegenüber dem Betroffenen:

- Informationspflicht bei Erhebung bzw. Zweckänderung von personenbezogenen Daten, unterschieden nach:
  - Erhebung bei der betroffenen Person
  - Erhebung nicht bei der betroffenen Person („Dritterhebung“)
- Auskunftsrecht der betroffenen Person
- Recht auf Berichtigung
- Recht auf Löschung
- Recht auf Einschränkung der Verarbeitung
- Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Beschränkung der Zulässigkeit automatisierter Entscheidungen im Einzelfall.

Entsprechend Art. 12 Abs. 1 DS-GVO muss der Verantwortliche geeignete Maßnahmen treffen, um diesen Pflichten nachzukommen. D. h., es muss in jeder App die Möglichkeit vorhanden sein, dass jeder Verantwortliche den Verpflichtungen gegenüber betroffenen Personen hinsichtlich dieser Rechte nachkommen kann.

9.4.1 Informationspflichten

Jede App muss den aus Art. 13 und Art. 14 DS-GVO resultierenden Informationspflichten genügen, d. h. vor, spätestens bei Erhebung der personenbezogenen Daten sind betroffenen Personen die notwendigen Angaben entsprechend Art. 13 bzw. Art. 14 DS-GVO zur Verfügung zu stellen. Die Informationen müssen dabei stets in einer klaren und einfachen Sprache vermittelt werden, wie es Art. 12 DS-GVO fordert.

Die folgenden Anforderungen weisen nicht alle in Art. 13 und Art. 14 DS-GVO geforderten Informationen in einer separaten Anforderung aus, sondern nur diejenigen, die zusätzlich ausgelegt werden.

Anforderung 84: Jede App **MUSS** individuelle, auf die App spezifisch zugeschnittene Datenschutzhinweise beinhalten.

Anforderung 85: Datenschutzhinweise **MÜSSEN** alle in Artikel 13, 14 der Datenschutz-Grundverordnung genannten Informationen beinhalten. Dazu gehört auch, dass betroffene Personen über die Zwecke der Verarbeitung, die verarbeiteten Daten, und die Verarbeitung selbst informiert werden **MÜSSEN**.

Anforderung 86: Nutzt die Anwendung von Dritten bereitgestellte Softwarebibliotheken, Frameworks oder ähnliche Softwareprodukte, **MÜSSEN** die Datenschutzhinweise hierüber informieren. Die Information **MUSS** betroffene Personen insbesondere darüber informieren, wie der Hersteller der App gewährleistet, dass die Anbieter dieser eingesetzten Software-Produkte keinerlei Zugriff auf personenbezogene Daten erhalten können.

Anforderung 87: Die Datenschutzhinweise **MÜSSEN** insbesondere auch eine Beschreibung der getroffenen Maßnahmen zur Sicherheit der Verarbeitung in allgemein verständlicher Form beinhalten.

Anforderung 88: Datenschutzhinweise **MÜSSEN** jederzeit in der App abrufbar sein, auch ohne vorherige Anmeldung.

Anforderung 89: Datenschutzhinweise **MÜSSEN** unmittelbar von der Startseite der App aus aufrufbar bzw. erreichbar sein.

Anforderung 90: Es **MUSS** sichergestellt werden, dass die Datenschutzhinweise nicht durch Pop-Ups oder andere visuelle Elemente verdeckt werden.

Anforderung 91: Im Falle der Änderung der Datenschutzhinweise **MUSS** dem Nutzer dies vorher bekannt gegeben und die Möglichkeit des Widerrufs gegebener Einwilligungen angeboten werden.

Anforderung 92: Datenschutzhinweise **MÜSSEN** mit maximal zwei Klicks von der Startseite der App aus erreichbar und als Datenschutzhinweise gekennzeichnet sein.

Anforderung 93: Der Zweck der Datenerhebung **MUSS** dem Nutzer bei der ersten Nutzung sofort kenntlich gemacht und **MUSS** in den Datenschutzhinweisen dokumentiert werden.

Anforderung 94: Die Speicherung von Informationen **MUSS** in den Datenschutzhinweisen zusammen mit der Speicherdauer und dem Zweck der Speicherung erläutert werden. Dies gilt für alle Informationen unabhängig vom Zweck.

Anforderung 95: Bei An- bzw. Abwahlmöglichkeiten (Opt-In / Opt-Out) in Bezug auf Datenschutzeinstellungen **MUSS** der Nutzer eindeutig erkennen können, ob die jeweilige Funktion an- oder ausgeschaltet ist. Dies **MUSS** durch einen eindeutigen Beschreibungstext erfolgen. Bei Schiebeschaltern **MUSS**, um die Barrierefreiheit zu gewährleisten, eine eindeutige Beschriftung erfolgen.

Anforderung 96: Beim ersten Start der App nach erfolgter Installation der Anwendung:
- **MUSS** der Nutzer nach seiner Zustimmung zu Verarbeitungen, die ein Opt-In erfordern, gefragt werden und
- **SOLLTE** der Nutzer über Verarbeitungen, zu denen es ein Opt-Out gibt, über diese Möglichkeit sowie der Handhabung dieser Widerspruchsmöglichkeit informiert werden.

9.4.2 Auskunftsrecht

Jede betroffene Person hat das Recht auf Auskunft bzgl. der über ihn verarbeiteten bzw. gespeicherten Daten. Auf dieses Recht muss auch im Rahmen der im Abschnitt 9.4.1 genannten Informationspflicht hingewiesen werden. Idealerweise wird bei der Information bzgl. des Rechts auf Auskunft auch eine Telefonnummer wie auch eine spezielle nicht-personalisierte E-Mail-Adresse angegeben, sodass Anfragen auch bei einem Personalwechsel richtig ankommen.

Nach Art. 15 Abs. 3 DS-GVO muss der Verantwortliche betroffenen Personen auch eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung stellen. Apps müssen daher auch eine entsprechende Funktionalität bereitstellen bzw. der Anbieter/Hersteller einer App muss entsprechende Prozesse etabliert haben, um dieses Betroffenenrecht erfüllen zu können.

Anforderung 97: Der Betroffene **MUSS** die Möglichkeit haben, jederzeit Einblick in alle zu seiner Person gespeicherten Daten zu erhalten. Dies umfasst auch die Möglichkeit, Änderungen seiner gespeicherten Daten nachzuvollziehen.

Anforderung 98: Der Betroffene **MUSS** die Möglichkeit haben, eine Kopie seiner Daten zu erhalten. Dies **KANN** als Ausdruck oder einen für die jeweilige betroffene Person verwertbaren elektronischen Export aller zu seiner Person gespeicherten Daten umgesetzt werden.

9.4.3 Recht auf Berichtigung

Nach Art. 16 DS-GVO hat jede betroffene Person das Recht, dass unrichtige Daten berichtigt werden. Da Daten die Grundlage jeder medizinischen Behandlung und Forschung darstellen, liegt die Korrektur unrichtiger Daten selbstverständlich auch im ureigenen Interesse der die Daten verarbeitenden Stelle.

Allerdings hat nach Art. 16 DS-GVO jeder Patient auch das Recht, dass unvollständige Daten vervollständigt werden, ggf. auch mittels einer ergänzenden Erklärung. Hier kann es zu unterschiedlichen Interpretationen seitens des Verantwortlichen und der betroffenen Person bzgl. der Interpretation von „unvollständig“ kommen. Der europäische Gesetzgeber verlangt daher, dass dieses Recht „unter Berücksichtigung der Zwecke der Verarbeitung“ zu erfolgen hat. D. h. die Beurteilung bzgl. Unvollständigkeit muss aus Sicht des Verarbeitungszweckes erfolgen.

Jeder Patient muss im Rahmen der Informationspflicht (siehe Kapitel 9.4.1) darauf hingewiesen werden, dass für ihn diese Rechte bestehen.

Anforderung 99: Es **MUSS** eine Möglichkeit geben, auf Aufforderung des Betroffenen Daten zu seiner Person zu korrigieren.

Anforderung 100: Es **MUSS** eine geeignete Funktion vorhanden sein, welche es Betroffenen ermöglicht, die zu ihrer Person erhobenen und/oder verarbeiteten personenbezogenen Daten zu aktualisieren oder zu ergänzen.

Anforderung 101: Es **MUSS** protokolliert werden, wer wann welche Daten eines Betroffenen auf dessen Wunsch änderte. Die Protokollierung **MUSS** einen Zeitstempel, eindeutige ID der ändernden Person sowie die geänderten Daten umfassen. Es **SOLLTE** die Eingabe der Begründung „Änderung erfolgte auf Wunsch des Betroffenen“ möglich sein.

Anforderung 102: Wurden Daten vom Betreiber der Datenaustauschplattform an andere Stellen übermittelt, so **SOLLTE**, sofern zumutbar, diese Stellen über erfolgte Berichtigungen informiert werden, sofern diese Benachrichtigung im Interesse des Betroffenen liegt.

9.4.4 Recht auf Einschränkung der Verarbeitung („Sperrung“)

Gemäß Art. 18 DS-GVO hat jeder Patient das Recht, unter den Voraussetzungen von Art. 18 Abs. 1 DS-GVO von dem Verantwortlichen die Einschränkung der Verarbeitung (= „Sperrung“) zu verlangen. Auch auf dieses Recht muss im Rahmen der Informationspflicht (siehe Kapitel 9.4.1) hingewiesen werden. Zugleich sollte er darauf hingewiesen werden, dass dieses Recht ggf. durch gesetzliche Bestimmungen eingeschränkt wird.

Der Verantwortliche muss dabei beachten, dass gemäß Art. 18 Abs. 2 DS-GVO eine derartige Sperrung nur mit Einwilligung der betroffenen Person rückgängig gemacht werden darf. Ansonsten darf eine Verarbeitung, von einer Speicherung abgesehen, nur

- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder

- zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder
- aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats

erfolgen. Weiterhin muss der Verantwortliche entsprechend den Vorgaben von Art. 18 Abs. 3 DS-GVO die betroffene Person, die eine Sperrung erwirkte, unterrichten, bevor die Einschränkung aufgehoben wird.

Anforderung 103: In der App **MUSS** eine Möglichkeit vorhanden sein, um personenbezogene Daten mit einer Markierung „gesperrt" zu versehen. Eine weitere Verarbeitung von als gesperrt markierten Daten **DARF NICHT** erfolgen.

Anforderung 104: Eine Sperrung **DARF NICHT** aufgehoben werden, ohne die betroffene Person zuvor zu informieren.

9.4.5 Recht auf Löschung

Nach Art. 17 DS-GVO hat jede betroffene Person das Recht, dass sie betreffende Daten gelöscht werden, wenn die Umstände aus Art. 17 Abs. 1 DS-GVO zutreffen und die Ausnahmetatbestände aus Art. 17 Abs. 3 DS-GVO nicht anzuwenden sind. Über dieses Recht ist jede betroffene Person im Rahmen der Informationspflicht (siehe Kapitel 9.4.1) ebenfalls zu informieren. Zugleich sollte darauf hingewiesen werden, dass dieses Recht ggf. durch gesetzliche Bestimmungen wie z. B. durch die Vorgabe gesetzlicher Aufbewahrungsfristen eingeschränkt wird.

Anforderung 105: Ein Informationssystem **MUSS** einem Verantwortlichen eine Möglichkeit bzw. Funktion bieten, damit der Verantwortliche nicht mehr benötigte Daten resp. zu löschende Daten identifizieren kann.

Anforderung 106: Es **MUSS** eine Löschfunktion implementiert werden, welche eine Rekonstruktion gelöschter Informationen ausschließt.

Anforderung 107: Es **SOLLTE** eine Möglichkeit geben, damit Verantwortliche eine Anonymisierung als Löschfunktion nutzen können. Das Ergebnis einer Anonymisierung **MUSS** nachweisbar keine Re-Identifikation bzw. De-Anonymisierung erlauben.

Anforderung 108: Es **MUSS** in einem Löschkonzept[68] festgelegt werden, wann welche Daten zu löschen sind.

Anforderung 109: Liegt keine gesetzliche Grundlage zur Speicherung der Daten vor, **MÜSSEN** die Daten auf Anweisung des Betroffenen unverzüglich gelöscht werden.

Anforderung 110: Entfällt der Verwendungszweck und es liegt keine gesetzliche Grundlage zur Speicherung der Daten vor, **MÜSSEN** die Daten unverzüglich gelöscht werden.

Anforderung 111: Unverschlüsselte Datenträger **MÜSSEN** aus Sicherheitsgründen vor deren Wiederverwendung datenschutzgerecht gelöscht werden. Die Formatierung ist als sicheres Löschverfahren ungeeignet.

Anforderung 112: Vor einer Weitergabe von Datenträgern an externe Stellen zur datenschutzgerechten Entsorgung **MÜSSEN** Datenträger vor der Übergabe an die externe Stelle datenschutzgerecht gelöscht werden.

Anforderung 113: Die Löschung der Daten **MUSS** unter Angabe des Löschgrunds sowie des Anwenders, der die Löschung vornahm, protokolliert werden.

Anforderung 114: Die Deinstallation einer App **MUSS** so gestaltet sein, dass vertrauliche Nutzerdaten und zugehörige anwendungsspezifische Informationen aus der

[68] Bzgl. Erstellung siehe z. B. GMDS, GDD, bvitg: Leitfaden für die Erstellung von Löschkonzepten im Gesundheitswesen. Stand: 20. Juni 2020. Online, zitiert am 2022-06-24; verfügbar unter https://gesundheitsdatenschutz.org/html/loeschkonzept.php

Laufzeitumgebung, vom Endgerät, aus Sicherheitsmodulen und von anderen Speichermedien gelöscht werden.

9.4.6 Widerspruchsrecht

Nach Art. 21 Abs. 6 DS-GVO hat jede betroffene Person das Recht, aus Gründen, „die sich aus ihrer besonderen Situation ergeben“, einer Verarbeitung der sie betreffenden Daten zu widersprechen. Entsprechend Art. 21 Abs. 4 DS-GVO muss jede betroffene Person ausdrücklich auf dieses Recht hingewiesen werden, d. h. auch auf dieses Recht ist im Rahmen der Informationspflicht (siehe Kapitel 9.4.1) hinzuweisen.

Dabei ist zu berücksichtigen, dass auch darauf hingewiesen wird, dass ein Widerspruchsrecht ggf. durch gesetzliche Regelungen eingeschränkt wird, z. B. eine Speicherung aufgrund gesetzlicher Bestimmungen trotz seines Widerspruchs erfolgen muss.

9.4.7 Recht auf Datenübertragbarkeit

Gemäß Art. 20 DS-GVO hat jeder Patient unter den Voraussetzungen von Art. 20 Abs. 1 lit. a, b DS-GVO das Recht, von ihm bereitgestellte Daten

- vom Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten

sowie

- sie einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln bzw. sie übermitteln zu lassen.

Jede betroffene Person ist im Rahmen der Informationspflicht (siehe Kapitel 9.4.1) über dieses Recht zu informieren. Es sollte dabei aber auch darauf hingewiesen werden, dass kein Empfänger dieser Daten gesetzlich dazu verpflichtet ist, diese Daten überhaupt oder in dem vom Verantwortlichen bereitgestellten Format anzunehmen.

App-Entwickler sollten sich daher schon bei der Konzeption einer App überlegen, wie die Spezifikation hinsichtlich dieser Anforderung aussehen könnte.

Anforderung 115: Die App **MUSS** der betroffenen Person die Möglichkeit bieten, ihre Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu exportieren.

Anforderung 116: Die App **SOLLTE** der betroffenen Person die Möglichkeit bieten, ihre Daten zu einem anderen Anbieter respektive zu einer anderen App oder einer elektronischen Plattform wie beispielsweise einer elektronischen Patientenakte zu übertragen.

Anforderung 117: Sind Schnittstellen im System vorhanden, welche dem Datenimport oder -export dienen, **MÜSSEN** diese Schnittstelle dokumentiert sein.

Anforderung 118: Werden Daten an Dritte weitergegeben, so **MUSS** entweder eine gesetzliche Grundlage hierfür vorhanden sein oder die betroffene Person der Weitergabe zugestimmt haben.

Anforderung 119: Die Rechtmäßigkeit der Übermittlung von Daten ins Ausland **MUSS** vor der Übermittlung geprüft worden sein.

Anforderung 120: Erfolgt eine Übermittlung in ein Drittland, also außerhalb des EWR, so **MUSS** hierbei ein der EU angemessenes Datenschutzniveau beim Datenimporteur garantiert sein.

Anforderung 121: Ist die Rechtmäßigkeit einer Übermittlung nicht eindeutig sichergestellt, **MUSS** die Übermittlung verhindert werden.

9.4.8 Profilbildung / automatisierte Einzelfallentscheidung

Gemäß Art. 22 Abs. 1 DS-GVO dürfen betroffene Personen nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen werden, welche der betroffenen Person gegenüber eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen kann. Eine Ausnahme besteht entsprechend Art. 22 Abs. 2 DS-GVO, wenn die Entscheidung

- für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
- aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
- mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

Bei der Verarbeitung von Daten der besonderen Kategorien wie Gesundheitsdaten, genetischen oder biometrischen Daten ist jedoch immer die ausdrückliche Einwilligung der betroffenen Person erforderlich; die zweite Möglichkeit (Art. 9 Abs. 2 lit. g DS-GVO) ist im Umfeld der hier besprochenen Szenarien regelhaft nicht anwendbar.

Möchten App-Hersteller oder App-Betreiber daher Daten zu Zwecken wie der Reichweitenmessung, einer Optimierung der bedarfsgerechten Weiterentwicklung der App oder Ähnlichem verarbeiten und dazu Profile von Anwendern verwenden, so ist hierzu immer die ausdrückliche Einwilligung der betroffenen Personen erforderlich.

Anforderung 122: Eine automatisierte Einzelfallentscheidung mit rechtlichen oder ähnlichen Auswirkungen für die betroffene Person **DARF** in der App **NICHT** erfolgen. Jede entsprechende Entscheidung **MUSS** durch einen Menschen erfolgen.

Anforderung 123: Die Erstellung von Profilen und deren Auswertung zum Zwecke der bedarfsgerechten Gestaltung, der Reichweitenmessung, der Marktforschung der App oder zu ähnlichen Zwecken **MUSS** auf Basis einer ausdrücklichen Einwilligung (Opt-In) erfolgen und die Verarbeitung inkl. der Profilbildung in den Datenschutzhinweisen beschrieben werden.

Anforderung 124: Vor einer Zusammenführung eines Profils mit weiteren Daten des Nutzers **MUSS** der Nutzer in die Zusammenführung einwilligen (Opt-In). Die Zusammenführung **MUSS** in den Datenschutzhinweisen mit dem konkreten Verarbeitungszweck und der konkreten Speicherdauer erläutert werden.

Anforderung 125: Vor der Aufzeichnung und Auswertung von geräteübergreifenden Nutzungsverhaltens in der App **MUSS** die ausdrückliche Einwilligung (Opt-In) des Nutzers eingeholt werden. Die Verarbeitung **MUSS** in den Datenschutzhinweisen unter Angabe des konkreten Verarbeitungszwecks sowie der konkreten Speicherdauer genannt werden. Macht der Nutzer von seinem Widerrufsrecht Gebrauch, so **MUSS** die Aufzeichnung unverzüglich gestoppt und die vorhandenen Daten gelöscht werden.

Anforderung 126: Der Nutzer **MUSS** die Möglichkeit haben, sich die Tracking-Daten vor dem Versand anzeigen zu lassen.

Anforderung 127: Für eine Analyse des Nutzerverhaltens (einschließlich Geolokalisierung) auf der Basis vollständiger IP-Adressen **MUSS** eine ausdrückliche Einwilligung durch den Nutzer erfolgen (Opt-In). Die Verarbeitung **MUSS** in den Datenschutzhinweisen erläutert werden.

9.5 Sicherheit der Verarbeitung

Art. 5 Abs. 1 lit. f DS-GVO verlangt, dass personenbezogene Daten nur „in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich

Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen“. Um den angemessenen Schutz festlegen zu können, müssen der Schutzbedarf der Daten und das Risiko der Verarbeitung bestimmt werden.

Hinsichtlich der Bewertung des Schutzbedarfs enthält ErwGr. 91 DS-GVO die Aussage, dass insbesondere die Sensibilität der Daten die Wahrscheinlichkeit eines „hohen“ Risikos vermuten lässt, sodass bei einer Verarbeitung der in Art. 9 Abs. 1 DS-GVO genannten besonderen Kategorien von Daten grundsätzlich von einem hohen oder sogar sehr hohen Schutzbedarf auszugehen ist. D. h. bei der Verarbeitung sensibler Daten wie Gesundheitsdaten, genetischen Daten wie auch biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person ist immer von einem hohen Risiko und dementsprechend von einem hohen Schutzbedarf auszugehen.

Jede Verarbeitung personenbezogener Daten beinhaltet grundsätzlich ein Risiko für die betroffene Person, deren Daten verarbeitet werden. Die Risiken müssen dabei aus Sicht der betroffenen Person betrachtet werden: Relevant ist, welche Risiken für die betroffene Person existieren. In Deutschland werden häufig nur materielle Risiken (Finanzen, Gesundheit, ...) betrachtet, was u. a. an unserer zivilrechtlichen Rechtsprechung bzgl. Haftung liegt. Europarechtlich sind aber auch immaterielle Risiken zu betrachten, beispielsweise, wenn eine unbefugte Offenbarung von Geheimnissen Betroffenheit oder ein Schamgefühl bei der betroffenen Person auslöst oder eine Diskriminierung / Stigmatisierung zur Folge hat. ErwGr. 75 und 83 DS-GVO führen beispielhaft verschiedene Risiken auf. Entsprechend ErwGr. 83 ist es unerheblich, ob die Risiken aus einer beabsichtigten, einer unbeabsichtigten oder auch einer unrechtmäßigen Handlung resultieren, daher müssen bei der Entwicklung einer App hinsichtlich der Gewährleistung der IT-Sicherheit immer auch fehlerhafte oder unbeabsichtigte Handlungen berücksichtigt werden.

9.5.1 IT-Sicherheit

Art. 1 Abs. 1 DS-GVO beschreibt, dass die DS-GVO insbesondere dem „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“ dient. Hierzu verfolgt die DS-GVO einen Risiko-orientierten Ansatz: Art. 32 DS-GVO fordert nicht die Gewährleistung des höchstmöglichen Niveaus hinsichtlich der Sicherheit der Verarbeitung, sondern es muss ein *angemessenes* Schutzniveau sichergestellt werden.

Art. 32 DS-GVO schreibt vor, dass unter Berücksichtigung

- des Stands der Technik,
- der Implementierungskosten,
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten

geeignete technische und organisatorische Maßnahmen getroffen werden müssen, um ein dem *Risiko angemessenes Schutzniveau* zu gewährleisten. Diese Maßnahmen schließen u. a. Folgendes ein (Art. 32 Abs. 1 DS-GVO):

- Pseudonymisierung personenbezogener Daten
- Verschlüsselung personenbezogener Daten
- Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten
- Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Aufgrund dieser Vorgabe in Art. 32 DS-GVO muss daher nachvollziehbar begründet werden, wenn eine der in Art. 32 DS-GVO genannten Maßnahmen wie beispielsweise Verschlüsselung nicht genutzt wird.

Anforderung 128: Es **MUSS** ein dem Risiko angemessenes Schutzniveau gewährleistet werden. Hierzu MUSS ein Risikomanagementsystem vorhanden sein, in welchem u. a. alle betrachteten sowie aufgetretenen Risiken sowie die Maßnahmen zur Risikobehandlung dokumentiert sind.

Anforderung 129: Es **MUSS** geprüft werden, ob eine Pseudonymisierung genutzt werden kann, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Ist eine Pseudonymisierung nicht einsetzbar, **MUSS** begründet werden, warum dies nicht der Fall ist.

Anforderung 130: Im Falle einer Pseudonymisierung **MÜSSEN** technische und organisatorische Maßnahmen vorhanden sein, die gewährleisten, dass die verarbeiteten personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden können.

Anforderung 131: Es **MUSS** geprüft werden, ob eine Verschlüsselung genutzt werden kann, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Ist eine Verschlüsselung nicht einsetzbar, **MUSS** begründet werden, warum dies nicht der Fall ist.

Anforderung 132: Personenbezogene sowie personenbeziehbare Daten **SOLLEN** auf einem mobilen Gerät nur verschlüsselt gespeichert werden. Bei Speicherung auf einem externen Speichergerät wie einer SD- oder microSD-Karte **MÜSSEN** Daten verschlüsselt gespeichert werden. Die Verschlüsselung dieser Daten **MUSS** mit einem von einem Anwender erzeugten und nur diesem bekannten Schlüssel erfolgen.

Anforderung 133: Die Übertragung personenbezogener oder personenbeziehbarer Gesundheitsdaten zwischen Clients und Servern wie auch zwischen Servern selbst **MUSS** entsprechend dem jeweiligen Stand der Technik generell verschlüsselt erfolgen.

Verantwortlich für die Gewährleistung der Sicherheit der Verarbeitung ist nach Art. 32 DS-GVO sowohl der für die Verarbeitung Verantwortliche als auch – sofern vorhanden – der Auftragsverarbeiter. Letzterer natürlich nur für den Teil, den der Auftragsverarbeiter zu verantworten hat. Aus Art. 5 DS-GVO folgt eine Nachweispflicht, die aber indirekt auch von Art. 32 Abs. 3 DS-GVO verlangt wird.

Weiterhin verlangt die DS-GVO, dass dieser dem Risiko der Verarbeitung angemessene Schutz auf Dauer sicherzustellen ist. D. h. die

- Vertraulichkeit,
- Integrität,
- Verfügbarkeit und
- Belastbarkeit

für Systeme und Dienste im Zusammenhang mit der Verarbeitung der personenbezogenen Daten ist für den gesamten Lebenszeitraum zu gewährleisten.

Anforderung 134: Es **MUSS** ein Berechtigungs- und Rollenkonzept erstellt und gepflegt werden, aus dem eindeutig abzulesen ist, wer welche Rolle (funktionell und strukturell) und damit verbundene Rechte bzgl. des Datenzugriffs hat.

Anforderung 135: Bzgl. der Rollen- und Rechtevergabe im Berechtigungs- und Rollenkonzept **MUSS** das Need-to-know-Prinzip angewendet werden.

Anforderung 136: Im Berechtigungs- und Rollenkonzept **MUSS** beschrieben sein, welche Funktionsrollen nicht miteinander vereinbar sind und somit nicht von einer Person gleichzeitig

wahrgenommen werden dürfen. Es **MÜSSEN** technische und organisatorische Maßnahmen getroffen werden, um diese Trennung sicherzustellen.

Anforderung 137: Eine Kombination von Rollen bzw. Zugriffsrechten für eine Person, welche der Person mehr Rechte auf Datenzugriffe erteilt, als für ihre Aufgabe nötig ist, **MUSS** durch technische und organisatorische Maßnahmen verhindert werden.

Anforderung 138: Im Berechtigungskonzept **MUSS** festgelegt werden, wer aufgrund welcher Geschehnisse auf Protokolldaten zugreifen darf.

Anforderung 139: Die App **MUSS** dem Nutzer eine Möglichkeit bieten, sich über in der Vergangenheit liegende erfolgreiche durchgeführte und erfolglos versuchte Anmeldevorgänge zu informieren. Die Zeitspanne, über den derartige Anmeldevorgänge angezeigt werden, **SOLLTE** vom Nutzer konfigurierbar sein.

Anforderung 140: Die App **MUSS** nach einer vom Nutzer auswählbaren, angemessenen Zeitspanne, in welcher die App nicht verwendet wurde (idle time), eine erneute Authentisierung erfordern, bevor ein Zugriff auf sensible Daten möglich ist.

Anforderung 141: Von Dritten bereitgestellte Softwarebibliotheken, Frameworks oder ähnliche Softwareprodukte **MÜSSEN** vor ihrer Verwendung hinsichtlich der Gewährleistung einer sicheren Verarbeitung geprüft werden. Die Prüfung und das Ergebnis **MÜSSEN** dokumentiert werden.

Anforderung 142: Nutzt die Anwendung von Dritten bereitgestellte Softwarebibliotheken, Frameworks oder ähnliche Softwareprodukte, **MÜSSEN** ungenutzte Funktionen von eingesetzter Drittanbieter-Software deaktiviert werden. Es **MUSS** sichergestellt sein, dass diese ungenutzten Funktionen durch Dritte nicht aktiviert werden können.

Anforderung 143: Nutzt die Anwendung von Dritten bereitgestellte Softwarebibliotheken, Frameworks oder ähnliche Softwareprodukte, **MÜSSEN** diese von Drittanbietern bereitgestellte und genutzte Software in der aktuell verfügbaren stabilen (stable) Version verwendet werden, experimentelle Versionen **DÜRFEN NICHT** genutzt werden.

Anforderung 144: Nutzt die Anwendung von Dritten bereitgestellte Softwarebibliotheken, Frameworks oder ähnliche Softwareprodukte, **MÜSSEN** diese Software-Produkte durch den Hersteller der App regelmäßig auf Schwachstellen überprüft und bzgl. der Sicherheit bei der weiteren Nutzung beurteilt werden. Die Prüfung und die Beurteilung **MUSS** dokumentiert werden. Drittanbieter-Software mit bekannten Sicherheitslücken **DARF NICHT** eingesetzt werden, ggf. **MUSS** sogar ein Produktrückruf durchgeführt werden, wenn anders die Sicherheit der sensiblen Gesundheitsdaten nicht gewährleistet werden kann.

Anforderung 145: Zur Gewährleistung der Verfügbarkeit der Daten **MUSS** die Anwendung die Möglichkeit der Erstellung von Backups sowie die Wiederherstellung von Daten aus den Backup-Daten anbieten.

Anforderung 146: Werden Backup-Möglichkeiten des Betriebssystems und / oder Cloud-Backups verwendet, so **MÜSSEN** alle personenbezogenen Daten entsprechend dem Stand der Technik verschlüsselt sein. Es **MUSS** durch die Verschlüsselung vollkommen ausgeschlossen sein, dass weder Hersteller des Betriebssystems noch Cloud-Anbieter einen Zugriff auf die Daten haben können bzw. die Daten entschlüsseln können[69].

[69] Dies beinhaltet auch, dass das für die Entschlüsselung notwendige Geheimnis (also der Schlüssel) nicht in einer Cloud gespeichert werden darf, wenn der Cloud-Anbieter oder ein Dritter Zugriff darauf haben könnte. Cloud-Anbieter können beispielsweise bei virtuellen Maschinen einen Snapshot der virtuellen Maschine und so auch beispielsweise mittels Brute-Force-Attacken im BIOS einer virtuellen Maschine abgelegte Schlüssel zu erhalten. All diese Möglichkeiten eines Anbieters/Betreibers einer Cloud müssen berücksichtigt und durch entsprechende Schutzmaßnahmen ein Zugriff sicher ausgeschlossen werden.

Dabei müssen die Schutzmaßnahmen gegebenenfalls eine Pseudonymisierung und eine Verschlüsselung der personenbezogenen Daten beinhalten. Ferner muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen, welche die Sicherheit der Verarbeitung gewährleisten, existieren.

Wird Pseudonymisierung und / oder Verschlüsselung eingesetzt, so muss das Vorgehen, die eingesetzten Verfahren und die regelmäßige Überprüfung der Sicherheit der Verfahren in einem entsprechenden Konzept dargestellt werden.

Anforderung 147: Wird Pseudonymisierung in einer App eingesetzt, so **MUSS** das Verfahren der Pseudonymisierung in einem Pseudonymisierungskonzept beschrieben werden.

Anforderung 148: In dem Pseudonymisierungskonzept **MUSS** beschrieben werden, in welchen Abständen die eingesetzten Methoden der Pseudonymisierung auf ihre Sicherheit geprüft werden. Das Ergebnis der Prüfung, d. h. die Wahrscheinlichkeit der De-Pseudonymisierung, **MUSS** in einer Verfahrensbeschreibung festgehalten und Aufsichtsbehörden auf Nachfrage zur Verfügung gestellt werden.

Anforderung 149: Die zur Pseudonymisierung eingesetzte Verfremdungsmethode **MUSS** durch anerkannte Autoritäten wie Behörden[70] im Umfeld der IT-Sicherheit anerkannt sein. Die sichere Implementierung **MUSS** von entsprechend geschultem Fachpersonal, welches an der Implementierung nicht beteiligt war, geprüft werden.

Anforderung 150: Wird Verschlüsselung in einer App eingesetzt, so **MUSS** das Verfahren der Verschlüsselung in einem Verschlüsselungskonzept beschrieben werden. Für die Implementierung von kryptografischen Verfahren **SOLLTEN** nur etablierte und dem aktuellen Stand der Technik entsprechende Krypto-Bibliotheken genutzt werden.

Anforderung 151: Das Verschlüsselungskonzept **MUSS** u. a. den Lebenszyklus von kryptographischem Schlüsselmaterial beinhalten, inklusive der Darstellung, wann bzw. auch aus welchen Gründen Schlüssel / Zertifikate ablaufen sowie dem Umgang beim Ablauf von Schlüsseln / Zertifikaten.

Anforderung 152: Das Verschlüsselungskonzept **MUSS** insbesondere eine Darstellung der Gewährleistung einer sicheren Schlüsselerzeugung auf dem mobilen Endgerät beinhalten. Insbesondere **MUSS** der Schlüsselerzeugung eine qualitativ hochwertige Zufallszahlenquelle zugrunde liegen. Die Vertraulichkeit des Schlüsselmaterials **MUSS** während des gesamten Lebenszyklus der Verwendung der Schlüssel gewährleistet werden. Der Schlüssel **MUSS** geheim gehalten werden, nur der erzeugende Anwender darf diesen benutzen können. Insbesondere **DÜRFEN** Hersteller und Betreiber der App **NICHT** Zugriff auf Schlüssel und / oder zur Schlüsselerzeugung genutzter Zufallszahl haben.

Anforderung 153: Kryptographische Verfahren **SOLLTEN** in austauschbaren Modulen implementiert sein, damit im Falle einer nicht mehr einsetzbaren Bibliothek diese gegen eine andere ausgetaucht werden kann.

Anforderung 154: Im Verschlüsselungskonzept **MUSS** beschrieben werden, in welchen Abständen die eingesetzten Methoden der Verschlüsselung auf ihre Sicherheit geprüft werden. Das Ergebnis der Prüfung, d. h. die Wahrscheinlichkeit der Entschlüsselung der Daten, **MUSS** in einer Verfahrensbeschreibung festgehalten und Aufsichtsbehörden auf Nachfrage zur Verfügung gestellt werden.

[70] Z. B. US National Institute of Standards and Technology, European Union Agency for Network And Information Security oder Bundesamt für Sicherheit in der Informationstechnik

Eine ausführliche Darstellung der Thematik findet sich in der Praxishilfe[71] von bvitg und GMDS. Einige grundlegende Anforderungen, damit wenigstens ein stabiles Grundniveau bzgl. IT-Sicherheit gewährleistet werden kann, lauten:

- Existieren in einer Soft- oder Hardware Sicherheitslücken, so ist ein sicherer Betrieb nicht mehr möglich, bis die Sicherheitslücken behoben wurden oder die missbräuchliche Verwendung dieser Sicherheitslücken durch entsprechende Maßnahmen sicher verhindert wird.

Anforderung 155: Bekannt gewordene Schwachstellen in der Software oder Hardware des Systems **MÜSSEN** behoben oder gegen Missbrauch abgesichert werden. Dies gilt auch für von Dritten bereitgestellte Softwarebibliotheken, Frameworks oder ähnliche Softwareprodukte.

Anforderung 156: Ungeplante Programmabbrüche (Exceptions) **MÜSSEN** abgefangen und kontrolliert werden. Die App **MUSS** insbesondere bei einer Exception jegliche Zugriffe auf sensible Daten abbrechen und entsprechende Daten im Speicher löschen.

- Gleichermaßen dürfen IT-Komponenten, bei denen der Hersteller oder Dritte wie beispielsweise andere Entwickler insbesondere die Open Source Community keine Pflege und Wartung mehr leisten und somit auch Sicherheitslücken nicht geschlossen werden, nicht verwendet werden, wenn das System sicher betrieben werden soll.

Anforderung 157: Software-Komponenten, für die es keine Wartung oder Pflege durch den Lieferanten, Hersteller oder Entwickler gibt, **DÜRFEN NICHT** verwendet werden. Dies gilt auch für von Dritten bereitgestellte Softwarebibliotheken, Frameworks oder ähnliche Softwareprodukte.

- Grundsätzlich müssen die Rechte von Anwendern so weit wie möglich eingeschränkt werden. Ein Anwender/Benutzer einer App sollte nur auf die Daten zugreifen und die Funktionen nutzen können, die benötigt werden. Denn Anwendungen, die im Kontext des Anwenders laufen, haben i. d. R. dieselben Rechte, somit könnte Malware eigentlich nicht benötigte Rechte für Angriffe nutzen. Daher ist eine Einschränkung auf das erforderliche Maß aus Sicht der IT wünschenswert.

Anforderung 158: Die Berechtigungen von Benutzern und Anwendungen **MÜSSEN** auf ein für deren Aufgaben notwendiges Minimum reduziert werden.

- Ebenso gefährdet ein Vollzugriff auf Betriebssystem und Hardware eines Endgerätes die Sicherheit des Systems. Daher darf eine Anwendung, die nicht systemrelevante Änderungen durchführen muss, nicht im sog. „privilegierten“ Modus (= mit root-/Admin-Rechten) betrieben werden. Der Normalfall muss auch bei mobilen Anwendungen der Betrieb mit unprivilegierten Rechten sein.

Anforderung 159: Die Applikation **MUSS** mit unprivilegierten Benutzerrechten auskommen, um auf dem Endgerät lauffähig zu sein.

- Aber auch Zugriffe auf Daten durch fremde Anwendungen oder auch das Betriebssystem selbst gefährden die Sicherheit und Privatheit der Daten. Gerade unerwünschte Zugriffe des Betriebssystems können App-Entwickler nicht jederzeit verhindern. In diesen Fällen muss dies aber nachvollziehbar sein.

[71] bvitg, GMDS: Sicherheit personenbezogener Daten: Umgang mit Art. 32 DS-GVO. (2018) Online, zitiert am 2022-06-24; verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/sicherheit_verarbeitung.php

Anforderung 160: Verarbeitungen, die nicht durch die App erfolgen, **MÜSSEN** identifiziert und diese Zugriffe bzw. auch Zugriffsversuche inklusive der Daten(-arten) sowie eines Zeitstempels in einem Protokoll dokumentiert werden.

- Gerade medizinische Software-Anwendungen enthalten besonders sensible Informationen, nämlich die Gesundheitsdaten von Anwendern. Daher ist auch bei Endgeräten, die potenziell von mehreren Menschen parallel genutzt werden, zu gewährleisten, dass nur diejenigen Personen Zugriff auf die sensiblen Informationen bekommen, welche auch dazu berechtigt sind.

Anforderung 161: Die Nutzung von schutzbedürftigen Funktionen des Systems und der Zugriff auf vertrauliche Daten **DARF NICHT** ohne erfolgreiche Authentifizierung und Autorisierung möglich sein.

- Anwender agieren mit einem Software-System des Öfteren anders, als es sich die jeweiligen Software-Entwickler vorgestellt hatten. Daher kommt es eher regelhaft zu unerwarteten Eingaben in entsprechende Bildschirmmasken durch Anwender. Diese Eingaben werden entsprechend an das System übertragen und können, falls im Rahmen der Software-Entwicklung keine Vorsorge getroffen wurden, unerwartete Effekte auslösen – vom Absturz des Systems, ungültigen Daten oder Werte in Feldern bis hin zur unbefugten Offenbarung von Informationen könnte alles geschehen, je nach Gestaltung des Systems. Daher muss ein System gegen unerwartete Benutzereingaben, Weiten in Feldern usw. durch entsprechende Validierungsmaßnahme wie auch der Behandlung von auftretenden Fehlern in der Anwendung geschützt werden.

Anforderung 162: Das System **MUSS** robust gegen unerwartete Eingaben sein. Insbesondere **MÜSSEN** alle Eingaben validiert werden.

- Um Fehlbedienungen durch Anwender möglichst zu vermeiden und damit die Gefährdung der Daten zu minimieren, müssen Anwender vor Nutzung einer App geschult werden. Ein Hersteller einer medizinischen App muss daher immer eine deutschsprachige (bzw. bei Bereitstellung für andere Länder in der jeweiligen Landessprache) Bedienungsanleitung bereitstellen und den Anwendern der App einen leichten Zugang zur Bedienungsanleitung ermöglichen. Idealerweise bietet die App ergänzend zur Bedienungsanleitung eine kurze Einführung in die Bedienung an.

Anforderung 163: Der Hersteller einer App **MUSS** eine deutschsprachige Bedienungsanleitung bereitstellen, die so detailliert und so verständlich ist, dass durch Studieren der Bedienungsanleitung durch Anwender der App Fehler in deren Nutzung weitestgehend verhindert werden können. Die Bedienungsanleitung **SOLLTE** eine Best-Practice-Anleitung beinhalten, mit welchen Einstellungen in der App ein Maximum an Datenschutz und IT-Sicherheit erzielt werden kann. Die App **KANN** durch eine Einführung in die Bedienung den Umgang mit der App zusätzlich erleichtern.

- Stellen die Anwender Fehler fest, muss eine Möglichkeit bestehen, den Hersteller einer App zu informieren, damit dieser die Fehler beseitigt. Dabei muss berücksichtigt werden, dass ein Fehler ggf. den Start einer App verhindert, d. h. über die App selbst keine Meldung mehr erfolgen kann. Daher muss eine alternative Kontaktmöglichkeit, z. B. über eine Hotline-Telefonnummer oder eine Mailadresse vorhanden sein.

Anforderung 164: Anwender **MÜSSEN** die Möglichkeit haben, in einer Anwendung aufgetretene Fehler einer Stelle zu melden, welche die Fehler in angemessener Zeit beseitigt. Die Meldung **KANN** über die App erfolgen. Es **MUSS** mindestens ein von der App unabhängiger Weg wie beispielsweise eine Hotline-Telefonnummer oder eine E-Mail-Adresse existieren, über die man eine entsprechende Meldung abgeben kann, auch wenn die App selbst durch den Fehler nicht mehr reagiert.

- Bei jeder Sitzung („session“) mit Netzwerkzugriff besteht prinzipiell die Gefahr, dass ein Angreifer die Sitzung eines legitimen Benutzers übernimmt und ggf. auch weiterführt („session hijacking“); der Angreifer agiert dann wie der legitime Benutzer mit allen Rechten und Zugriffsmöglichkeiten, die dieser hat. Hierzu muss ein entsprechender Schutz implementiert werden wie beispielsweise die Nutzung von geheimen Session-IDs, die Verwendung von Time-Stamps oder auch verschlüsselten Verbindungen.

Anforderung 165: Sitzungen **MÜSSEN** gegen eine unautorisierte Übernahme geschützt werden.

In Softwaresystemen und auch in mobilen Anwendungen werden regelmäßig Protokolldateien und im Falle von Systemabstürzen auch sog. „Crash Reports“ erstellt, welche zur Behebung von Fehlern in der Anwendung ausgewertet werden. Für die Analyse durch den App-Hersteller oder den App-Betreiber ist regelmäßig die ausdrückliche Einwilligung des jeweiligen Nutzers erforderlich.

Anforderung 166: Für Protokolldaten wie auch für Crash Reports **MÜSSEN** dem geltenden Recht entsprechende Aufbewahrungszeiträume und Löschfristen festgelegt und eingehalten werden.

Anforderung 167: Protokolldaten wie auch für Crash Reports **DÜRFEN NICHT** sensible Daten, insbesondere keine Gesundheitsdaten enthalten.

Anforderung 168: In den Versand und die Auswertung von Protokolldaten und/oder Crash Reports **MUSS** der Nutzer ausdrücklich einwilligen, ansonsten **DARF** ein Versand oder eine Auswertung **NICHT** erfolgen.

9.5.2 Privacy by design/default

Art. 25 DS-GVO verlangt „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“, was in der Öffentlichkeit meistens als „Privacy by Design/Default“ bezeichnet wird. Während Privacy by Design schon auf die konzeptionelle Phase zielt, verlangt Privacy by Default, dass zu Anfang immer eine datenschutzfreundliche Grundeinstellung existiert.

Weder Privacy by Design noch das in Bezug auf Software dazu gehörende Pendant IT-Security by Design stehen dabei im Widerspruch mit agiler Softwareentwicklung. Die Gewährleistung von IT-Sicherheit ist sowohl ein dynamischer als auch ein kontinuierlicher Prozess. Somit lässt sich IT-Sicherheit sehr gut in agile Entwicklungsprozesse integrieren, denn eine agile Entwicklung bietet die Möglichkeiten, auf kurzfristige Änderungen zu reagieren, veränderte Anforderungen in Software abzubilden. Allerdings müssen die meist statisch ausgelegten Sicherheitsanalysen an den agilen Entwicklungsprozess angepasst werden. Ebenfalls muss bei der Erstellung der Anforderungen beachtet werden, dass eine agile Entwicklung meist feature-orientiert und somit funktionsgetrieben erfolgt; auch Anforderungen aus dem Bereich Datenschutz und IT-Sicherheit müssen daher entsprechend formuliert werden, d. h. ausdrücklich und konkret benannt werden, was gefordert wird.

Beispiel 7: Wird im Rahmen einer agilen Entwicklung die Anforderung „Benutzer muss sich mit einem Passwort anmelden“, so ist nicht beschrieben, was gefordert wird. Muss das Passwort bestimmten Kriterien genügen? Muss das Passwort gewechselt werden können? Darf das Passwort im Klartext gespeichert werden? Usw. Die Wahrscheinlichkeit, dass die Umsetzung in der agilen Entwicklung nicht den Wünschen bzw. Anforderungen von Datenschutz- und IT-Sicherheitsexperten genügt, ist relativ groß, der Fehler liegt allerdings nicht bei den Entwicklern, sondern bei den Datenschutz- und IT-Sicherheitsexperten, welche die Anforderung nicht ausdrücklich und konkret genug formulierten.

9.5.2.1 Allgemeines

Grundlegendes zum Thema Privacy by Design/Default findet man in der Praxishilfe von bvitg, GDD und GMDS[72]. Der europäische Datenschutzausschuss veröffentlichte im Oktober 2020 Leitlinien zum Thema.[73] Es empfiehlt sich, den Text zu lesen, um die Sicht der europäischen Aufsichtsbehörden zum Thema kennenzulernen.

Normadressat von Art. 25 DS-GVO ist der für die Daten Verantwortliche, was nicht zwingend der Hersteller einer Software sein muss. Entsprechend ErwGr. 78 DS-GVO „[…] sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Auslegung der Produkte, Dienste und Anwendungen zu berücksichtigen“. Resultierend aus Art. 25 i. V. m. ErwGr. 78 DS-GVO dürfen Verantwortliche wie beispielsweise Krankenkassen oder Krankenhäuser daher nur Apps im Rahmen der Patientenversorgung einsetzen, welche entsprechend dem Konzept des Privacy by Design/Default geplant und entwickelt wurde.

Art. 25 DS-GVO verlangt das Treffen geeigneter technisch-organisatorischer Maßnahmen, sowohl zur Umsetzung der in Art. 5 DS-GVO genannten Datenschutzgrundsätze (siehe auch Kapitel 9.1) wie auch zur Durchsetzung der Betroffenenrechte (siehe Kapitel 9.4). Dies muss unter Berücksichtigung

- des Stands der Technik
- der Implementierungskosten
- der Art, Umfang, Umstände und Zwecke
- der Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen

erfolgen. Die Maßnahmen müssen dabei dafür ausgelegt sein,

- die in Art. 5 DS-GVO genannten Datenschutzgrundsätze wirksam umzusetzen,
- die Rechte der betroffenen Personen zu schützen sowie
- die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen.

Dabei enthält Art. 25 DS-GVO im Gegensatz zu Art. 32 DS-GVO keine Beschränkung bzgl. der „Angemessenheit“ der Maßnahmen: Die getroffenen Maßnahmen müssen die Anforderungen von Art. 25 vollumfänglich umsetzen.

[72] bvitg, GDD, GMDS: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO). Online, zitiert am 2022-06-24; verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/privacy_design_default.php

[73] EDPB: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Online, zitiert am 2022-06-24; verfügbar unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_de

9.5.2.2 Privacy by Design: 7 grundlegende Prinzipien

Privacy by Design wird i. d. R. mit der Umsetzung der „7 grundlegenden Prinzipien“, aufgestellt von der ehemaligen kanadischen Datenschutzbeauftragten Ann Cavoukian[74,75], gleichgesetzt:

1. Proaktiv, nicht reaktiv; als Vorbeugung und nicht als Abhilfe
2. Datenschutz als Standardeinstellung
3. Datenschutz ist in das Design eingebettet
4. Volle Funktionalität – eine Positivsumme, keine Nullsumme
5. Durchgängige Sicherheit. Schutz während des gesamten Lebenszyklus[76]
6. Sichtbarkeit und Transparenz – für Offenheit sorgen
7. Wahrung der Privatsphäre der Nutzer: Für nutzerzentrierte Gestaltung sorgen

1,2,4,5,6,7 ist immer (auch) projekt-/umsetzungsspezifisch. 3 und 5 hängen vom System ab: was bietet das IT-System, was stellt der Hersteller zur Verfügung.

9.5.2.3 Umsetzung von Privacy by Design

Die damalige kanadische Datenschutzbeauftragte Ann Cavoukian, die „Privacy by Design“ ins Leben rief, empfahl 2011 Unternehmen[77]:

1) Ein Unternehmen muss einen Privacy by Design-Leiter und/oder ein Team einrichten, indem es die geeigneten Personen identifiziert.
2) Proaktive Prozesse und Praktiken zum Datenschutz durch Design einführen, umsetzen und einhalten:
    a) Anwendung auf das Design und die Architektur von Infrastruktur, IT-Systemen und Geschäftspraktiken, die mit personenbezogenen Daten interagieren oder deren Verwendung beinhalten;
    b) Beschreibung aller Kernzwecke und Hauptfunktionen, die von diesen Infrastrukturen, Systemen und Praktiken erfüllt werden, einschließlich, aber nicht beschränkt, auf die Gewährleistung der Sicherheit und den Schutz der Privatsphäre bei personenbezogenen Daten;
    c) Datenminimierung einbeziehen und den höchstmöglichen Grad an Datenschutz für personenbezogene Daten bieten, während diese gleichzeitig den anderen Kernzwecken dienen und die anderen Hauptfunktionen erfüllen;
    d) Bereitstellung dieses Grades an Datenschutz durch den Einsatz der maximal möglichen Mittel, die erforderlich sind, um die Sicherheit, Vertraulichkeit und Integrität personenbezogener Daten während des gesamten Lebenszyklus der Daten

[74] Ann Cavoukian: Privacy by Design - The 7 Foundational Principles. Online, zitiert am 2022-06-24; verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[75] Ann Cavoukian: Privacy by Design: Strong Privacy Protection - Now, and Well into the Future. Online, zitiert am 2022-06-24; verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf

[76] Eine Einführung in das 2004 von Microsoft veröffentlichtes Konzept „Security Development Lifecycle“ findet sich z. B. in

- Michael Howard & Steve Lipner (2006) The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software. Microsoft Press. ISBN 9780735622142
- The Security Development LifeCycle. Online, zitiert am 2022-09-01; verfügbar unter https://social.technet.microsoft.com/wiki/contents/articles/7100.the-security-development-lifecycle.aspx
- Secure Software Development Life Cycle Processes. Online, zitiert am 2022-09-01; verfügbar unter https://www.cisa.gov/uscert/bsi/articles/knowledge/sdlc-process/secure-software-development-life-cycle-processes

[77] Ann Cavoukian: Privacy by Design in Law, Policy and Practice - A White Paper for Regulators, Decision-makers and Policy-makers. (2011) Online, zitiert am 2022-06-24; verfügbar unter http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf

zu gewährleisten, von der ursprünglichen Erhebung über die Verwendung, Speicherung, Verbreitung bis zur sicheren Vernichtung am Ende des Lebenszyklus;

e) Wann immer dies angemessen ist, ist dieser Datenschutz automatisch vorzusehen, sodass keine Maßnahmen für einzelne Benutzer oder Kunden erforderlich sind, um die Privatsphäre ihrer personenbezogenen Daten zu schützen;

f) Sicherstellen, dass Infrastruktur, IT-Systeme und Geschäftspraktiken, die mit personenbezogenen Daten interagieren oder deren Verwendung beinhalten, angemessen transparent bleiben und einer unabhängigen Überprüfung durch alle relevanten Interessengruppen, einschließlich Aufsichtsbehörden, betroffener Personen, Nutzer und Kunden sowie Partnerorganisationen, unterliegen;

g) Förderung der Gestaltung und Aufrechterhaltung benutzerzentrierter Systeme und Praktiken, einschließlich starker Datenschutzvorgaben, angemessener Datenschutzhinweise und anderer benutzerfreundlicher Funktionen.

Zur Unterstützung eines umfassenden Privacy by Design-Programms muss ein Unternehmen nach Ansicht von einigen internationalen Datenschutz-Aufsichtsbehörden[78]:

(1) Angemessene Schulungen zum Thema Datenschutz und Sicherheit für seine Mitarbeiter durchführen;

(2) Ein System zur Überwachung aller Projekte, die regelmäßig personenbezogene Daten verarbeiten, einführen;

(3) Von den Projektleitern verlangen, dass sie für alle Projekte Dokumente zum Datenschutz entwerfen, pflegen, einreichen und aktualisieren, um sicherzustellen, dass Produkt-, Programm- oder Serviceteams die Auswirkungen ihrer Produkte, Programme und Dienstleistungen auf den Datenschutz von der ersten Stunde an bis zur endgültigen Einführung bewerten; und

(4) Ein internes Auditteam mit der Durchführung regelmäßiger Audits beauftragen, um die vollständige Umsetzung ausgewählter Dokumente zum Datenschutz und deren Überprüfung durch die zuständigen Manager zu verifizieren.

Eine Umsetzung von Privacy by Design könnte in Anlehnung an die von Ann Cavoukian aufgestellten Prinzipien z. B. beinhalten:

- Richtlinien/Policy zum Datenschutz festlegen, also beispielsweise:
  - Das Unternehmen sollte den Datenschutz im gesamten Unternehmen und in jeder Phase der Entwicklung seiner Produkte und Dienstleistungen fördern.
  - Der Schutz der Privatsphäre sollte zu Beginn des Planungsprozesses in die Geschäftspraktiken einbezogen werden.
  - Umfassende Datenschutzmanagementverfahren sollten während des gesamten Lebenszyklus von Produkten und Dienstleistungen aufrechterhalten werden.
- Verantwortlichkeiten definieren, z. B.
  - Datenverarbeitung im Büro, Home Office usw.
  - Geschäftsprozessverantwortliche
  - Produktentwickler

[78] Ausführlich diskutiert wurde das Thema 2012 auf der Konferenz „Privacy by Design: From Rhetoric to Reality“ (https://www.privacylaws.com/events-gateway/events/privacy-by-design-2012/). Im 363-Seiten umfassenden und 2014 erschienenen von Ann Cavoukian herausgegebenen Band „Privacy by Design: From Rhetoric to Reality“ (Online, zitiert am 2022-08-05; verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/PbDBook-From-Rhetoric-to-Reality.pdf) findet sich auf Seite 192 vermutlich erstmalig die Angabe der dargestellten Punkte.

    - Technische Lösungsentwickler / Manager
    - Datenschutzbeauftragter
    - …
- Weiterbildung für die an der Verarbeitung beteiligten Personen anbieten/ermöglichen, was u. a. nachfolgende Punkte beinhalten sollte:
    - Integration von Datenschutzschulungen und Sensibilisierungsprogrammen
    - Rollen- und aufgabenspezifische Inhalte für alle beteiligten Personen
    - Interdisziplinäres Publikum beachten: Geschäftsprozessverantwortliche, Softwareentwickler, Projektmanager, Vertriebsmitarbeiter, ...
- Rahmenwerk für ein Datenschutzmanagement implementieren, welches u. a. beinhaltet
    - Festlegung der Verwaltungsstruktur und Beibehaltung während des Verarbeitungszeitraums
    - Erstellung und Pflege einer Bestandsaufnahme, welche personenbezogenen Daten verarbeitet werden und welche Datenübertragungsmechanismen erfolgen
    - Einhaltung interner Datenschutzrichtlinien und Überprüfung der Einhaltung entsprechend der festgelegten Vorgaben
    - Durchführung von Schulungen und Sensibilisierungsprogrammen mit den an der Verarbeitung beteiligten Personen
    - Management von Informationssicherheitsrisiken
    - Management der Risiken bei der Datenverarbeitung durch Dritte
    - Festlegung des Umgangs mit Hinweisen/Meldungen (z. B. Whistleblower)
    - Festlegung des Umgangs mit und der Reaktion auf Anfragen und Beschwerden von Personen und Überprüfung der Einhaltung dieser Vorgaben
    - Festlegung eines Monitorings für neue betriebliche Praktiken und Überprüfung der Umsetzung der Festlegung sowie der Durchführung des Monitorrings
    - Festlegung eines Verfahrens zur Verwaltung von Datenschutzverletzungen und Überprüfung der Einhaltung des Verfahrens
    - Monitoring der Datenverarbeitung
    - Verfolgung externer Kriterien (z. B. Gesetzesänderungen)
- Überprüfungen bzgl. Umsetzung der Policy, Wahrnehmung von Verantwortlichkeiten, Durchführung von Weiterbildungen usw.
- Und natürlich: Dokumentation.

Speziell für den Einsatz von Oracle®-Datenbanken wurde 2013 eine Empfehlung für den Umgang mit Privacy by Design veröffentlicht[79]; da diese Datenbank im Gesundheitswesen oft eingesetzt wird, ist diese Empfehlung vermutlich auch von Interesse. Und grundsätzlich sind die Empfehlungen auf den Einsatz von anderen Enterprise-Strukturen sehr gut übertragbar.

9.5.2.4 Privacy by Design: Europäische Agentur für Netz- und Informationssicherheit (ENISA)

Es gibt Empfehlungen der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) zum Thema[80]:

[79] Ann Cavoukian, Mark Dixon: Privacy and Security by Design: An Enterprise Architecture Approach (2013) Online, zitiert am 2022-06-24; verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf

[80] Europäischen Agentur für Netz- und Informationssicherheit (ENISA): Privacy and Data Protection by Design – from policy to engineering (2014) Online, zitiert am 2022-06-24; verfügbar unter https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

- Vier eher technische Empfehlungen:
    - Datenminimierung (Minimize): Beschränken Sie die Verarbeitung personenbezogener Daten so weit wie möglich.
    - Datentrennung (Separate): Trennen Sie die Verarbeitung personenbezogener Daten so weit wie möglich, insbesondere von/nach unterschiedlichen Verarbeitungszwecken.
    - Pseudonymisierung (Abstract): Beschränken Sie so weit wie möglich die Details, in denen personenbezogene Daten verarbeitet werden.
    - Verbergen (Hide): Personenbezogene Daten schützen oder nicht verlinkbar oder nicht beobachtbar machen. Stellen Sie sicher, dass es nicht öffentlich oder bekannt wird.
- Vier eher organisatorische Anforderungen:
    - Informieren (Inform): Informieren Sie die betroffenen Personen rechtzeitig und angemessen über die Verarbeitung ihrer personenbezogenen Daten.
    - Kontrolle (Control): Geben Sie den betroffenen Personen eine angemessene Kontrolle über die Verarbeitung ihrer personenbezogenen Daten.
    - Durchsetzen (Enforce): Verpflichten Sie sich, personenbezogene Daten datenschutzgerecht zu verarbeiten und dies angemessen durchzusetzen.
    - Demonstrieren (Demonstrate): Zeigen Sie, dass Sie personenbezogene Daten datenschutzgerecht verarbeiten.

Die ENISA-Empfehlungen sind vielleicht „greifbarer“ als die 7 grundlegenden Prinzipien von Ann Cavoukian, adressieren aber letztlich identische Anforderungen.

9.5.2.5 Daraus resultierende Anforderungen an Mobile Apps

Anforderung 169: Bei der Planung von Apps **MÜSSEN** von Anfang an die Anforderungen der Datenschutz-Grundverordnung berücksichtigt werden. Die Dokumentation der App-Entwicklung **MUSS** dies darstellen.

Anforderung 170: Datenschutz und IT-Sicherheit **MÜSSEN** für den gesamten Lebenszyklus des Systems berücksichtigt werden, angefangen bei Anforderungsanalyse und Design der Anwendung bis hin zur Abkündigung der App, d. h. der Beendigung der Weiterentwicklung und Pflege der App sowie der Beendigung der Bereitstellung der App.

Anforderung 171: In der Design-Phase **MUSS** berücksichtigt werden, dass die App besonders sensible Daten aus dem Gesundheitsbereich verarbeitet. Die Architektur **MUSS** dementsprechend das besonders hohe Schutzniveau bei der Verarbeitung, beginnend mit der Erhebung bis hin zur Löschung der Daten, gewährleisten.

Anforderung 172: Apps **MÜSSEN** die in Kapitel 3 Datenschutz-Grundverordnung enthaltenen Betroffenenrechte gewährleisten. In der Dokumentation der App **MUSS** die Gewährleistung der Betroffenenrechte nachvollziehbar dargestellt sein.

Anforderung 173: Apps **MÜSSEN** die in Art. 5 Datenschutz-Grundverordnung beschriebenen „Grundsätze für die Verarbeitung personenbezogener Daten“ einhalten, d. h. insbesondere auf die Einhaltung der Anforderungen bzgl. Datenminimierung, Zweckbindung, Speicherbegrenzung sowie Integrität und Vertraulichkeit entwickelt werden. In der Dokumentation der App **MUSS** die Einhaltung der Vorgaben nachvollziehbar dargestellt sein.

Anforderung 174: In einer APP **MUSS** die Grundeinstellung der App den maximal möglichen Datenschutz darstellen. Ein Benutzer **KANN** den Datenschutz durch Änderung der Einstellungen aktiv herabsenken.

Anforderung 175: Es **DÜRFEN NICHT** personenbezogene Daten verarbeitet werden, welche zur Erreichung des Zweckes nicht zwingend erforderlich sind. Die Nutzung weiterer Daten **MUSS** als Rechtsgrundlage eine ausdrückliche Einwilligung haben. Die betroffene Person **MUSS** die Konfiguration der Anwendung selbst zur Verarbeitung weiterer Daten anpassen.

Anforderung 176: Bei Updates der App **MÜSSEN** die individuellen Einstellungen, insbesondere die Einstellungen zum Datenschutz, in der neuen Version berücksichtigt werden. Ist die Übernahme der Einstellungen nicht möglich, **MUSS** zuvor eine Information des Nutzers erfolgen, welche die Möglichkeit des Backups der Einstellungen sowie nach dem Update die Wiederherstellung der Einstellungen aus dem Backup beinhaltet.

9.5.3 Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung (abgekürzt DSFA) soll in den Fällen, in denen eine Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt, helfen, die Risiken zu minimieren und durch Darstellung der Maßnahmen zur Reduzierung der Risiken auch für Dritte nachvollziehbar aufzeigen, wie Verantwortliche für die Datenverarbeitung mit diesen Risiken umgehen.

Dabei beschreibt Art. 35 DS-GVO verschiedene Fälle, in denen eine DSFA erfolgen muss. Weiterhin *dürfen* nationale Datenschutz-Aufsichtsbehörden Listen veröffentlichen, wann eine DSFA nicht erforderlich ist (sog. „Whitelist“), aber sie *müssen* Listen veröffentlichen, wann eine DSFA erforderlich ist. Alle Listen müssen, sofern diese Verarbeitungstätigkeiten umfassen, welche mit dem Angebot von Waren oder Dienstleistungen in mehreren Mitgliedstaaten im Zusammenhang stehen, dem Kohärenzverfahren nach Art. 63 DS-GVO unterworfen werden, d. h. dem Europäischen Datenschutz-Ausschuss vorgelegt werden. Die Entscheidung zur deutschen Liste findet sich auf der EDSA-Homepage[81], die Liste selbst ist auf der Homepage der Datenschutzkonferenz verfügbar[82].

Unabhängig davon steht es jedem Verantwortlichen selbstverständlich frei, auch in anderen Fällen eine DSFA durchzuführen, beispielsweise zur Darstellung der Einhaltung der Vorgaben der DS-GVO hinsichtlich der Sicherheit der Verarbeitung.

Die Verbände bvitg, DKG und GMDS veröffentlichten eine Praxishilfe[83], in welcher der Umfang wie auch die Durchführung einer DSFA ausführlich beschrieben wird. Im Folgenden daher nur kurze Hinweise, gedacht als Einführung. Entsprechend der DSK-Liste ist eine DSFA insbesondere erforderlich (Nummerierung entspricht der Nummerierung in der DSK DSFA-Muss-Liste) bei:

2) Verarbeitung von genetischen Daten, wenn zugleich mindestens eines der nachfolgenden Kriterien erfüllt wird:
    a. Daten zu schutzbedürftigen Betroffenen wie Patienten,
    b. Innovative Nutzung oder Anwendung neuer technologischer organisatorischer Lösungen wie z. B. im Bereich der medizinischen Forschung,
    c. Bewerten oder Einstufen (Scoring),

[81] EDPB: Opinion 5/2018 on the draft list of the competent supervisory authorities of Germany regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Online, zitiert am 2022-06-24; verfügbar unter https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52018-draft-list-competent-supervisory_en

[82] DSK: Anwendungshinweise - Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO für den nicht-öffentlichen Bereich. Online, zitiert am 2022-06-24; verfügbar unter https://www.datenschutzkonferenz-online.de/anwendungshinweise.html bzw. direkt pdf-Datei unter https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf

[83] bvitg, DKG, GMDS: Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO. Online, zitiert am 2022-06-24; verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/dsfa.php

d. Abgleichen oder Zusammenführen von Datensätzen wie z. B. Zusammenführen von Datensätzen aus mehreren Versorgungseinrichtungen,
e. Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert, wie beispielsweise dem Recht auf Löschung, da die Daten aus Forschungsinteresse vorerst nicht gelöscht werden sollten.

Werden in einer App genetische Informationen verarbeitet, wird regelhaft eine DSFA erforderlich sein.

10) Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Verarbeitung der so zusammengeführten Daten, sofern
   - die Zusammenführung oder Verarbeitung in großem Umfang vorgenommen werden,
   - für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den betroffenen Personen erhoben wurden,
   - die Anwendung von Algorithmen einschließen, die für die betroffenen Personen nicht nachvollziehbar sind, und
   - der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im Vorhinein bestimmte Zwecke dienen.

   Werden in einer App Daten aus verschiedenen Quellen wie beispielsweise Krankenhäusern, Arztpraxen oder auch Wearables zusammengeführt, die Daten zudem ggf. nicht direkt beim Patienten, sondern bei den Versorgungseinrichtungen oder anderen Leistungserbringern erhoben, so wird eine DSFA erforderlich sein.

   Werden die Daten im Rahmen von KI-Anwendungen eingesetzt, sind die Algorithmen eher regelhaft von den betroffenen Personen nicht nachvollziehbar, sodass auch bei Apps mit KI-Ansätzen eher regelhaft eine DSFA erforderlich ist.

15) Anonymisierung von personenbezogenen Daten besonderer Kategorien (Art. 9 Abs. 1 DS-GVO) nicht nur in Einzelfällen (in Bezug auf die Zahl der betroffenen Personen und die Angaben je betroffener Person) zum Zweck der Übermittlung an Dritte.

   Letztlich führt dies dazu, dass bei der Anonymisierung von aus der Versorgung stammenden Patientendaten zu Zwecken der Weitergabe der Daten regelhaft eine DSFA erforderlich ist.

Anforderung 177: Es **MUSS** für jede Verarbeitung geprüft werden, ob eine Datenschutz-Folgenabschätzung erforderlich ist oder nicht. Das Ergebnis der Prüfung **MUSS** dokumentiert werden, das Prüfergebnis **MUSS** von Aufsichtsbehörden oder anderen Prüfinstanzen nachvollzogen werden können.

Anforderung 178: Die Prüfung, ob eine Datenschutz-Folgenabschätzung erforderlich ist oder nicht, **MUSS** insbesondere die Vorgaben der Datenschutz-Aufsichtsbehörden berücksichtigen.

Anforderung 179: Ist eine Datenschutz-Folgenabschätzung erforderlich, **MUSS** die Dokumentation mindestens den Vorgaben von Art. 35 Abs. 7 DS-GVO genügen.

Anforderung 180: Ist ein Datenschutzbeauftragter benannt worden, so **MUSS** der Verantwortliche gemäß Art. 35 Abs. 2 DS-GVO bei einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten einholen.

9.5.4 Verzeichnis der Verarbeitungstätigkeiten

Verantwortliche sowie - soweit vorhanden - deren Vertreter werden nach Art. 30 Abs. 1 DS-GVO verpflichtet, ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Auftragsverarbeiter sowie – soweit vorhanden – deren Vertreter werden nach Art. 30 Abs. 2 DS-GVO verpflichtet, ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung zu führen. Art. 30 Abs. 5 DS-GVO enthält die Regelung, dass Unternehmen oder

Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, kein entsprechendes Verzeichnis führen müssen. Diese Ausnahme gilt jedoch nur, wenn keine Verarbeitung der in Art. 9 Abs. 1 DS-GVO genannten besonderen Datenkategorien erfolgt, was insbesondere natürlich auch Gesundheitsdaten einschließt.

> Beispiel 8: Ein Arzt, der Patienten eine App zur Angsttherapie zur Verfügung stellt, verarbeitet Gesundheitsdaten. Daher gilt die Ausnahme in Art. 30 Abs. 5 DS-GVO nicht.
>
> Beispiel 9: Ein App-Anbieter führt ein Kundenverzeichnis aller Käufer seiner medizinischen App zur Ernährungsberatung bei Übergewicht. Dadurch ist bekannt, dass die Käufer Ernährungsprobleme haben, somit „infiziert" das Gesundheitsdatum, die Kundendatei. Auch hier greift daher die Ausnahme von Art. 30 Abs. 5 DS-GVO nicht.

Der Zweck zur Anlage und Führung eines Verzeichnisses, besteht grundsätzlich in der Umsetzung der Verpflichtung nach Art. 30 DS-GVO, aber entsprechend ErwGr. 82 DS-GVO dient ein entsprechendes Verzeichnis auch zum Nachweis der Einhaltung der DS-GVO. Grundsätzlich ist ein Verzeichnis schriftlich zu führen, wobei ein elektronisches Format ebenfalls möglich ist.

Auf Nachfrage muss das Verzeichnis einer Datenschutz-Aufsichtsbehörde vorgelegt werden. Verzeichniseinträge müssen daher zur Vorlage bei der zuständigen Aufsichtsbehörde in Papier- oder elektronischer Form (Textformat) exportierbar sein.

Das Verzeichnis ist grundsätzlich in deutscher Sprache zu führen. Entsprechend ErwGr. 82 DS-GVO ist jeder Verantwortliche wie auch jeder Auftragsverarbeiter verpflichtet, mit der Aufsichtsbehörde zusammenzuarbeiten und der zuständigen Aufsichtsbehörde auf deren Anfrage das Verzeichnis der Verarbeitungstätigkeiten vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können. Hierzu muss das Verzeichnis in einer Sprache verfasst sein, die alle Beschäftigten voll umfänglich verstehen können. Dies ist nur bei der jeweiligen Landessprache der Fall, d. h. in Deutschland muss das Verzeichnis der Verarbeitungstätigkeiten in deutscher Sprache geführt werden.

Art. 30 Abs. 1 DS-GVO beinhaltet die Mindestinhalte eines entsprechenden Verzeichnisses der Verarbeitungstätigkeiten[84], die wesentlichen Inhalte sowie geforderte Pflichtangaben eines Verzeichnisses werden im Folgenden aufgeführt:

a) Name und Kontaktdaten des Verantwortlichen, gegebenenfalls des gemeinsam mit ihm Verantwortlichen, Vertreter des Verantwortlichen und eines etwaigen Datenschutzbeauftragten; die zweifelsfreie Identifikation des Verantwortlichen sowie eines Ansprechpartners wie auch des Datenschutzbeauftragten dient der Transparenz der Verarbeitung.
b) Zweck der Verarbeitung: Die Zweckbestimmung ermöglicht i. d. R. einen Rückschluss auf die Rechtsgrundlage, ohne diese konkret in ein Verzeichnis aufzunehmen.

[84] Die DSK veröffentlichte Muster für entsprechende Verzeichnisse im pdf-Format, die ggf. elektronisch abgebildet werden können (Stand: Februar 2018):

- Muster für Verantwortliche: https://www.datenschutzkonferenz-online.de/anwendungshinweise.html bzw. pdf-Datei unter https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_verantwortliche.pdf
- Muster für Auftragsverarbeiter: https://www.datenschutzkonferenz-online.de/anwendungshinweise.html bzw. pdf-Datei unter https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_auftragsverarbeiter.pdf
- Hinweise zu den Mustern: https://www.datenschutzkonferenz-online.de/anwendungshinweise.html bzw. pdf-Datei unter https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf

c) Beschreibung der Kategorien betroffener Personen sowie personenbezogener Daten, d. h. beispielsweise Gruppen von Personen, z. B. Mitarbeiter, Patienten, Datengruppen wie z. B. Stammdaten (Name, Adresse, Krankenkasse).

d) Kategorien von Empfängern, denen die personenbezogenen Daten offengelegt wurden bzw. werden, einschließlich Empfängern in Drittländern oder internationale Organisationen.

Hinweis 7: Empfänger ist entsprechend Art. 4 Ziff. 9 DS-GVO „jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht". Insbesondere gilt dies sowohl für interne als auch für externe Empfängergruppen wie beispielsweise Auftragsverarbeiter, Straf- und Ermittlungsbehörden oder Krankenkassen.

e) Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich Angabe des betreffenden Drittlands oder betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 UA 2 DS-GVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien.
Zu beachten: Auch geplante oder mögliche Übermittlungen sind anzugeben!

f) Wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien. Dabei muss die Angabe der Löschfristen so konkret wie möglich erfolgen, die Angabe einer allgemeinen Aufbewahrungsfrist oder sogar eine Angabe zu unterlassen, wird als nicht ausreichend angesehen.

g) Wenn möglich ist eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1. DS-GVO in das Verzeichnis aufzunehmen, dies kann z. B. auch durch einen Verweis auf ein Sicherheitskonzept und/oder TOM erfolgen.

Sofern anstelle der Führung der Informationen im Verzeichnis selbst auf an anderer Stelle dokumentierte Konzepte verwiesen wird (z. B. Löschkonzept, Sicherheitskonzept), sind diese bei einer Anforderung des Verzeichnisses durch die Aufsichtsbehörde dieser ebenfalls zur Verfügung zu stellen.

Anforderung 181: Der Verantwortliche einer App **MUSS** alle Verarbeitungstätigkeiten in sein nach Art. 30 DS-GVO zu führendes Verzeichnis der Verarbeitungstätigkeiten dokumentieren.

Anforderung 182: Die Dokumentation **MUSS** mindestens alle in Art. 30 Abs. 1 DS-GVO geforderten Inhalte umfassen.

Anforderung 183: Der Verantwortliche **MUSS** Auftragsverarbeiter verpflichten, falls erforderlich ebenfalls ein entsprechendes Verzeichnis gemäß Art. 30 Abs. 2 DS-GVO zu führen.

9.5.5 Datenpannen und Meldepflicht[85]

Die DS-GVO enthält Regelungen bzgl. der Verletzung des Schutzes personenbezogener Daten. Art. 4 Ziff. 12 DS-GVO enthält die Definition einer „Verletzung des Schutzes personenbezogener Daten": Demnach handelt es sich um eine Verletzung der Sicherheit, welche

- ob **unbeabsichtigt** oder **unrechtmäßig**,
- zur **Vernichtung**, zum **Verlust**, zur **Veränderung**, oder zur **unbefugten Offenlegung**
- von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt,
- die **übermittelt, gespeichert** oder auf **sonstige Weise verarbeitet wurden**.

[85] Grundsätzlich sei hier auf die „Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten" der Artikel-29-Datenschutzgruppe verwiesen, welche von EDSA auf seiner ersten Sitzung anerkannt wurden. Online, zitiert am 2022-06-24; verfügbar unter https://ec.europa.eu/newsroom/article29/items/612052

Eine Verletzung des Schutzes personenbezogener Daten liegt daher nicht nur dann vor, wenn Unberechtigte Zugang zu diesen Daten bekommen, sondern auch, wenn diese Daten unbeabsichtigt oder unrechtmäßig vernichtet, verändert oder verloren gehen.

9.5.5.1 Verzeichnis der Datenpannen

Art. 33 Abs. 5 DS-GVO verlangt, dass der Verantwortliche Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen dokumentiert. Diese Dokumentation muss der zuständigen Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen von Art. 33 DS-GVO ermöglichen, d. h. auf Anforderung der Aufsichtsbehörde zur Verfügung gestellt werden. Insbesondere kann die Aufsichtsbehörde anhand dieses Verzeichnisses prüfen, ob alle meldepflichtigen Vorfälle auch gemeldet wurden.

Grundsätzlich müssen in diesem Verzeichnis alle Datenpannen dokumentiert werden.

Anforderung 184: Der Verantwortliche **MUSS** alle Datenpannen dokumentieren. Dies **MUSS** in einem entsprechenden Verzeichnis der Datenpannen erfolgen.

9.5.5.2 Meldepflicht bei Datenpannen: Aufsichtsbehörde

Art. 33 Abs. 1 DS-GVO verlangt, dass der Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten diese Verletzung unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, der Aufsichtsbehörde meldet. D. h., es meldet nie der Auftragsverarbeiter, immer nur der Verantwortliche. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden nach Bekanntwerden der Verletzung, so ist ihr eine Begründung für die Verzögerung beizufügen.

Die Meldung an die Aufsichtsbehörden muss entsprechend Art. 33 Abs. 3 DS-GVO dabei mindestens die folgenden Informationen beinhalten:

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe
   - der Kategorien der Daten (z. B. Bankdaten, Gewerkschaftsdaten oder Gesundheitsdaten) und
   - der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien der Personen (z. B. Patienten oder Beschäftigte) und
   - der ungefähren Zahl der betroffenen personenbezogenen Datensätze
2. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
4. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Anforderung 185: Es **MUSS** ein Prozess zum Umgang mit Datenpannen etabliert sein.

Anforderung 186: Der Prozess zum Umgang mit Datenpannen **MUSS** beinhalten, dass alle in Art. 33 DS-GVO genannten Informationen zusammengetragen und zusammen mit der Datenpanne dokumentiert werden. Die Dokumentation **MUSS** im Verzeichnis der Datenpannen erfolgen.

Anforderung 187: Der Prozess zum Umgang mit Datenpannen **MUSS** gewährleisten, dass eine Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde erfolgt, soweit dies erforderlich ist.

Es müssen daher neben der Verletzung selbst noch diverse Informationen bereitgestellt werden, sodass selbst eine Zeitspanne von 72 Stunden nur schwierig einzuhalten sein kann. Insbesondere die Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen bedingt letztlich eine vollständige Analyse des Vorfalls, welche ja selbst auch Einiges an Zeit kosten wird.

Bei der EU-Vorgabe von 72 Stunden ist zu beachten, dass die EU-Verordnung 1182/71[86] Regeln für die Fristen, Daten und Termine beinhaltet, die bei allen europäischen Regelungen, die selbst keine abweichenden Vorgaben beinhalten, anzuwenden sind. Da die DS-GVO keine eigenen Regelungen hinsichtlich des Umgangs mit Fristen, Daten und Termine beinhaltet, gelten somit die Vorgaben der Verordnung 1182/71. Hierbei sind bei der Vorgabe von den in Art. 33 DS-GVO vorgegebenen 72 Stunden insbesondere zu beachten:

- Art. 3 Abs. 1: Ist für den Anfang einer nach Stunden bemessenen Frist der Zeitpunkt maßgebend, in welchem ein Ereignis eintritt oder eine Handlung vorgenommen wird, so wird bei der Berechnung dieser Frist die Stunde nicht mitgerechnet, in die das Ereignis oder die Handlung fällt.
- Art. 3 Abs. 2 lit. a: Eine nach Stunden bemessene Frist beginnt am Anfang der ersten Stunde und endet mit Ablauf der letzten Stunde der Frist.
- Art. 3 Abs. 3: Die Fristen umfassen die Feiertage, die Samstage und die Sonntage, soweit diese nicht ausdrücklich ausgenommen oder die Fristen nach Arbeitstagen bemessen sind.

Somit zählen Wochenenden und Feiertage bei der Fristberechnung hinzu. Die ergänzende Regelung von Art. 3 Abs. 5 VO 1182/7 beinhaltet die Vorgabe, dass jede Frist von zwei oder mehr Tagen mindestens zwei Arbeitstage umfassen muss; dies gilt jedoch nur bei nach Tagen bemessenen Fristen. Dies führt in der Konsequenz dazu, dass die 72-Stunden-Frist zur Abgabe einer Meldung unabhängig vom Wochentag oder vorhandenen Arbeitszeitregelungen unmittelbar mit dem Zeitpunkt der Kenntnisnahme durch den Verantwortlichen beginnt und nach 72 Stunden endet, unabhängig ob das Auslaufen der Frist an einem Feiertag, Wochenende oder zu einem Zeitpunkt außerhalb der Arbeitszeit erfolgt.

Die Meldefrist/-Zeit beginnt ab dem Zeitpunkt, ab welchem dem Verantwortlichen die Verletzung bekannt wurde. Hierbei ist zu beachten, dass zum Kreis des Verantwortlichen alle Beschäftigten gehören: Nimmt ein Beschäftigter die Verletzung zur Kenntnis, so hat der Verantwortliche die Verletzung zur Kenntnis genommen. Daher ist es erforderlich, dass einerseits Prozesse bzgl. der Weitergabe der Informationen beim Verantwortlichen etabliert, andererseits alle Beschäftigten hinsichtlich der Weitergabe der Information bzgl. der Verletzung des Schutzes personenbezogener Daten geschult werden.

Auftragsverarbeiter gelten als der „verlängerte“ Arm des Verantwortlichen, d. h. hat der Auftragsverarbeiter Kenntnis von der Verletzung, gilt dies als Kenntnisnahme des Verantwortlichen und die Zeitspanne, in welcher eine Meldung zu erfolgen hat, beginnt. Grundsätzlich ist der Auftragsverarbeiter durch Art. 33 Abs. 2 DS-GVO gesetzlich verpflichtet, eine Verletzung unverzüglich dem Verantwortlichen zu melden. Je nach vertraglicher Gestaltung können bei einer „unverzüglichen“ (= ohne schuldhaftes Verzögern) Meldung aber 2-3 Tage vergehen, man denke nur an

[86] Verordnung (EWG, Euratom) Nr. 1182/71 des Rates vom 3. Juni 1971 zur Festlegung der Regeln für die Fristen, Daten und Termine. Online, zitiert am 2022-06-24; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A31971R1182

Freitagnachmittag und anschließendes Wochenende. Bekommt der Verantwortliche die Meldung aber ggf. mit 48 Stunden Verzögerung, bleibt kaum noch Zeit zur Bearbeitung des Vorfalls durch den Verantwortlichen. Daher sollten vertragliche Regelungen eine entsprechend schnelle Meldung des Auftragsverarbeiters an den Verantwortlichen beinhalten, wobei der Verantwortliche in diesen Fällen natürlich auch die Bearbeitung des Vorfalls an Wochenenden und Feiertagen gewährleisten muss.

Ausnahme von der Meldepflicht: Art. 33 Abs. 1 DS-GVO enthält einen Ausnahmetatbestand von der grundsätzlich zu erfolgenden Meldung aller Verletzungen. Wenn eine Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, muss keine Meldung erfolgen. Die Bewertung kann für Verantwortliche mitunter schwierig sein, aufgrund der Tatsache, dass ein Verstoß gegen die Meldepflicht bußgeldbewehrt (Art. 83 Abs. 4 lit. b DS-GVO) ist, empfiehlt es sich, im Zweifelsfall eine Meldung abzugeben.

9.5.5.3 Meldepflicht bei Datenpannen: Betroffene Personen

Art. 34 Abs. 1 DS-GVO verlangt, dass eine Verletzung des Schutzes personenbezogener Daten der bzw. den betroffenen Personen unverzüglich gemeldet wird, wenn die Verletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. D. h. es muss nicht zwingend ein hohes Risiko vorhanden sein, es reicht, wenn die Verletzung voraussichtlich ein hohes Risiko darstellen *könnte*.

Eine Benachrichtigung betroffener Personen hinsichtlich der Verletzung des Schutzes personenbezogener Daten muss mindestens beinhalten:

1. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
2. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
3. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Dabei sind die Anforderungen aus Art. 34 Abs. 2 DS-GVO zu beachten, wonach die Informationen in „klarer und einfacher Sprache“ zu erfolgen haben: Die Vorgaben von Art. 12 DS-GVO bzgl. der Transparenzpflicht bei der Information müssen auch nach Art. 34 DS-GVO eingehalten werden.

Ausnahme von der Meldepflicht: Art. 34 Abs. 3 DS-GVO enthält einen Ausnahmetatbestand von der Meldepflicht. Eine Meldung an die betroffene Person muss nicht erfolgen, wenn mindestens eine der nachfolgenden Bedingungen erfüllt ist:

1. Der Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen, dass die betroffenen personenbezogenen Daten für alle unbefugten/unberechtigten Personen unzugänglich sind. Dies kann z. B. durch den Einsatz von dem Stand der Technik entsprechender Verschlüsselung gewährleistet sein.
2. Der Verantwortliche stellte durch nachfolgende Maßnahmen sicher, sodass für die betroffenen Personen durch die Verletzung aller Wahrscheinlichkeit nach kein hohes Risiko mehr besteht. Dies kann z. B. dadurch geschehen, wenn beim Diebstahl eines mobilen Datenträgers unmittelbar nach dem Diebstahl ein „Remote Wipe[87]“ erfolgte.

[87] Remote Wipe ist ein Sicherheitsfeature, welches erlaubt, aus der Ferne Daten auf einem Computer, Smartphone oder Tablet zu löschen. Allerdings funktioniert Remote Wipe nur mit existierender Verbindung zu einem Netzwerk (Internet oder Mobilfunknetz, je nach eingesetzter IT-Lösung). Daher kann man von einem erfolgreichen Löschen der Daten erst dann ausgehen, wenn das Gerät den Erhalt des Löschbefehls sowie die

3. Die Meldung ist mit einem unverhältnismäßigen Aufwand verbunden. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden. In diesen Fällen kann beispielsweise eine Veröffentlichung des Vorfalles in regionalen oder überregionalen (je nach Gruppe betroffener Personen) Tageszeitungen erfolgen. Ein bloßes Bekanntgeben auf der eigenen Homepage alleine wird i. d. R. nicht ausreichen, da man nicht davon ausgehen kann, dass die betroffenen Personen zeitnah die Homepage aufsuchen. Eine Darstellung auf der eigenen Homepage kann nur eine ergänzende Maßnahme darstellen, z. B., um ergänzend zum Zeitungsartikel weitere Informationen bereitzustellen.

Anforderung 188: Liegt eine Pflicht zur Meldung einer Datenpanne gegenüber betroffenen Personen vor und hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, **MÜSSEN** die Betroffenen informiert werden. Dies **SOLLTE** über eine Benachrichtigung innerhalb der App geschehen. Wird die App von der betroffenen Person nicht mehr genutzt oder wurde die App gelöscht und dies ist dem Verantwortlichen bekannt, so **MUSS** eine Meldung über die Datenpanne auf alternativen Wegen[88] wie beispielsweise per postalischen Versand oder großflächiger Anzeige in einer überregionalen Tageszeitung erfolgen.

Anforderung 189: Entsprechende Informationen **MÜSSEN** stets über eine elektronische Signatur verfügen.

Anforderung 190: Vor Anzeige einer entsprechenden Information **MUSS** die Herkunft der Information durch Prüfung der elektronischen Signatur validiert werden. Zeigt das Validierungsergebnis der Signatur eine invalide Information an, **DARF** die Information **NICHT** angezeigt werden.

9.5.5.4 Umgang mit Datenpannen: Was ist zu tun?

Es muss ein Team gebildet werden, welches die Datenpannen bearbeitet. Zum Team sollten mindestens gehören:

- Der Datenschutzbeauftragte. Wenn kein Datenschutzbeauftragter benannt wurde, ein Jurist mit entsprechendem datenschutzrechtlichem Fachwissen.
- Ein Mitglied der Geschäftsführung, welches
  a) den Vorfall aus Unternehmenssicht bewerten und insbesondere die Entscheidung bzgl. Meldepflicht treffen und
  b) eine Entscheidung hinsichtlich der Kosten, welche zu ergreifende Maßnahmen i. d. R. beinhalten, beschließen kann.
- Ein IT-Sicherheitsexperte, welcher
  a) den Vorfall aus IT-Sicht bewertet,
  b) Maßnahmen zur Behebung der Verletzung vorschlägt und
  c) Maßnahmen, soweit möglich, zur Abmilderung der möglichen nachteiligen Auswirkungen für die betroffenen Personen vorschlagen kann.
- Ein Fachexperte aus dem betrieblichen Umfeld, aus welchem die Daten stammen, welcher die Bedeutung des Vorfalls für betroffene Personen beurteilen kann. Im Umfeld der

durchgeführte Löschung bestätigte. Die Abgabe des Remote Wipe Löschbefehles alleine reicht nicht aus, um davon ausgehen zu können, dass das Risiko aller Wahrscheinlichkeit nach nicht mehr besteht.

[88] Der Verantwortliche muss Daten über die Person haben, ansonsten hätte keine Datenpanne erfolgen können. Diese Daten dürfen zur Information eines Betroffenen nach Art. 34 DS-GVO verwendet werden. Im Zweifelsfall sollte sich der Verantwortliche mit seiner zuständigen Datenschutz-Aufsichtsbehörde in Verbindung setzen und das Vorgehen mit dieser Behörde absprechen.

Fragestellung dieser Ausarbeitung wird dies regelhaft ein entsprechendes medizinisches Fachwissen voraussetzen.

Weiterhin muss ein Prozess zum Umgang mit Datenpannen etabliert werden. Dieser Prozess muss mindestens beinhalten:

- Welche Vorfälle werden zu welchen Zeitpunkten durch wen an wen gemeldet?
- Wer hat welche Zuständigkeiten?
  - Wie erfolgt durch wen bis wann eine Risikobewertung?
  - Wer darf der Aufsichtsbehörde melden?
  - Wer meldet an die betroffenen Personen? Oder führt eine entsprechende öffentliche Bekanntgabe durch?
  - Wenn kein Datenschutzbeauftragter benannt wurde: Wer ist Ansprechpartner für die zuständige Aufsichtsbehörde?
- Wie sind die Regelungen bzgl. Auftragsverarbeiter?
  - Wer ist Anlaufstelle für Auftragsverarbeiter?
  - Wann muss/kann ein Auftragsverarbeiter melden?
  - Welche Zuarbeit muss ein Auftragsverarbeiter in welchem Zeitraum leisten? Nur innerhalb der vereinbarten Servicezeiten oder ggf. auch außerhalb? Letzteres kann mit zusätzlichen Kosten verbunden sein.
- Wer führt das gesetzlich geforderte Verzeichnis der Datenschutzpannen?

Dieser Prozess muss in das vorhandene Risikomanagement integriert werden. Insbesondere müssen alle Beschäftigten in einer Schulung bzgl. des Umgangs mit entsprechenden Vorfällen unterwiesen werden; da im Vorfeld nicht bekannt ist, welche Beschäftigte eine (mögliche) Verletzung des Schutzes personenbezogener Daten entdecken und daher das Wissen um den Prozess kennen müssen. Desgleichen sollte eine entsprechende vertragliche Vereinbarung mit dem Auftragsverarbeiter existieren.

9.6 Kooperationen

Die Form der Zusammenarbeit bestimmt grundsätzlich das datenschutzrechtliche Vertragsverhältnis. Darf der Verarbeiter die personenbezogenen Daten nur in Übereinstimmung mit der Weisung des Verantwortlichen verarbeiten, liegt eine Auftragsverarbeitung vor. Handelt es sich hingegen um (mehr oder weniger) gleichberechtigte Partner, besteht eine gemeinsame Verantwortlichkeit.

> Beispiel 10: Softwarehersteller agieren bei der Wartung von Software in der Regel als Auftragsverarbeiter, aber gerade im Kontext der klinischen Forschung ist es denkbar, dass eine Forschungseinrichtung eine App entwickelt, die von allen Forschungspartnern gemeinsam genutzt wird, was eine gemeinsame Verantwortlichkeit i. S. d. DS-GVO beinhalten könnte.

Die nachstehende Tabelle verdeutlicht zunächst in einer knappen Übersicht die grundlegenden Unterschiede zwischen einer Auftragsverarbeitung und einer gemeinsamen Verantwortlichkeit, die daraufhin in den beiden Unterkapiteln 8.1 und 8.2 konkretisiert werden.

Kriterium	Auftragsverarbeitung	Gemeinsame Verantwortlichkeit
Grundsatz	Weisungsgebundene Verarbeitung von Daten durch Auftragnehmer	(Gleichberechtigte) Partnerschaft mit gemeinsamer Verantwortung
Erlaubnistatbestand	Verantwortlicher verfügt über einen Erlaubnistatbestand	Die gemeinsam an der Verarbeitung Beteiligten haben einen (gemeinsamen) Erlaubnistatbestand
Voraussetzung für Verarbeitung	Vertrag oder anderes Rechtsinstrument gemäß Art. 28 Abs. 3 DS-GVO	Aufteilung der Pflichten gemäß Art. 26 Abs. 1 DSG-VO (und entsprechende vertragliche Regelung / Vereinbarung)

Tabelle 2: Gegenüberstellung Auftragsverarbeitung und "Gemeinsame Verantwortlichkeit"

9.6.1 Auftragsverarbeitung

Laut der Artikel-29-Datenschutzgruppe muss eine Organisation für eine Einstufung als Auftragsverarbeiter zwei grundlegende Bedingungen erfüllen: Sie muss in Bezug auf den für die Verarbeitung Verantwortlichen rechtlich eigenständig sein und sie muss personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten[89].

Dass die Verarbeitung im Auftrag und auf Weisung des Verantwortlichen erfolgt, soll sicherstellen, dass der Verantwortliche „Herr" der Verarbeitung bleibt. Dem wird vor allem dadurch Rechnung getragen, dass der Auftragnehmer gegenüber dem Verantwortlichen weisungsgebunden ist. Die Daten befinden sich zwar im Machtbereich des Auftragsverarbeiters, sie dürfen jedoch nur in Übereinstimmung mit den Weisungen des Verantwortlichen verarbeitet werden. Eigene Entscheidungsbefugnisse stehen ihm im Hinblick auf die personenbezogenen Daten nur so weit zu, wie sie im Auftragsverhältnis vereinbart sind.

Dies gilt insbesondere auch im Rahmen des Umgangs mit Verletzungen des Schutzes personenbezogener Daten („Datenpannen", siehe auch Kapitel 9.5.4). Grundsätzlich beginnt die 72-stündige Frist, in welcher ein Verantwortlicher der zuständigen Datenschutz-Aufsichtsbehörde eine Datenpanne melden muss, entsprechend Art. 33 Abs. 1 DS-GVO zum Zeitpunkt des Bekanntwerdens („[…] nachdem ihm die Verletzung bekannt wurde, […]"). Im Rahmen einer Verarbeitung im Auftrag kann die Verletzung des Schutzes personenbezogener Daten auch einem Auftragsbearbeiter bekannt werden, welcher ja zur Sphäre des Verantwortlichen zählt. Die Artikel-29-Datenschutzgruppe führte hierzu aus,[90] dass grundsätzlich dem Verantwortlichen eine Datenschutzverletzung bekannt wurde, sobald ihn der Auftragsverarbeiter davon in Kenntnis gesetzt hat. D. h. regelhaft beginnt die 72-Stunden-Meldefrist, wenn der Auftragsverarbeiter den Verantwortlichen informierte. Jedoch setzt dies voraus, dass der Vertrag zur Gestaltung der Auftragsverarbeitung entsprechend gestaltet ist. Insbesondere müssen die Pflichten des Auftragsverarbeiters bzgl. Information des Verantwortlichen bei Auftreten einer Verletzung des Schutzes personenbezogener Daten die gesetzlichen Vorgaben der EU-Verordnung 1182/71 berücksichtigen. Die von Art. 33 Abs. 2 DS-GVO geforderte „unverzügliche" Information des Verantwortlichen durch den Auftraggeber muss somit Feiertage, Wochenenden usw. umfassen und darf nicht auf die Supportzeiten des Auftragsverarbeiters (z. B. werktags von 8.00 bis 17.00 Uhr) begrenzt sein. Im Vertrag zur Auftragsverarbeitung sollten Verantwortliche bei der

[89] Artikel-29-Datenschutzgruppe, WP 169, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter". Online, zitiert am 2022-06-24; verfügbar unter http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf, Stand: 16.02.2010, S. 30

[90] Artikel-29-Datenschutzgruppe: Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01) (Stand: 2018-08-20) Online, zitiert am 2022-06-24; verfügbar unter https://ec.europa.eu/newsroom/article29/items/612052

Vereinbarung der Unterstützungsleistung entsprechend Art. 28 Abs. 3 lit. f DS-GVO auf entsprechende Regelungen achten.

Im Rahmen der Auftragsverarbeitung ist es erlaubt, dass der Verantwortliche die Entscheidung über die technischen und organisatorischen Mittel an den Auftragsverarbeiter delegiert, z. B. welche Hard- oder Software für die Datenverarbeitung eingesetzt wird. D. h. in diesem Umfeld kann und – je nach erteiltem Auftrag – muss ein Auftragsverarbeiter auch eigenständige Entscheidungen treffen, sofern die Zwecke und Mittel der Verarbeitung dadurch nicht verändert werden.

Sobald der Auftragsverarbeiter Daten zu eigenen Zwecken verarbeitet, handelt es sich um keine Auftragsverarbeitung. Denn in diesem Fall werden sowohl die Mittel als auch die Zwecke vom Auftragsverarbeiter bestimmt, er agiert somit als eigenständiger Verantwortlicher. Damit es sich um eine Auftragsverarbeitung handelt, ist die Verarbeitung ausschließlich entsprechend den Weisungen des Verantwortlichen durchzuführen.[91]

Für eine Auftragsverarbeitung sprechen daher insbesondere ausführliche Weisungen durch den für die Verarbeitung Verantwortlichen.

Die angesprochene Weisungsgebundenheit und einige andere Vereinbarungen, die in Art. 28 DS-GVO beschrieben sind, müssen bei Vorliegen einer Verarbeitung personenbezogener Daten im Auftrag in Form eines Vertrages verbindlich festgelegt werden. Zur Erstellung dieses Vertrages gibt es eine Praxishilfe[92], auf die an dieser Stelle verwiesen wird.

Die Auftragsverarbeitung, sprich die Weitergabe von Daten an einen Dienstleister, gilt als „privilegierte“ Form der Verarbeitung. Grundsätzlich muss im Falle einer Weitergabe von personenbezogenen Daten an eine externe Stelle eine gesonderte Rechtsgrundlage vorliegen. Das kann neben einer entsprechenden gesetzlichen Regelung insbesondere die Einwilligung der betroffenen Person sein. „Privilegiert“ ist die Auftragsverarbeitung dahingehend, dass sie eben keiner weiteren Rechtfertigung i.S.v. Art. 6 bis 10 DS-GVO bedarf als diejenige, auf die der Verantwortliche selbst die Verarbeitung stützt. Durch einen Vertrag zwischen Verantwortlichem und Auftragsverarbeiter, der die gesetzlichen Anforderungen nach Art. 28 DS-GVO erfüllt, wird eine rechtlich ausreichende Basis für die Weitergabe der Daten an einen Dienstleister geschaffen. Der Auftragnehmer ist datenschutzrechtlich kein Dritter i. S. v Art. 4 Nr. 10 DS-GVO, sondern wird datenschutzrechtlich wie Personal des Verantwortlichen angesehen[93].

Die angesprochenen Weisungsgebundenheit und einige andere Vereinbarungen, die in Art. 28 DS-GVO beschrieben sind, müssen bei Vorliegen einer Verarbeitung personenbezogener Daten im Auftrag in Form eines Vertrages verbindlich festgelegt werden. Zur Erstellung dieses Vertrages gibt es eine Praxishilfe, auf der an dieser Stelle verwiesen wird.

Anforderung 191: Wenn personenbezogene oder personenbeziehbare Daten im Auftrag durch andere Stellen verarbeitet werden, so **MUSS** vor Beginn der Verarbeitung ein Vertrag zur Auftragsverarbeitung abgeschlossen werden.

[91] Spoerr W.: Art. 28, Rn. 19 in: Wolff/Brink (Hrsg.) BeckOK Datenschutzrecht, 30. Ed. Stand: 01.11.2019

[92] BvD, bvitg, DKG, GDD, GMDS: Mustervertrag zur Auftragsverarbeitung (2018). Online, zitiert am 2022-06-24; verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/adv-vertrag.php

[93] So zu finden bei:

- Müller S, Stief M. (2019) Auftragsverarbeitung Orientierungshilfe, S.7. Online, zitiert am 2022-06-24; verfügbar unter https://www.datenschutz-bayern.de/technik/ orient/oh_auftragsverarbeitung.pdf
- Spoerr W.: Art. 28, Rn. 1 in: Wolff/Brink (Hrsg.) BeckOK Datenschutzrecht, 30. Ed. Stand: 01.11.2019

Anforderung 192: Der Auftraggeber **MUSS** sich vor sowie in regelmäßigen Abständen auch nach Erteilung der Auftragsvergabe von der Einhaltung der vertraglich vereinbarten datenschutzrechtlichen Vorgaben überzeugen, insbesondere auch von der Einhaltung der vertraglich vereinbarten technisch-organisatorischen Maßnahmen.

Anforderung 193: Der Auftragnehmer **MUSS** die Auftragsausführung dergestalt dokumentieren, dass der Auftraggeber die ordnungsgemäße Durchführung eines Auftrags kontrollieren kann. Der Auftraggeber **MUSS** den Auftragnehmer vertraglich hierzu verpflichten und die Umsetzung regelmäßig kontrollieren.

Anforderung 194: Alle vom Auftragsverarbeiter eingesetzten Personen, die auftragsgemäß auf personenbezogene Daten des Verantwortlichen zugreifen können, **MÜSSEN** von Auftragsverarbeiter auf das Datengeheimnis verpflichtet und über ihre Datenschutzpflichten belehrt werden.[94] Der Auftraggeber **MUSS** den Auftragsverarbeiter zu einem entsprechenden Vorgehen vertraglich hierzu verpflichten.

Anforderung 195: Der Auftragsverarbeiter **MUSS** gewährleisten, dass alle von ihm beauftragten Unterauftragnehmer bzgl. der durch sie erfolgenden Verarbeitung personenbezogener Daten an dieselben vertraglichen Pflichten gebunden werden, denen er selbst unterliegt. Der Auftraggeber **MUSS** den Auftragsverarbeiter zu einem entsprechenden Vorgehen vertraglich hierzu verpflichten.

9.6.2 Gemeinsame Verantwortlichkeit

Eine gemeinsame Verantwortlichkeit gemäß Art. 26 DS-GVO ist gegeben, wenn zwei oder mehr Verantwortliche gemeinsam über die Zwecke und Mittel der Verarbeitung entscheiden. Diese Rechtsfigur wird auch als „Joint Controllership“ bezeichnet. Hierunter können je nach Gestaltung eine Reihe von Verarbeitungen fallen.[95]

Gemäß der Interpretation der Artikel-29-Datenschutzgruppe muss der Begriff „gemeinsam“ „im Sinne von „zusammen mit“ oder „nicht alleine“ in unterschiedlichen Spielarten und Konstellationen ausgelegt werden“.[96] Wie der EuGH in seinem Facebook-Urteil feststellte, muss nicht jeder der Verantwortlichen gleich viel Verantwortung haben und über alle Daten verfügen, damit von einer gemeinsamen Verantwortung gesprochen werden kann.[97]

Liegt eine gemeinsame Verantwortlichkeit vor, verpflichtet Art. 26 Abs. 1 DS-GVO die Verarbeitenden zum Abschluss einer Vereinbarung. In erster Linie müssen sie hierin ihre Pflichten aus der DS-GVO untereinander aufteilen, insbesondere was die Wahrnehmung der Betroffenenrechte angeht, und wer welchen Informationspflichten nach den Art. 13 und 14 DS-GVO nachkommt. Die weiteren Anforderungen an die Vereinbarung über die gemeinsame Verantwortlichkeit und deren Mindestinhalt schreibt Art. 26 Abs. 1 DS-GVO fest. Ein Verstoß gegen Art. 26 DS-GVO ist nach Art. 83

[94] Hierzu kann beispielsweise das Muster der Datenschutzkonferenz angepasst und verwendet werden, welches im Kurzpapier 19 „Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO“ zu finden ist. Online, zitiert am 2022-06-02; verfügbar unter https://www.datenschutzkonferenz-online.de/kurzpapiere.html bzw. pdf-Datei unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf

[95] DSK, Kurzpapier Nr. 13: Auftragsverarbeitung, Art. 28 DS-GVO. Online, zitiert am 2022-06-24; verfügbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf, Stand: 17.12.2018, S. 4f.

[96] Artikel-29-Datenschutzgruppe. (2010) WP 169 Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, Abschnitt III.1.d) Zweites Element: „allein oder gemeinsam mit anderen“, S. 22. Online, zitiert am 2022-06-24; verfügbar unter http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf

[97] Europäischer Gerichtshof (EuGH). Urt. V. 05. Juni 2018, AZ: C-210/16. Rn. 38. Online, zitiert am 2022-06-24; verfügbar unter http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=d &mode=lst&dir=&occ=first&part=1&cid=568857

Abs. 4 lit. a DS-GVO bußgeldbewehrt. Unterlassen es zwei Verantwortliche, eine erforderliche Vereinbarung zur Gemeinsamen Verantwortlichkeit abzuschließen, liegt somit der Tatbestand einer Ordnungswidrigkeit vor.[98]

In der Praxishilfe „Art. 26 DS-GVO: Gemeinsam Verantwortliche“ der GMDS finden sich sowohl eine ausführliche Interpretation der Regelungen als auch einige Hinweise zur Vertragsgestaltung[99].

Bei der Beurteilung der Tatsache, ob die Parteien gemeinsam über Zwecke und Mittel bestimmen können, kommt es allerdings weniger auf die vertragliche Ausgestaltung an, ausschlaggebend ist vielmehr, dass eine solche Entscheidungsbefugnis in der Realität auch tatsächlich gegeben ist. Damit kommt es hinsichtlich der Beurteilung also maßgeblich auf die Betrachtung und Bewertung anhand der tatsächlichen Gegebenheiten an[100]. Dabei ist der Grad der Verantwortlichkeit unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilten.[101]

Bei einer gemeinsamen Verantwortlichkeit muss zwischen allen Verantwortlichen eine „Vereinbarung“ abgeschlossen werden, in welcher in transparenter Form festgelegt ist, welcher Verantwortliche welche Verpflichtungen der DS-GVO erfüllt. Diese Vereinbarung enthält insbesondere auch die Regelungen hinsichtlich der Zuständigkeit sowie der Gewährleistung bezüglich der Rechte von betroffenen Personen. Die Vereinbarung stellt also eine übereinstimmende Willenserklärung dar, wobei die Funktion der Vereinbarung, eine Rechtssicherheit herzustellen, entsprechend klare Festlegungen verlangt. Obgleich Art. 26 DS-GVO keine ausdrückliche Vorgabe an die Form der Vereinbarung enthält,[102] wird aus Gründen der Transparenzpflicht sowie zur Gewährleistung der Rechtssicherheit für die Vertragsparteien, insbesondere in Anbetracht drohender Bußgelder, in Deutschland in Fällen einer gemeinsamen Verantwortlichkeit regelhaft ein Vertrag abgeschlossen, was ebenfalls seitens EDSA empfohlen wird.[103]

Die wohl wichtigste Konsequenz der gemeinsamen Verantwortlichkeit für jeden der Verantwortlichen folgt aus Art. 26 Abs. 3 DS-GVO: Kein Verantwortlicher kann sich der Pflicht entziehen, für die Ansprüche des jeweils von der Datenverarbeitung Betroffenen zuständig zu sein.

---

[98] Auler, Die Gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO. Online, zitiert am 2022-06-24; verfügbar unter https://www.telemedicus.info/article/3407-Die-Gemeinsame-Verantwortlichkeit-nach-Art.-26-DS-GVO.html, Stand: 02.04.2019

[99] GMDS: Art. 26 DS-GVO: Gemeinsam Verantwortliche. Online, zitiert am 2022-06-24; verfügbar unter https://gesundheitsdatenschutz.org/download/Art.26-Gemeinsam_Verantwortliche.pdf, Stand: 17.06.2018

[100] Hartung J. Art. 26 Rn. 14 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-719325

[101] Europäischer Gerichtshof (EuGH) Urt. v. 10. Juli 2018, AZ: C-25/17. Rn. 66. Online, zitiert am 05.08.2022 verfügbar unter https://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

[102] Besprechung siehe z. B. Schneider R. „Gemeinsame Verantwortlichkeit. Entstehung, Ausgestaltung und Rechtsfolgen des Innenverhältnisses gemäß Art. 26 DSGVO“, Kap. 3.1.1 Rechtsnatur der Vereinbarung, insbesondere S. 119 „Ungeachtet der vorherigen Ausführungen ist zu sehen, dass die interne Vereinbarung gemeinsamer Verantwortlicher im deutschen Recht gemäß §§ 145, 147 BGB aufgrund der Willensübereinstimmung aller Mitverantwortlichen regelmäßig einen Vertrag darstellt.“ Springer Verlag, 2021. ISBN 978-3-658-36011-5, https://doi.org/10.1007/978-3-658-36012-2

[103] Europäische Datenschutzausschuss (EDSA): Leitlinie 7/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Rn. 173. Online, zitiert am 05.08.2022 verfügbar unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_de

Wie die Verantwortlichen intern ihre Pflichten verteilt haben, spielt also nur im Innenverhältnis eine Rolle. Der Betroffene kann seine Rechte jedoch gegenüber jedem Einzelnen der Beteiligten geltend machen.[104]

Im Gegensatz zur Auftragsverarbeitung besteht bei der gemeinsamen Verantwortlichkeit keine „Privilegierungswirkung". Verantwortlichkeit ist keine Befugnis zur Datenverarbeitung. Sie stellt nur klar, wer welche Aufgaben aus der DS-GVO zu erfüllen hat. Bei Art. 26 handelt es sich daher weder um eine Rechtsgrundlage für eine Verarbeitung durch mehrere Verantwortliche, noch bedarf es einer Rechtsgrundlage dafür, dass sich mehrere Verantwortliche zusammenschließen. Die Übermittlung personenbezogener Daten unter gemeinsam Verantwortlichen ist ein eigener Verarbeitungsvorgang im Sinne von Art. 4 Nr. 2 DS-GVO und bedarf einer Rechtsgrundlage. Soweit der jeweilige Verantwortliche im Rahmen der gemeinsamen Verantwortlichkeit personenbezogene Daten verarbeitet, benötigt er für diese Verarbeitung dementsprechend eine eigene Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO und soweit besondere Kategorien personenbezogener Daten verarbeitet werden nach Art. 9 Abs. 2 DS-GVO[105].

Weiterhin muss betroffenen Personen entsprechend Art. 26 Abs. 2 S. 2 DS-GVO das „Wesentliche" der Vereinbarung zur Verfügung gestellt werden. Entsprechend dem Schutzzweck der Norm müssen unter dem wesentlichen der Vereinbarung resp. des Vertrags alle Informationen verstanden werden, welche einerseits die Transparenz der Verarbeitung gegenüber der betroffenen Person gewährleistet, andererseits einer betroffenen Person die Wahrnehmung ihrer Rechte ermöglicht, insbesondere, ob und bei welcher der Parteien eine Anlaufstelle für betroffene Personen besteht. Weiterhin gehören hierzu natürlich alle Informationen nach Art. 13, 14 DS-GVO, insbesondere:

- Namen, Anschrift und Kontaktdaten aller Verantwortlichen
- Die Zwecke, die die Verantwortlichen gemeinsam verfolgen
- Die Zwecke, die Verantwortliche einzeln verfolgen (unter Angabe der jeweiligen Verantwortlichen)
- Die Daten, die verarbeitet werden, inkl. der Angabe, welcher Verantwortliche für welche Verarbeitung zuständig ist sowie an welchen Orten welche Verarbeitung erfolgt
- Darstellung der tatsächlichen Funktionen und Beziehungen der Verantwortlichen, was auch die Beendigungsregelungen der gemeinsamen Verantwortlichkeit beinhaltet, aber auch eine Darstellung, wer welche Funktionen hinsichtlich der Gewährleistung der Betroffenenrechte übernimmt, insbesondere, welcher Verantwortliche für die Informationspflichten nach Art. 13 und 14 DS-GVO verantwortlich ist.

Anforderung 196: Wenn personenbezogene oder personenbeziehbare Daten durch zwei oder mehr Verantwortliche, welche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, verarbeitet werden, so **MUSS** vor Beginn der Verarbeitung ein Vertrag entsprechend den Vorgaben von Art. 26 DS-GVO abgeschlossen werden.

Anforderung 197: Der Vertrag **MUSS** beinhalten, welcher Verantwortliche welche aus der DS-GVO resultierende Verpflichtung erfüllt sowie welche Verpflichtungen ggf. gemeinsam erfüllt werden und die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln.

[104] Auler L. (2019) Die Gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO. Online, zitiert am 2022-06-24; verfügbar unter https://www.telemedicus.info/article/3407-Die-Gemeinsame-Verantwortlichkeit-nach-Art.-26-DS-GVO .html, Stand: 02.04.2019

[105] DSK, Kurzpapier Nr. 16: Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO. Online, zitiert am 2022-06-24; verfügbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf. Stand: 19.03.2018, S. 1

Anforderung 198: Das Wesentliche der Vereinbarung **MUSS** der betroffenen Person zur Verfügung gestellt werden.

9.7 Benennung eines Datenschutzbeauftragten

9.7.1 Pflicht zur Benennung

Gemäß Art. 37 Abs. 1 lit. c DS-GVO muss ein Datenschutzbeauftragter benannt werden, wenn „die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 besteht".

In den ErwGr. 75 bzw. 91 ist zu finden, dass im Bereich des „Umfangs der Datenverarbeitung" zwei Einflussgrößen zu berücksichtigen sind: zum einen die Anzahl der Personen, zum anderen die Menge der verarbeiteten Daten. Entsprechend ErwGr. 91 ist bzgl. des Umfangs auch zu berücksichtigen, ob große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene verarbeitet werden, was letztlich auch wiederum den Umfang der Datenmenge („große Mengen") adressiert.

In den „Leitlinien in Bezug auf Datenschutzbeauftragte"[106] des europäischen Datenschutzausschusses wird empfohlen, bei der Klärung der Frage, ob sich von einer umfangreichen Verarbeitung sprechen lässt, die folgenden Faktoren zu berücksichtigen:

- die Zahl der betroffenen Personen – entweder als bestimmte Zahl oder als Anteil an der maßgeblichen Bevölkerung
- das Datenvolumen und/oder das Spektrum an in Bearbeitung befindlichen Daten
- die Dauer oder Permanenz der Datenverarbeitungstätigkeit
- die geografische Ausdehnung der Verarbeitungstätigkeit.

Besteht die Notwendigkeit oder auch der Wunsch einen Datenschutzbeauftragten zu benennen, so ist darauf zu achten, dass gemäß Art. 38 Abs. 6 DS-GVO bei der Person kein Interessenkonflikt hinsichtlich anderer Tätigkeiten, Aufgaben oder Pflichten bzgl. der Pflichten und Aufgaben des Datenschutzbeauftragten vorliegen darf.[107]

Anforderung 199: Ein Datenschutzbeauftragter **DARF NICHT** benannt werden, wenn Interessenskonflikte bzgl. der Aufgaben und Pflichten eines Datenschutzbeauftragten vorliegen bzw. vorliegen könnten.

Existiert ein Datenschutzbeauftragter, so müssen betroffenen Personen die Kontaktdaten zur Verfügung gestellt werden. Dies muss nicht der Name des Datenschutzbeauftragten sein, sondern kann auch eine Funktionsemailadresse wie z. B. datenschutz@beispiel.de sein, wenn sichergestellt ist, dass hierbei die Vertraulichkeit der Kontaktaufnahme gewährleistet wird.

---

[106] Europäischer Datenschutzausschuss: von der Artikel-29-Datenschutzgruppe übernommene Papiere „Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)". Online, zitiert am 2022-06-24; verfügbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

[107] Der Ausschuss Berufsbild des BvD erarbeitete ein Berufsbild für den Beruf der Datenschutzbeauftragten und betrachtet in Kapitel 4.6 auch die Benennung eines Datenschutzbeauftragten. Wer sich noch nicht mit dem Thema „Benennung eines DSB" beschäftigte, findet hier einen guten Einstieg. Online, zitiert am 2022-09-15; verfügbar unter https://www.bvdnet.de/bvd-ausschuesse/ausschuss-berufsbild/
Auch im Kurzpapier 12 der DSK „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern" wird auf die Benennung in aller Kürze auf 1 ½ Seiten eingegangen, sodass man hier das Meinungsbild der deutschen Aufsichtsbehörden dargestellt bekommt. Online, zitiert am 2022-09-15; verfügbar unter https://www.datenschutzkonferenz-online.de/kurzpapiere.html bzw. pdf-Datei unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_12.pdf

Anforderung 200: Der Kontakt zum Datenschutzbeauftragten der verantwortlichen Stelle **MUSS** öffentlich verfügbar gemacht werden, sodass betroffene Personen die oder den Datenschutzbeauftragten kontaktieren können.

Anforderung 201: Der Datenschutzbeauftragte **MUSS** von betroffenen Personen vertraulich kontaktiert werden können.

9.7.2 Information des und Prüfung durch den Datenschutzbeauftragten

Gemäß Art. 38 Abs. 1 DS-GVO muss ein Datenschutzbeauftragter „ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden“ werden. Entsprechend Art. 39 Abs. 1 lit. a DS-GVO ist der Datenschutzbeauftragte zur Überwachung der Einhaltung der Vorgaben aller datenschutzrechtlichen Bestimmungen verpflichtet. Der Datenschutzbeauftragte muss daher nicht nur informiert werden, sondern es müssen alle Informationen bereitgestellt werden, damit der Datenschutzbeauftragte seinen Prüfpflichten genügen kann.

D. h. der Datenschutzbeauftragte muss sowohl bei Planung als auch bei inhaltlichen Änderungen (z. B. Änderung der Art der Datenerhebung oder der zu erhebenden Daten) hinzugezogen werden.

9.8 Verarbeitung in einem Drittland/Drittstaat

Im Kontext der DS-GVO wird unter „Drittland“ (oder auch „Drittstaat“) ein Staat verstanden, welcher weder der EU angehört noch zu den Staaten des EWR zählt. Im Beschluss[108] des Gemeinsamen EWR-Ausschusses wurde vereinbart, dass die DS-GVO in das EWR-Abkommen aufgenommen wird und die DS-GVO somit in den drei EWR-Staaten Island, Liechtenstein und Norwegen Geltung erlangt. Somit unterliegt die Verarbeitung personenbezogener Daten in den EWR-Staaten demselben Schutz wie innerhalb der EU selbst. Daher gelten die Länder des EWR-Abkommens nicht als Drittländer.

Bei allen anderen Ländern, d. h. allen Drittländern, kann nicht davon ausgegangen werden, dass ein dem EU-Recht entsprechender Schutz personenbezogener Daten vorhanden ist. Daher muss vor Beginn einer Verarbeitung in einem Drittland, was immer auch eine Übermittlung einschließt, geprüft werden, ob bei einer Verarbeitung in diesem Drittland die Vorgaben der DS-GVO eingehalten werden.

Hinweis 8: Neben dem Europäischen Wirtschaftsgemeinschaft (EWG) existiert noch die Europäische Freihandelsassoziation (EFTA). Zusätzlich zu den EWR Staaten Island, Liechtenstein, Norwegen gehört als viertes Land die Schweiz zur EFTA. Der Beschluss des Gemeinsamen EWR-Ausschusses gilt daher nicht für die Schweiz. Die Schweiz ist aus datenschutzrechtlicher Hinsicht ein Drittland wie jedes andere Land außerhalb der EU bzw. EWR auch.

Hinweis 9: Nach Vollzug des Brexits gilt seit dem 1. Januar 2022 auch das Vereinigte Königreich bzw. jedes der vier Mitgliedsländer England, Wales, Schottland und Nordirland als Drittland.

Eine Verarbeitung personenbezogener Daten in einem Drittland ist grundsätzlich erlaubt (von einigen bundeslandesspezifischen Regelungen in Deutschland einmal abgesehen), aber da in diesen Staaten anderes als europäisches Recht gilt, ist die Verarbeitung in einem Drittland nur unter bestimmten Voraussetzungen erlaubt.

[108] Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 Vom 6. Juli 2018 zur Änderung des Anhangs XI (Elektronische Kommunikation, audiovisuelle Dienste und Informationsgesellschaft) und des Protokolls 37 (mit der Liste gemäß Artikel 101) des EWR-Abkommens [2018/1022]. Online, zitiert am 2022-08-04; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:22018D1022

Hinweis 10: Bei der Verarbeitung von Daten, welche durch § 203 StGB vor einer unbefugten Offenbarung geschützt werden, ist darauf zu achten, dass bei der Verarbeitung in jedem Ausland, d. h., unabhängig ob es ein Drittland oder ein anderes EU-Land ist, das Schutzniveau von § 203 StGB erhalten bleibt. Sollte dies der Fall sein, wird empfohlen, vor Beginn der Entwicklung einer App sich mit dieser von datenschutzrechtlichen Fragen unabhängigen Thematik auseinanderzusetzen[109].

Grundsätzlich muss bei jeder Verarbeitung personenbezogener oder personenbeziehbarer Daten in einem Drittland der Schutz dieser personenbezogenen Daten der europäischen Bürger erhalten bleiben. D. h. **Verantwortlicher und Auftragsverarbeiter müssen gewährleisten**, **dass bei einer Verarbeitung in einem Drittland** wie auch bei einer Verarbeitung durch eine internationale Organisation **das durch die DS-GVO gewährleistete Schutzniveau für natürliche Personen vollumfänglich erhalten bleibt**.

Art. 44ff DS-GVO regelt, unter welchen Bedingungen eine „Übermittlung“ in ein Drittland statthaft ist. Dabei ist der Begriff „Übermittlung“ i. S. d. englischen Begrifflichkeit „transfer“ auszulegen und gilt somit sehr weit[110]: Die DS-GVO versteht unter „Übermittlung“ alle Handlungen, durch welche ein Empfänger Kenntnis der personenbezogenen Daten erhält. „Empfänger“ wird in Art. 4 Ziff. 9 DS-GVO definiert und stellt einen sehr umfassenden Begriff dar, d. h. es spielt keine Rolle

- ob Empfänger eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, ist oder
- ob es sich um einen Dritten handelt oder nicht.

"Empfänger" ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, welcher personenbezogene Daten offengelegt werden.

Nach Art. 44 DS-GVO müssen zwei Voraussetzungen bei einer Verarbeitung in einem Drittland erfüllt sein:

1. Die „sonstigen Bestimmungen dieser Verordnung“ müssen eingehalten werden. D. h. insbesondere muss die Rechtmäßigkeit der Verarbeitung gewährleistet sein, bei der Verarbeitung von besonderen Kategorien von Daten wie beispielsweise Gesundheitsdaten muss ein Erlaubnistatbestand nach Art. 9 DS-GVO vorliegen.
2. Die Vorgaben von Kapitel V DS-GVO, dies sind die Art. 44 ff. DS-GVO, müssen erfüllt werden. Insbesondere muss eine mindestens der nachfolgend genannten Bedingungen zutreffen:
    - Die EU-Kommission stellte für das Drittland ein angemessenes Schutzniveau[111] fest (Art. 45 DS-GVO). Eine Übermittlung personenbezogener Daten in ein Land mit einem Angemessenheitsbeschluss der EU-Kommission bedarf keiner besonderen Genehmigung (Art. 45 Abs. 1 S. 2 DS-GVO), insbesondere auch keine Genehmigung durch eine Datenschutz-Aufsichtsbehörde.
    - Die Datenübermittlung in das Drittland erfolgt vorbehaltlich geeigneter Garantien (Art. 46 DS-GVO), wobei hier insbesondere die Nutzung der Standarddatenschutzklauseln entsprechend Art. 46 Abs. 2 lit. c DS-GVO

[109] Z. B. durch die folgende Praxishilfe:
- GMDS, BvD: Verarbeitung von durch § 203 StGB geschützte Daten im Ausland durch Dienstleister – Rahmenbedingungen. (Stand: 22. Juli 2022). Online, zitiert am 2022-08-04; verfügbar unter https://gesundheitsdatenschutz.org/html/schweigepflicht_ausland.php

[110] So z. B. Schantz P.: Art. 44 Rn. 10 in: Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3848735907

[111] European Commission: Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection. Online, zitiert am 2022-06-24; verfügbar unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

hervorzuheben sind. Standarddatenschutzklauseln sind die von der von der EU-Kommission beschlossenen Vertragsklauseln. Bei Nutzung der Standarddatenschutzklauseln ist für eine Übermittlung in ein Drittland ebenfalls keine besondere Genehmigung einer Aufsichtsbehörde erforderlich.

- Es existieren verbindliche interne Datenschutzvorschriften („Binding Corporate Rules“), welche die Übermittlung in ein Drittland legitimieren (Art. 47 DS-GVO).
- Eine der in Art. 49 DS-GVO genannten Ausnahmen ist für bestimmten Fall anwendbar.

Alle Instrumente müssen bei der Verarbeitung der Daten ein dem EU-Recht entsprechendes Datenschutzniveau gewährleisten[112].

Entsprechend Art. 44 S. 1 HS 2 DS-GVO müssen alle Vorgaben der DS-GVO auch im Falle einer Weiterübermittlung durch den Drittlandempfänger gewährleistet werden („die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden“). Dies gilt insbesondere auch, wenn Drittlandempfänger Daten auf Grund für den Drittlandempfänger geltenden Rechtsvorgaben die ihm übermittelten Daten an Behörden in einem Drittland weitergeben muss.

Hinweis 11: Grundsätzlich reicht die Übermittlung von einem Datum wie beispielsweise der IP-Adresse damit ein Drittstaatentransfer erfolgt. Beim Einsatz von Tools wie beispielsweise einem SDK oder Schriftarten von Drittanbietern ist daher darauf zu achten, dass hierbei keine Daten an den Drittanbieter übermittelt werden, wenn hierfür kein gesetzlicher Erlaubnistatbestand vorliegt. Weiterhin ist zu beachten, dass auch ein Datum wie beispielsweise eine IP-Adresse ein Gesundheitsdatum darstellen kann, wenn der Empfänger dieses Datum (im genannten Beispiel die IP-Adresse) der medizinischen App und damit dem medizinischen Zweck zuordnen kann. In diesen Fällen muss für die Übermittlung einer der in Art. 9 DS-GVO genannten Erlaubnistatbestände vorliegen, wie beispielsweise die ausdrückliche Einwilligung der betroffenen Person.

9.8.1 Standarddatenschutzklauseln

Die aktuell von der EU-Kommission für eine Übermittlung in ein Drittland anzuwendenden Standarddatenschutzklauseln, welche die EU-Kommission jedoch „Standardvertragsklauseln“ nannte, stammen vom 7. Juni 2021.[113] Im Kontext von „Mobile Apps“ im Gesundheitswesen wird bei einer Drittlandverarbeitung die Nutzung der Standardvertragsklauseln der EU-Kommission in Drittländern ohne Angemessenheitsbeschluss die Regel sein, die anderen Möglichkeiten zur Legitimierung der Drittlandverarbeitung sind in diesem Umfeld eher theoretischer Natur.

Bei Verwendung dieser von der EU-Kommission beschlossenen Vertragsklauseln besteht für eine Übermittlung bzw. für eine Verarbeitung personenbezogener Daten in einem Drittland keine Anzeigepflicht bei einer Aufsichtsbehörde. Jedoch gilt dies nur, wenn die Klauseln nicht verändert wurden: **Jede Abweichung von den Klauseln führt zur Anzeigepflicht**. Ergänzungen stellen entsprechend ErwGr. 109 DS-GVO i. d. R. keine Abweichung dar:

> ErwGr. 109: „[…] noch ihn daran hindern, ihnen weitere Klauseln oder zusätzliche Garantien hinzuzufügen, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den von der

[112] Siehe auch EuGH Urt. v. 06.10.2015, Az. C-362/14 („Schrems-Urteil“). Online, zitiert am 2022-06-24; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A62014CJ0362

[113] Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Text von Bedeutung für den EWR). Online, zitiert am 2022-06-24; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32021D0914

Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln stehen […]“

Aber auch wenn entsprechend Art. 46 Abs. 2 DS-GVO bei Verwendung der Standardvertragsklauseln keine Genehmigung einer Aufsichtsbehörde erforderlich ist, haben Aufsichtsbehörden selbstverständlich ein Kontrollrecht, ggfs. auch eine Kontrollpflicht. Insbesondere haben Aufsichtsbehörden auch das Recht, Datenübermittlungen zu kontrollieren. Auf Standardvertragsklauseln basierende Übermittlungen in ein Drittland können von Aufsichtsbehörde ausgesetzt oder auch verboten werden, wenn durch die Übermittlung EU- oder nationale Datenschutzvorschriften verletzt werden, beispielsweise wenn

- der Datenimporteur die Standardvertragsklauseln missachtet,
- der Datenimporteur sich weigert, mit den Datenschutzaufsichtsbehörden „redlich“ zusammenzuarbeiten oder
- die Datenübermittlung sich wahrscheinlich negativ auf die Rechte betroffener Personen auswirkt.

Werden personenbezogene Daten auf der Grundlage von Standardvertragsklauseln in ein Drittland übermittelt, so müssen diese Klauseln entsprechend den Vorgaben des Schrems II-Urteils des EuGH[114] den Fortbestand des hohen Schutzniveaus sowohl bei der Übermittlung als auch bei der Verarbeitung in einem Drittland gewährleisten. D. h. werden personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt, so muss **ein Schutzniveau gewährleistet werden**, welches **dem in der Union garantierten Schutzniveau der Sache nach gleichwertig ist**. Bei der im Zusammenhang mit einer Drittland-Übermittlung erforderlichen Beurteilung sind entsprechend den Vorgaben des EuGH insbesondere

- die vertraglichen Regelungen zu berücksichtigen, die zwischen dem in der Union ansässigen Verantwortlichen bzw. seinem dort ansässigen Auftragsverarbeiter und dem im betreffenden Drittland ansässigen Empfänger der Übermittlung vereinbart wurden, sowie
- die maßgeblichen Elemente der Rechtsordnung dieses Landes, soweit diese einen etwaigen Zugriff der Behörden dieses Drittlands auf die übermittelten personenbezogenen Daten betreffen

zu beachten. Auch bei der Verwendung der Standardvertragsklauseln **müssen** in der **Union ansässige Verantwortliche** bzw. dort ansässige **Auftragsverarbeiter geeignete Garantien vorsehen und prüfen**, ob durch diese geeigneten Garantien **ein der DS-GVO gleichwertiges Schutzniveau erreicht wird**. Kann der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter keine hinreichenden zusätzlichen Maßnahmen ergreifen, um einen solchen Schutz zu gewährleisten, ist er – bzw. in zweiter Linie die zuständige Aufsichtsbehörde – verpflichtet, die Übermittlung personenbezogener Daten in das betreffende Drittland auch bei Nutzung der Standardvertragsklauseln auszusetzen oder zu beenden.

[114] EuGH: Urt. v. 16.07.2020, Az. C-311/18 („Schrems II-Urteil“). Online, zitiert am 2022-06-24; verfügbar unter https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1
Weitergehende Informationen/Kommentierung zum Schrems II-Urteil siehe z. B. GMDS: Handlungsempfehlung bzgl. Umgang mit dem Urteil EuGH C-311/18 („Schrems II“). Stand 4. September 2020. Online, zitiert am 2022-06-24; verfügbar unter https://gesundheitsdatenschutz.org/html/schrems_ii.php

9.8.2 „Transfer-Impact-Assessment“ (TIA)

Um das Risiko wie auch das durch die ergriffenen Maßnahmen erzielte Schutzniveau zu beurteilen, ist vor Beginn einer Übermittlung von Daten in ein Drittland ein „Transfer-Impact-Assessment“ (TIA) erforderlich.[115] Klausel 14 der Standardvertragsklauseln beinhaltet folgende Bedingungen:

a) Die Parteien sichern zu, keinen Grund zu der Annahme zu haben, dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, den Datenimporteur an der Erfüllung seiner Pflichten gemäß diesen Klauseln hindern. […]

b) Die Parteien erklären, dass sie hinsichtlich der Zusicherung in Buchstabe a insbesondere die **folgenden Aspekte gebührend berücksichtigt** haben:

   i. die besonderen Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten,

   ii. die angesichts der besonderen Umstände der Übermittlung **relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten)** sowie die geltenden Beschränkungen und Garantien,

   iii. alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden.

c) […]

d) Die Parteien erklären sich damit einverstanden, die Beurteilung nach Buchstabe b zu dokumentieren und sie der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

Die Pflicht zu einer TIA erwächst also direkt aus den Standardvertragsklauseln. Entsprechend den aus Klausel 14 resultierenden Vorgaben beinhaltet eine TIA grundsätzlich eine eigenständige Analyse des Sicherheitsniveaus des Drittlandes, in welches Daten übermittelt werden sollen. Dabei muss für jedes Drittland, welches in eine Verarbeitung eingebunden ist, eine eigene TIA erstellt werden, da in den verschiedenen Ländern ja unterschiedliche rechtliche Rahmenbedingungen existieren.[116]

Im Rahmen der TIA werden die entsprechenden Aspekte der Übermittlung/Verarbeitung im Drittland dokumentiert. Hierzu gehört insbesondere eine systematische Beschreibung des geplanten Datentransfers beinhaltend

[115] Siehe auch EuGH, Urt. v. 2020-07-16 Az. C-311/18 („Schrems II“), Rn. 131: „Insoweit ist darauf hinzuweisen, dass es gemäß Art. 46 Abs. 1 der DSGVO, falls kein Angemessenheitsbeschluss der Kommission vorliegt, Sache des in der Union ansässigen Verantwortlichen bzw. des dort ansässigen Auftragsverarbeiters ist, insbesondere geeignete Garantien vorzusehen.“ D. h. der Datenexporteur hat eine Prüfpflicht. Online, zitiert am 2022-09-24; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62018CJ0311

[116] Zu beachten: Einige Cloud-Anbieter beinhalten in ihren Vertragsklauseln, dass Daten „auf der ganzen Welt“ gespeichert werden können oder „Beschäftigte aus aller Welt“ zur Störungsbeseitigung eingesetzt werden. Ob „alle Welt“ oder diverse Länder aufgezählt werden: Für jedes potenzielle Land (ggf. also auch für alle Länder der Welt) muss dann eine TIA durchgeführt werden.

- die Darstellung des Zweckes, aus welchem auch die Erforderlichkeit der Übermittlung abgeleitet werden kann,
- die Daten bzw. Kategorien der Daten, inkl. deren Sensibilität,
- eine Bewertung der Verhältnismäßigkeit der Übermittlung in Bezug auf den verfolgten Zweck.

Weiterhin sind alle Rahmenbedingungen zu dokumentieren, welche für die Bewertung herangezogen wurden. Gemäß Klausel 14 lit. b) Nr. ii) sind sowohl die Rechtslage als auch die rechtlichen Gepflogenheiten im Drittland zu identifizieren und zu bewerten. Natürlich sind auch die Maßnahmen zu dokumentieren, welche ein der DS-GVO gleichwertiges Schutzniveau gewährleisten. Die festzuhaltende abschließende Beurteilung stellt immer nur eine Momentaufnahme dar, da sich die Umstände ändern können, inklusive der Rechtslage im Drittland. Daher sollte im Rahmen einer TIA auch immer die Zeitspanne wie auch Umstände festgelegt werden, nach der die Ergebnisse spätestens evaluiert werden müssen.

Am 1. September 2021 veröffentlichte die „International Association of Privacy Professionals“ (IAPP) Vorlagen für den Transfer in Drittstaaten bzw. die USA[117]. Dabei handelt es sich um zwei Excel-Tabellen:

1. Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities. In dieser Tabelle sind u.a. Wahrscheinlichkeiten für einen behördlichen Zugriff auf bei einem Cloud-Anbieter gespeicherte personenbezogene Daten eines (EU) Verantwortlichen anzugeben.
2. EU SCC Transfer Impact Assessment (TIA). Auch in dieser Vorlage wird in Schritt 4 abgefragt, wie wahrscheinlich ein aus europäischer Sicht unzulässige Zugriff auf Daten ist.

Beide Listen stammen von David Rosenthal und stellen bislang die einzige den Autoren bekannte öffentlich frei verfügbare Vorlagen für eine TIA dar. Anzumerken ist, dass der EuGH die Wahrscheinlichkeit eines Zugriffs nicht adressiert, sondern allein schon die Möglichkeit eines Zugriffs aus Sicht des EuGH als unzulässig anzusehen ist. Ähnlich äußerte sich EDSA zum Thema: Betroffenenrechte müssen gewährleistet werden, lediglich bzgl. der Sicherheit der Verantwortung kann über Angemessenheit argumentiert werden.

Dennoch können die Excel-Tabellen bei der Erstellung der die Standardvertragsklauseln ergänzenden TIA hilfreich sein: Schritt 1 bis Schritt 3 in den Tabellen stellen eine gute Übersicht dar, was bei Transfer in Drittstaaten geregelt ist, oder eben nicht.

9.8.3 Anforderungen an eine Verarbeitung in einem Drittland

Anforderung 202: Jede Datenübermittlung in ein Drittland **MUSS** sicher identifiziert werden.

Anforderung 203: Eine Datenübermittlung in ein Drittland **DARF NICHT** erfolgen, wenn hierfür keine Rechtsgrundlage existiert.

Anforderung 204: Bei einer personenbezogenen Datenverarbeitung in einem Drittland ohne Angemessenheitsbeschluss **MÜSSEN** die Standardvertragsklausen[118] der Europäischen Kommission verwendet werden. Dies **MUSS** auch erfolgen, wenn eine Verarbeitung in Drittländern nicht sicher ausgeschlossen werden kann.

[117] International Association of Privacy Professionals (IAPP): Transfer Impact Assessment Templates. Online, zitiert am 2022-06-24; verfügbar unter https://iapp.org/resources/article/transfer-impact-assessment-templates/

- EU SCC Transfer Impact Assessment (TIA), Excel-Tabelle mit Stand 2021-08-21
- Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities, Excel-Tabelle mit Stand 2021-07-31

[118] Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Text von Bedeutung für den EWR). Online, zitiert am 2022-06-24; verfügbar unter https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de&uri=CELEX%3A32021D0914

Anforderung 205: Für jedes Drittland, welches in eine Verarbeitung eingebunden ist, **MUSS** ein eigenes Transfer-Impact-Assessment erstellt werden.

Anforderung 206: Soll die Datenverarbeitung in einem Drittland durchgeführt werden oder ist ein Zugriff auf die Daten aus einem Drittland nicht ausgeschlossen, **MUSS** der Verantwortliche zuvor ein Transfer-Impact-Assessment durchführen.

Anforderung 207: Das Transfer-Impact-Assessment **MUSS** zur Dokumentation hinzugenommen werden.

Anforderung 208: Bei einer personenbezogenen Datenverarbeitung in einem Drittland ohne Angemessenheitsbeschluss **MÜSSEN** durch den Datenexporteur zusätzliche Maßnahmen getroffen werden, welche eine unbefugte Kenntnisnahme personenbezogener Daten auch durch staatliche Stellen im Drittland wirksam verhindern.

Anforderung 209: Bei Verwendung von Tools von Drittherstellern wie beispielsweise einem SDK oder einer API oder Schriftarten **MUSS** gewährleistet werden, dass keine Daten an den Drittanbieter ohne gesetzlichen Erlaubnistatbestand übermittelt werden.

Anforderung 210: **KANN** der Empfänger eines Datums dieses Datum der medizinischen App und damit dem medizinischen Zweck zuordnen, so **MUSS** ein in Art. 9 DS-GVO genannter Erlaubnistatbestand wie beispielsweise die ausdrückliche Einwilligung der betroffenen Person vorliegen.

9.9 Datenschutzerklärung / Datenhinweise für Apps

Wie auch für Webseiten sind auch bei Apps Datenschutzhinweise für betroffene Personen ein unverzichtbares Element. Jedoch existieren im Vergleich zur Webseite besondere Bedingungen:

- Einerseits ist die Datenverarbeitung und -nutzung bei Apps regelhaft anders als auf einer Webseite, andererseits verfügen mobile Geräte nur ein deutlich kleineres Display und somit existieren andere Vorgaben hinsichtlich der Anzeige der Informationen.
- Auch werden regelhaft bei jeder Installation einer App nicht nur Daten verarbeitet (was auch beim Aufruf einer Webseite geschieht), sondern es wird eher regelhaft auch auf Schnittstellen des Endgerätes zugegriffen, um so Daten aus Adressbuch usw. zuzugreifen oder Geräte wie Kamera oder Mikrofon nutzen zu können. D. h. bei einer App wird eher regelhaft auf im Endgerät verfügbare Daten zugegriffen.
- Zudem haben Hersteller von mobilen Betriebssystemen und App-Store-Anbieter in begrenzten Umfang auch Zugriff auf Informationen, welchen Hersteller/Betreiber einer App nur sehr begrenzt beeinflussen kann.

Bei der Gestaltung von Datenschutzhinweisen für eine App gelten zwar grundsätzlich die datenschutzrechtlichen Anforderungen wie auch für Webseiten, aber den besonderen Rahmenbedingungen muss zusätzlich Rechnung getragen werden.

Die Datenschutzhinweise müssen selbstverständlich den Informationsvorgaben der Artikel 12 bis 14 DS-GVO genügen. Insbesondere ist zu beachten, dass diese Informationen gemäß Art. 13 DS-GVO betroffenen Personen spätestens zum Zeitpunkt der Erhebung der Daten zur Verfügung gestellt werden. Auch bei der Einholung einer Einwilligung müssen Informationen vor Abgabe der Einwilligung gegeben werden. Daher ist darauf zu achten, dass Datenschutzhinweise grundsätzlich vor Installation einer App und vor Einholung einer Einwilligung bereitgestellt und ohne Anlage oder Vorhandensein eines Kundenkontos betroffenen Personen zur Verfügung gestellt werden.

Weiterhin muss die betroffene Person über die Rechtsgrundlage der Verarbeitung informiert werden und ist über eine Drittstaatenverarbeitung aufzuklären. Sofern eine gemeinsame Verantwortlichkeit vorliegt, können die Informationen über das Wesentliche der Vereinbarung in die Datenschutzerklärung integriert werden.

Ein Beispiel, wie eine entsprechende Datenschutzerklärung aussehen könnte, finden Sie in Anhang 3.

10 Abkürzungen

Abs.	Absatz
API	Application Programming Interface
Apps	Application Software / Anwendungssoftware
Art.	Artikel
AV	Verarbeitung im Auftrag (Auftragsverarbeitung)
Az.	Aktenzeichen
BDSG	Bundesdatenschutzgesetz
BEREC	Body of European Regulators for Electronic Communication
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfDI	Bundesbeauftragte(r) für den Datenschutz und die Informationsfreiheit
BGH	Bundesgerichtshof
BMG	Bundesministerium für Gesundheit
BSI	Bundesamt für Sicherheit in der Informationstechnik
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands e.V.
Bvitg	Bundesverband Gesundheits-IT e.V.
CISA	U.S. Cybersecurity and Infrastructure Security Agency
DiGA	Digitale Gesundheitsanwendungen
DiPA	Digitale Pflegeanwendungen
DiGAV	Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung)
DKG	Deutsche Krankenhausgesellschaft e. V.
DSFA	Datenschutz-Folgenabschätzung
DS-GVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
ECS	Electronic Communications Service
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EDSA	Europäischer Datenschutzausschuss
ENISA	Agentur der Europäischen Union für Cybersicherheit
ErwGr.	Erwägungsgrund/Erwägungsgründe
EU	Europäische Union
EuGH	Europäische Gerichtshof
EWR	Europäischer Wirtschaftsraum
FDA	U.S. Food and Drug Administration
ff.	Folgende
GDD	Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.
GEREK	Gremium europäischer Regulierungsstellen für elektronische Kommunikation
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.
GPS	Global Positioning System
HHS	U.S. Department of Health & Human Services
HWG	Gesetz über die Werbung auf dem Gebiet des Heilwesens (Heilmittelwerbegesetz)

IAPP	International Association of Privacy Professionals
i. d. R.	in der Regel
IMEI	International Mobile Equipment Identity
i. s. d.	Im Sinne der/des
IMSI	International Mobile Subscriber Identity
i. S. v.	Im Sinne von
i. V. m.	In Verbindung mit
IT	Informationstechnologie
lit.	littera (lat. „Buchstabe“)
LBS	Location Based Services
MDCG	Medical Device Coordination Group
MPBetreibV	Verordnung über das Errichten, Betreiben und Anwenden von Medizinprodukten (Medizinprodukte-Betreiberverordnung)
NIS	Network and Information Systems
NIST	U.S. National Institute of Standards and Technology
Nr.	Nummer
OCSP	Online Certificate Status Protocol
OLG	Oberlandesgericht
OTT	Over-the-top (Dienste)
OWASP	Open Web Application Security Project
RL	Richtlinie
RStV	Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag)
SCC	Standard Contractual Clauses (Standardvertragsklauseln)
SDK	Software Development Kit
SGB V	Sozialgesetzbuch (SGB) Fünftes Buch (V)
TIA	Transfer Impact Assessment
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TMG	Telemediengesetz
TTDSG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutz-Gesetz)
UA	Unterabsatz
Urt.	Urteil
UTC	Universal Time Coordinated
VDiPA	Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Pflegeanwendungen in der Sozialen Pflegeversicherung
VO	Verordnung
Ziff.	Ziffer

11 Literatur

11.1 Bücher

- Davies A, Mueller J. Developing Medical Apps and mHealth Interventions: A Guide for Researchers, Physicians and Informaticians. Springer Verlag 2020. ISBN 978-3-030-47501-7. https://doi.org/10.1007/978-3-030-47499-7
- Franz H. Handbuch zum Testen von Web- und Mobile-Apps. Springer Verlag, 2. Auflage 2015. ISBN 978-3-662-44027-8, https://doi.org/10.1007/978-3-662-44028-5
- Gkoulalas-Divanis A, Bettini C. (eds.) Handbook of Mobile Data Privacy. Springer Verlag 2018. ISBN 978-3-319-98160-4. https://doi.org/10.1007/978-3-319-98161-1
- Gunasekera s. Android Apps Security - Mitigate Hacking Attacks and Security Breaches. Apress Media LLC, 2nd Edition 2020. ISBN: 978-1-4842-1681-1. https://doi.org/10.1007/978-1-4842-1682-8
- Hanschke I. Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten. Springer Verlag, 2. Auflage 2020. ISBN 978-3-658-28698-9, https://doi.org/10.1007/978-3-658-28699-6
- Jorzig A, Sarangi F. Digitalisierung im Gesundheitswesen - Ein kompakter Streifzug durch Recht, Technik und Ethik. Springer Verlag, 1. Auflage 2020. ISBN ISBN 978-3-662-58305-0. https://doi.org/10.1007/978-3-662-58306-7
- Kneuper R. Datenschutz für Softwareentwicklung und IT. Springer Verlag, 1. Auflage 2021. ISBN 978-3-662-63086-0, https://doi.org/10.1007/978-3-662-63087-7
- Liu B, Zhou W, Zhu T, Xiang Y, Wang K. (eds.) Location Privacy in Mobile Applications. Springer Verlag, 1. Auflage 2018. ISBN 978-981-13-1704-0. https://doi.org/10.1007/978-981-13-1705-7
- Müller KR. IT-Sicherheit mit System. Springer Verlag, 6. Auflage 2018. ISBN 978-3-658-22064-8, https://doi.org/10.1007/978-3-658-22065-5
- Rehmann W, Tillmans C. (Hrsg.) E-Health / Digital Health. C. H. Beck Verlag, 1. Auflage 2022. ISBN 978-3-406-76208-6
- Reuter C. (Hrsg.) Sicherheitskritische Mensch-Computer-Interaktion. Springer Verlag, 2. Auflage 2021. ISBN 978-3-658-32794-1, https://doi.org/10.1007/978-3-658-32795-8
- Scott A. Building Web Apps that Respect a User's Privacy and Security. O'Reilly Media, Inc., 2017 First Release. ISBN 978-1-491-95838-4
- Solmecke C, Taeger J, Feldmann T. (Hrsg.) Mobile Apps - Rechtsfragen und rechtliche Rahmenbedingungen. De Gruyter, 1. Auflage 2013. ISBN 978-3-11-030480-0
- Westhoff D. Mobile Security - Schwachstellen verstehen und Angriffsszenarien nachvollziehen. Springer Verlag, 1. Auflage 2020. ISBN 978-3-662-60854-8, https://doi.org/10.1007/978-3-662-60855-5

11.2 Internet

- BMG: Studie „Chancen und Risiken von Gesundheits-Apps" (CHARISMHA). Stand: 2016-04-24 URL: https://www.bundesgesundheitsministerium.de/service/publikationen/details/chancen-und-risiken-von-gesundheits-apps-charismha-kurzbericht.html bzw. pdf-Datei der Studie unter https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Gesundheit/Berichte/Abschlussbericht_CHARISMHA.pdfhttps://publikationsserver.tu-braunschweig.de/servlets/MCRFileNodeServlet/dbbs_derivate_00042279/charismha_gesamt.pdf
- Artikel-29-Datenschutzgruppe: Stellungnahme zu Apps auf intelligenten Endgeräten. (WP202) Stand: 2013-02-27) URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_de.pdf

- Bayerisches Landesamt für Datenschutzaufsicht: Prüfkatalog für den technischen Datenschutz bei Apps mit normalem Schutzbedarf. Stand: 2016-06-22. URL: https://www.lda.bayern.de/media/baylda_pruefkatalog_apps.pdf
- BSI: IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Gesundheits-Apps. Stand: 2021-06-06. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/gesundheitsapps.html
- BSI: Sicherheitsanforderungen an digitale Gesundheitsanwendungen (Technische Richtlinie BSI TR-03161, Trial Use). Stand: 2020-04-15. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03161/BSI-TR-03161.html
- BSI: Grundschutz-Kompendium - APP.1.4 Mobile Anwendungen (Apps) (Edition 2022). Stand: 01.02.2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/06_APP_Anwendungen/APP_1_4_Mobile_Anwendungen_Edition_2022.html
- CISA: Applying Zero Trust Principles to Enterprise Mobility. Stand: March 2022 (Draft for public comment). URL: https://www.cisa.gov/sites/default/files/publications/Zero_Trust_Principles_Enterprise_Mobility_For_Public_Comment_508C.pdf
- CISA: CEG Mobile Device Cybersecurity Checklist for Organizations. Stand: Nov. 2021. URL: https://www.cisa.gov/sites/default/files/publications/CEG_Mobile_Device_Cybersecurity_Checklist_for_Organizations_0.pdf
- CISA: CISA Zero Trust Maturity Model. Stand: June 2021. URL: https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf
- Datenschutzkonferenz: Gesundheitswebseiten und Gesundheits-Apps – Keine Weitergabe sensibler Daten an unbefugte Dritte! Entschließung vom 06.11.2019, URL: https://www.datenschutzkonferenz-online.de/media/en/20191106_entschlie%C3%9Fung_gesundheitswebseiten_dsk.pdf
- Datenschutzkonferenz: Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen. Entschließung 2016-04-07. URL: https://www.datenschutzkonferenz-online.de/media/en/20160407_en_wearables.pdf
- Deutsche Telekom AG. Privacy and Security Assessment Verfahren, technische Sicherheitsanforderungen, Abchnitt 12 „Mobile_Applikationen“. URL: https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicherheit/details/privacy-and-security-assessment-verfahren-342724 bzw. zip-Datei mit den Anforderungen https://www.telekom.com/resource/blob/314436/ad342242a06c51e07dc90d808816e57c/dl-technische-sicherheitsanforderungen-data.zip
- Düsseldorfer Kreis: Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter. Stand: 2014-06-16. URL: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/OH_Appentwicklung.pdf
- EDPS: Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions. Stand: 2016-11-07. URL: https://edps.europa.eu/data-protection/our-work/publications/guidelines/mobile-applications_en
- EDPS: Mobile-Health-Dienste. Stellungnahme 1/2015, 2015-05-21. URL: https://edps.europa.eu/data-protection/our-work/publications/opinions/mobile-health_de
- EDSA: Leitlinien 8/2020 über die gezielte Ansprache von Nutzer:innen sozialer Medien. Stand: 2021-04-13. URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_de
- ENISA: Privacy and data protection in mobile applications. Stand: 2018-01-29. UR: https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications
- ENISA: Smartphone Secure Development Guidelines. Stand 2017-02-10. URL: https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016

- FDA: Cybersecurity. URL https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity, insbesondere
    - Best Practices for Communicating Cybersecurity Vulnerabilities to Patients. Stand: 2021-10-01. URL: https://www.fda.gov/about-fda/cdrh-patient-science-and-engagement-program/best-practices-communicating-cybersecurity-vulnerabilities-patients
    - Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions. Stand: 2022-07-04 (Draft). URL: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
- FDA: Policy for Device Software Functions and Mobile Medical Applications. Stand: 2019-09. URL: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/policy-device-software-functions-and-mobile-medical-applications bzw. pdf guidance document https://www.fda.gov/media/80958/download
- HHS: Resources for Mobile Health Apps Developers. Stand: 2020-09-01. URL: https://www.hhs.gov/hipaa/for-professionals/special-topics/health-apps/index.html
- NIST: Special Publications (SP). URL http://csrc.nist.gov/publications/PubsSPs.html, insbesondere
    - Vetting the Security of Mobile Applications. Stand: 2019-04.URL: https://csrc.nist.gov/publications/detail/sp/800-163/rev-1/final
    - Securing Electronic Health Records on Mobile Devices. Stand: 2018-07-27. URL https://www.nccoe.nist.gov/healthcare/electronic-health-records-mobile-devices bzw. pdf-Datei unter https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-1.pdf
    - Securing Telehealth Remote Patient Monitoring Ecosystem. Stand: 2022-02-22. URL: https://www.nccoe.nist.gov/healthcare/securing-telehealth-remote-patient-monitoring-ecosystem bzw. pdf-Publication unter https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-30.pdf
- OWASP mobile security. URL: https://owasp.org/www-project-mobile-security/
- OWASP Web Security Testing Guide. URL: https://owasp.org/www-project-web-security-testing-guide/

11.3 Zeitschriftenartikel

- Aldini et al. (2021) Ask a(n)droid to tell you the odds: probabilistic security-by-contract for mobile devices. Soft Computing 25: 2295–2314. https://doi.org/10.1007/s00500-020-05299-4
- Autili et al. (2021) Software engineering techniques for statically analyzing mobile apps: research trends, characteristics, and potential for industrial adoption. Journal of Internet Services and Applications (12): Article number 3. https://doi.org/10.1007/13174.1869-0238
- Betzing et al. (2020) The impact of transparency on mobile privacy decision making. Electronic Markets (30):607–625. https://doi.org/10.1007/s12525-019-00332-3
- Bierekoven C. (2015) Datenschutzrechtliche Zulässigkeit von Gesundheits-Apps. Einordnung, Definition und Anforderungen an Gesundheits- und Lifestyle-Apps. ITRB: 114-120
- Buck C, Kaubisch D, Eymann T. (2016) Mobile Applikationen im Arbeitsalltag: Geringe Literacy als Sicherheitsgefahr für Unternehmen. HMD Praxis der Wirtschaftsinformatik (53): 87–97
- Cruz L, Abreu R, Lo D. (2019) To the attention of mobile software developers: guess what, test your app! Empirical Software Engineering (24): 2438–2468. https://doi.org/10.1007/s10664-019-09701-0
- Demissie B, Ceccato M, Shar L. (2020) Security analysis of permission re-delegation vulnerabilities in Android apps. Empirical Software Engineering (25): 5084–5136. https://doi.org/10.1007/s10664-020-09879-8

- Deypir M. (2019) Entropy-based security risk measurement for Android mobile applications. Soft Computing (23): 7303–7319. https://doi.org/10.1007/s00500-018-3377-5
- Gerber P, Volkamer M. (2015) Usability und Privacy im Android Ökosystem. DuD: 108-113
- Grundy Q, Chiu K, Bero L. (2019) Commercialization of User Data by Developers of Medicines-Related Apps: a Content Analysis. J Gen Intern Med (34): 2833–2841. https://doi.org/10.1007/s11606-019-05214-0
- Hinzpeter B. (2015) Datenschutzrechtliche Anforderungen im Zusammenhang mit Apps. PinG: 76-78
- Iwaya et al. (2019) E-Consent for Data Privacy: Consent Management for Mobile Health Technologies in Public Health Surveys and Disease Surveillance. MEDINFO 2019: 1223-1227. https://doi.org/10.3233/SHTI190421
- Katzenmeier C. (2019) Big Data, E-Health, M-Health, KI und Robotik in der Medizin. MedR (37): 259–271
- Kriwy P. (2020) Einstellung zum Datenschutz und mHealth-Nutzung. Ergebnisse einer Studierendenbefragung und des Health Information National Trends Survey. Präv Gesundheitsf (15): 218–225. https://doi.org/10.1007/s11553-019-00755-y
- Kunz T, Lange B, Selzer A. (2020) Datenschutz und Datensicherheitin Digital Public Health. Bundesgesundheitsbl (63): 206–214 https://doi.org/10.1007/s00103-019-03083-w
- Lei et al. (2016) A survey of privacy protection techniques for mobile devices. Journal of Communications and Information Networks: 86–92. https://doi.org/10.1007/BF03391582
- Matutis C. (2022) Der Einfluss der §§ 327 ff. BGB auf Vertragsgestaltung und AGB – nicht nur im „grünen Bereich“. GRUR-Prax: 195-198
- Minen et al. (2018) Privacy Issues in Smartphone Applications: An Analysis of Headache/Migraine Applications. Headache (58): 1014-1027. https://doi.org/10.1111/head.13341
- Morgenstern M, Pursche O, Clausing E. (2021) Die Sicherheitslage im IoT-Umfeld.DuD: 102–106
- Morera et al. (2016) Security Recommendations for mHealth Apps: Elaboration of a Developer’s Guide. J Med Syst (40): 152. https://doi.org/10.1007/s10916-016-0513-6
- Ortner R, Daubenbüchel F. (2016) Medizinprodukte 4.0 – Haftung, Datenschutz, IT-Sicherheit. NJW: 2918-2924
- Parker et al. (2017) A health app developer’s guide to law and policy: a multi-sector policy analysis. BMC Medical Informatics and Decision Making (17):141. https://doi.org/10.1186/s12911-017-0535-0
- Putschli C. (2017) Wearables und Datenschutz. DuD: 721-723
- Raber F, Krüger A. (2022) Transferring recommendations through privacy user models across domains. User Modeling and User-Adapted Interaction (32): 25–90. https://doi.org/10.1007/s11257-021-09307-6
- Rasthofer, et al. (2016) Harvester. Vollautomatische Extraktion von Laufzeitwerten aus obfuskierten Android-Applikationen.DuD:718-722
- Roth-Isigkeit D. (2022) Unionsrechtliche Transparenzanforderungen an intelligente Medizinprodukte. GesR: 278-285
- Rübsamen K. (2015) Rechtliche Rahmenbedingungen für mobileHealth. MedR (33): 485–491
- Salza et al. (2020) Third-party libraries in mobile apps. Empirical Software Engineering (25): 2341–2377. https://doi.org/10.1007/s10664-019-09754-1
- Schairer C, Rubanovich C, Bloss C. (2018) How Could Commercial Terms of Use and Privacy Policies Undermine Informed Consent in the Age of Mobile Health? AMA Journal of Ethics (20/9): E864-872
- Schippel R. (2020) Allgemeine Geschäftsbedingungen auf mobilen Endgeräten. ITRB: 43-47
- Schöttle H. (2018) Mobile Apps: Vorgaben der Datenschutz-Grundverordnung. Der Betrieb: 1197-1202

- Schreiber K, Esser J. (2022) Einheitliche Update-Zyklen im Spannungsfeld der §§ 327f, 327r BGB - Aktualisierung und Funktionsänderung. RDi: 317-323
- Schreier HG, Michels A. (2022) Negative Beschaffenheitsvereinbarungen im digitalen Vertragsrecht und bei Waren mit digitalen Elementen. Zum praktischen Umgang mit Mängellisten. RDi: 381-390
- Sriram RD, Subrahmanian E. (2020) Transforming Health Care through Digital Revolutions. Journal of the Indian Institute of Science (100): 753–772. https://doi.org/10.1007/s41745-020-00195-0
- Stürner M. (2022) Verträge über digitale Produkte: die neuen §§ 327–327u BGB. Teil 1: Grundlagen und vertragliche Pflichten. Juristische Ausbildung: 32–41
- Stürner M. (2022) Verträge über digitale Produkte: die neuen §§ 327–327u BGB. Teil 2: Gewährleistung, Unternehmerregress, Konkurrenzregelungen im Schuldrecht BT. Juristische Ausbildung: 159–168
- Torre et al. (2017) Supporting users to take informed decisions on privacy settings of personal devices. Personal and Ubiquitous Computing volume (22): 345–364. https://doi.org/10.1007/s00779-017-1068-3
- v. Czettritz P, Strelow T. (2017) „Beam me up, Scotty“ – die Klassifizierung von Medical Apps als Medizinprodukte. PharmR: 433-435
- Wiesemann H, Mattheis C, Wende S. (2020) Software-Updates bei vernetzten Geräten. MMR:139-144
- Zezschwitz F. (2020) Neue regulatorische Herausforderungen für Anbieter von Gesundheits-Apps. MedR (38): 196–201. https://doi.org/10.1007/s00350-020-5482-6

Anhang 1: Hinweise zur Prüfung hinsichtlich der Umsetzung von Datenschutzanforderungen bei medizinischen Apps

Grundsätzlich müssen alle Anforderungen aus dem Datenschutzrecht wie beispielsweise Sicherheit der Verarbeitung oder Betroffenenrechte umgesetzt werden. Nur weil Apps auf mobilen Geräten eingesetzt werden, gibt es hier keine Abstriche bei den rechtlichen Anforderungen. Nachfolgend finden sich Hinweise, wie man einige Fragestellungen angehen kann, ohne dass das Thema der Prüfung abschließend beantwortet wird; eine Prüfung ist immer abhängig von der jeweiligen App, der Zecke der Verarbeitung mit der App sowie der eingesetzten Verarbeitung selbst.[119, 120]

1) Analyse des Ursprungslandes
   Unter „Ursprungsland" einer App wird der Standort des Entwicklers der App angesehen. Die jeweilige Region bzw. Land beinhaltet Anhaltspunkte für eine Beurteilung hinsichtlich des Datenschutzes und der Cybersicherheit aus Sicht des für den Entwickler geltenden Rechts. Beispielsweise gibt es Länder, welche in ihrem jeweiligen nationalen Recht Zugriffsmöglichkeiten auf Daten vorschreiben.
2) Analyse der Datenschutzerklärung
   2.1) Zunächst ist zu prüfen, ob die Datenschutzerklärung in der Sprache der adressierten Anwender vorliegt. Entsprechend Art. 12 DS-GVO müssen Informationen in transparenter, verständlicher und leicht zugänglicher Form zur Verfügung gestellt werden, was insbesondere die Nutzung der jeweiligen Landessprache voraussetzt. Eine in Deutschland angebotene App muss daher über eine Datenschutzerklärung in deutscher Sprache verfügen, andere Sprachen sind nur als Erweiterung anzusehen. Eine für deutsche Personen angebotene App ohne deutschsprachige Datenschutzerklärung entspricht nicht den Vorgaben von Art. 12 DS-GVO und ist daher aus datenschutzrechtlicher Sicht nicht rechtskonform einsetzbar.
   2.2) Zu prüfen ist auch, ob die Datenschutzerklärung in der jeweiligen Sprache verständlich vorliegt. Auch wenn computergestützte automatische Übersetzungen heute zum Teil schon eine gute Qualität aufweisen, kommen immer wieder sinnentstellende Übersetzungen vor. Die entsprechend Art. 12 DS-GVO geforderte Verständlichkeit für die Benutzer der App muss gegeben sein, damit beispielsweise eine Einwilligung als Erlaubnistatbestand rechtsgültig eingeholt bzw. abgegeben werden kann.
   2.3) In jeder Datenschutzerklärung muss beschrieben sein, welche Rechte betroffene Personen haben und wie diese gewährleistet werden. Den Informationspflichten aus Art. 13 DS-GVO bzw. ggf. auch aus Art. 14 DS-GVO muss mit der Datenschutzerklärung genügt werden, aber natürlich muss in einer Datenschutzerklärung auch beschrieben werden, wie

[119] Speziell zur Prüfung der IT-Sicherheit veröffentlichte OWASP
- Einen „Mobile Security Testing Guide", welcher auch Abschnitte zum Test von Apps unter iOS- und Android-Betriebssystemen enthält. Online, zitiert am 2022-07-20; verfügbar unter https://mobile-security.gitbook.io/mobile-security-testing-guide/
- Eine „Mobile App Security Checklist". Online, zitiert am 2022-07-20; verfügbar unter https://github.com/OWASP/owasp-mstg/releases/
- Einen „OWASP Web Security Testing Guide", der insbesondere bei Apps mit Sever-Backend gut eingesetzt werden kann, dessen Hinweise z. B. zu alten Backups oder den Test bzgl. Identity Management sehr gut auf alle Apps anwendbar, aber auch ansonsten gut auf Apps im Allgemeinen übertragbar ist. Online, zitiert am 2022-07-15; verfügbar unter: https://owasp.org/www-project-web-security-testing-guide/

[120] Siehe auch NIST Special Publication 800-163 Rev. 1 „Vetting the Security of Mobile Applications" (Stand 2019-04). Online, zitiert am 2022-08-18; verfügbar unter https://csrc.nist.gov/publications/detail/sp/800-163/rev-1/final

Betroffenenrechte wie beispielsweise Auskunft oder Löschen seitens des Verantwortlichen umgesetzt werden bzw. wie eine betroffene Person die von der DS-GVO garantierten Betroffenenrechte ausüben kann.

2.4) In der jeweiligen Datenschutzerklärung finden sich Informationen, welche Daten verarbeitet werden, welche Rechte eine App beansprucht usw. Eine Datenschutzerklärung stellt somit das „Soll“ dar, welches es zu prüfen gilt. Werden mehr Daten verarbeitet, andere Zwecke erfüllt usw. ist die App aus datenschutzrechtlicher Sicht abzulehnen.

2.5) Bestandteil jeder Datenschutzerklärung muss auch der Ort der Verarbeitung sein, gleichermaßen die Speicherdauer resp. wann Daten gelöscht werden. Werden Daten nur lokal auf dem Gerät verarbeitet? Werden Daten in einer Cloud verarbeitet? Wenn ja, wo ist der Ort der Speicherung? Erfolgt eine Verarbeitung in einem Drittland? Wenn ja, mit welchen Maßnahmen wird das europäische Schutzniveau gewährleistet, wo kann eine betroffene Person die entsprechenden Verträge anfordern? Diese und ähnliche Fragen muss die Datenschutzerklärung beantworten.

2.6) Eine App ohne Datenschutzerklärung ist grundsätzlich abzulehnen, außer sie verarbeitet keine Daten. Ein Beispiel:

Ein Body Mass Index Rechner App, in welcher nur Körpergewicht und Größe eingegeben und das Ergebnis angezeigt wird, welche aber keine Daten in irgendeiner Form speichert und insbesondere auch nicht übermittelt, könnte ohne Datenschutzerklärung auskommen, da keine personenbezogenen oder personenbeziehbare Daten verarbeitet werden, auch keine Rechte auf Speicher oder Systemressourcen benötigt werden.

Ein Cloud-basierter BMI-Rechner hingegen übermittelt stets zumindest die IP-Adresse zzgl. Gesicht und Körpergröße, was immer auch eine Verarbeitung personenbezogener Daten darstellt und somit eine Datenschutzerklärung voraussetzt.

3) Analyse der Berechtigungen der App

Betriebssysteme von mobilen Geräten beinhalten ein Berechtigungssystem[121], auf welche Daten (z. B. Standortdaten) oder Systemressourcen (z. B. Mikrofon) eine App zugreifen darf.

Die von einer App zum Betrieb angeforderten Berechtigungen müssen mit der in der Datenschutzerklärung angegebenen Zwecke korrespondieren. Stellt eine App beispielsweise die Anzeige der nächstgelegenen Apotheke als Funktion bereit, so ist ein Zugriff auf die Standortdaten nicht erforderlich, da die Position auch von Hand eingegeben werden kann. Ein Beispiel:

Die Nutzung von Standortdaten stellt eine Komfortfunktion dar, da hierdurch dem Benutzer der App die Eingabe erspart bleibt. Eine entsprechende App, die ohne Zugriff auf den Standort nicht funktioniert, entspricht daher nicht den Vorgaben von Art. 25 DS-GVO bzgl. Privacy by Default. Jedoch ist es statthaft, dem Benutzer bei der Einrichtung darüber aufzuklären, dass die App zwar ohne Zugriff funktioniert, wenn der Benutzer den Standort mittels Angabe von Straße, Ort und Land von Hand eingibt, eine komfortablere Bedienung jedoch möglich ist, wenn die App auf die Standortdaten zugreifen darf.

4) Analyse bzgl. eingesetzter Third-party Library bzw. SDK

Entwickler nutzen häufig Bibliotheken von Drittanbietern, sog. Third-party Libraries, oder auch Software Development Kits (SDK), die regelhaft Third-party Libraries bereitstellen. Mit diesen Programmbibliotheken können relativ leicht Funktionen in die App integriert werden, was die gesamte Entwicklung deutlich erleichtert und insbesondere auch eine deutliche Zeitersparnis bei

[121] Siehe
- Android: Permissions on Android. Online, zitiert am 2022-07-08; verfügbar unter https://developer.android.com/guide/topics/permissions/overview
- iOS: Program Roles. Online, zitiert am 2022-07-08; verfügbar unter https://developer.apple.com/support/roles/

der Entwicklung bedeutet. Typische Beispiele für entsprechende Bibliotheken bei auf Android basierenden mobile Apps sind „Google Firebase Analytics“ oder „Google Analytics“.
Sehr oft ist eine Nutzung dieser von Drittanbietern bereitgestellten Softwarebibliotheken jedoch nicht möglich, ohne den Drittanbietern zugleich auch einen gewissen Zugriff auf Daten zu ermöglichen, beispielsweise um Benutzern der App Werbung anzuzeigen oder Daten über die Nutzung der App bzw. Softwarebibliothek zu erhalten, was eine Weitergabe von Daten des Benutzers der App an den Drittanbieter bedeutet.
In der Datenschutzerklärung sind daher immer alle eingesetzten Bibliotheken von Drittanbietern anzugeben[122] und ggf. erfolgende Offenbarungen von Nutzerdaten an den Drittanbieter sowie die Verwendungszwecke des Drittanbieters anzugeben. Vielfach sind Anbieter entsprechender Programmbibliotheken in einem Drittland, also einem Land außerhalb der EU bzw. EWR, sodass es bei einer Weitergabe von Daten an den Hersteller der eingesetzten Programmbibliotheken zu einer Übermittlung entsprechend Kapitel V DS-GVO kommt und alle Vorgaben von Kap. V DS-GVO eingehalten werden müssen, was i. d. R. den Abschluss von Standardvertragsklauseln zur Drittland-Übermittlung inkl. zusätzliche getroffener Sicherheitsmaßnahmen zur Gewährleistung eines dem europäischen Recht entsprechenden Datenschutzniveaus bedeutet: Bei einer Prüfung von Apps mit dem Einsatz entsprechender Programmbibliotheken sind daher die entsprechenden Unterlagen von Auditoren, Datenschutzbeauftragten usw. anzufordern und zu prüfen.

5) Dynamische Code-Analyse
Besteht Anlass zu einer genaueren Prüfung (z. B. aufgrund eines entsprechenden hohen Risikos für Rechte und Freiheiten betroffener Personen), so ist eine dynamische Code-Analyse unter Nutzung entsprechender Softwareentwicklungs-Werkzeuge anzuraten. Die Analyse des Quellcodes ermöglicht die Beurteilung der Qualität der Softwareentwicklung, insbesondere können potenzielle Sicherheitsrisiken wie evtl. vorhandene Buffer Overflow Möglichkeiten gefunden werden. Aber eine Code-Analyse ermöglicht auch die Überprüfung, welche Programmbibliotheken von Drittanbietern eingesetzt werden, sodass hierdurch ein Abgleich mit den Angaben aus der Datenschutzerklärung ermöglicht wird, d. h. ein Ist-Soll-Abgleich.
6) Analyse der Kommunikation
Gibt es eine Kommunikation mit externen Adressen, so ist zu überprüfen, ob
    a) die Kommunikation entsprechend dem Stand der Technik verschlüsselt erfolgt und
    b) welche IP-Adressen angesprochen werden, um so zu prüfen, ob eine Kommunikation mit einem Drittland erfolgt.

Eine unverschlüsselte Kommunikation entspricht nicht den Vorgaben von Art. 32 DS-GVO und ist daher abzulehnen. Erfolgt eine Kommunikation mit einem in einem Drittland ansässigen Akteur, so ist zu prüfen, ob diese in der Datenschutzerklärung angegeben ist und ob die Vorgaben von Kap. V DS-GVO eingehalten wurden. Ist eins von beidem oder beides nicht der Fall, so erfolgt eine rechtswidrige Drittlandübermittlung und ein rechtskonformer Einsatz der App wird kaum möglich sein.

[122] In einigen Ländern besteht die Pflicht, sog. „Software Bill of Materials“ (SBOM) zu führen, so z. B. die USA (siehe https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/). SBOM listet alle Bestandteile eines Softwareprojektes auf, insbesondere auch interne und externe Abhängigkeiten wie Programmbibliotheken. Weitere Informationen z. B. bei der amerikanischen Cybersecurity and Infrastructure Security Agency (CISA). Online, zitiert am 2022-07-22; verfügbar unter https://www.cisa.gov/sbom

Anhang 2: Sichere App-Entwicklung: Top 10 der Best Practices

1. Schreiben Sie einen sicheren Code
Bugs und Schwachstellen in einem Code sind der am meisten genutzte Ausgangspunkt. Angreifer versuchen durch Reverse Engineering einer Anwendung Bugs und Schwachstellen in dieser zu finden. Mit diesen versuchen die Angreifer, Ihren Code so zu manipulieren, dass Angreifer Zugriff auf die Anwendung und die Daten bekommen.

Von Anfang an muss daher auf die Sicherheit des Codes und damit der Anwendung geachtet werden. Der Code muss gehärtet werden, sodass dieser schwer zu knacken ist. Hierzu wird Code minimiert und verschlüsselt, um so ein Reverse Engineering zu erschweren. Auch müssen Code und Anwendung gründlich und wiederholt getestet werden. Fehler müssen unverzüglich nach Auftauchen behoben werden, daher ist der Code so zu gestalten, dass dieser leicht zu aktualisieren und zu patchen ist. Elektronische Signaturen werden eingesetzt, sowohl um Manipulationen zu erkennen als auch dafür Sorge zu tragen, dass nur autorisierte Patches und Updates eingespielt werden können.

2. Verschlüsseln Sie alle Daten
Jede einzelne über Ihre Anwendung ausgetauschte Information muss dem Stand der Technik entsprechend verschlüsselt werden. Selbst wenn dann Daten gestohlen werden, so können Unbefugte die Informationen nicht lesen und missbrauchen.

3. Besondere Vorsicht bei der Verwendung von Bibliotheken
Werden Bibliotheken von Drittanbietern verwendet, ist doppelt Vorsicht unabdingbar. Der Code muss besonders gründlich getestet werden, bevor dieser Code von Dritten in der App verwendet wird.

Auch bekannte Bibliotheken wie die oft eingesetzte Bibliothek log4j[123] weisen immer wieder Sicherheitslücken auf, die von Angreifern genutzt werden. Daher muss beim Einsatz von Bibliotheken von Drittherstellern ein Monitoring vorhanden sein, welches entsprechende Mailinglisten auf das Bekanntwerden von Sicherheitslücken überprüft. Weiterhin müssen organisatorische Maßnahmen wie z. B. ein Produktrückruf existieren, welche eine Ausnutzung aufgetauchter Sicherheitslücken gerade bei dem Einsatz Bibliotheken von Drittanbietern wirksam verhindern.

4. Nur autorisierte APIs verwenden
APIs, die nicht freigegeben sind und schlecht programmiert sind, können einem Hacker ungewollt Privilegien gewähren, die schwerwiegend missbraucht werden können.

Beispielsweise ermöglicht das lokale Zwischenspeichern von Autorisierungsdaten wie z. B. Login-Daten Programmierern eine einfache Wiederverwendung dieser Informationen bei entsprechenden API-Aufrufen. Allerdings bietet dies auch Angreifern die Möglichkeit, durch die Nutzung dieser zwischengespeicherten Autorisierungsdaten Privilegien zu missbrauchen können.

Autorisierungsdaten müssen daher durch den Einsatz kryptographischer Verfahren so geschützt werden, dass Angreifer keine Möglichkeit bekommen, die Informationen zur Kenntnis nehmen zu können. Auch muss für eine entsprechende Validierung bei allen Autorisierungen gesorgt werden, damit Angreifer beispielsweise nicht einen ausgelesenen Hash-Wert als Passwort übergeben und die Anwendung den Hashwert als Passwort akzeptiert.

[123] Bundesamt für Sicherheit in der Informationstechnik (BS): Java-Bibliothek Log4j – eine Bilanz. Online, zitiert am 2022-07-22; verfügbar unter https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Schwachstelle-log4Shell-Java-Bibliothek/log4j_node.html

5. Hochgradige Authentifizierung einsetzen
Einige der größten Sicherheitsverstöße sind auf eine schwache Authentifizierung zurückzuführen. Daher wird es zunehmend wichtiger, eine starke Authentifizierung zu verwenden. Die Authentifizierung erfolgt durch Passwörter und andere persönliche Identifikatoren, mit denen sich Anwender gegenüber einer Anwendung oder einem Gerät authentifizieren. Ein großer Teil der Stärke der Authentifizierung hängt daher von den Endbenutzern der Anwendung selbst ab. Allerdings kann und sollte man Benutzer zu einem sensibleren Umgang mit der Authentifizierung anhalten.

Beispielsweise kann eine Anwendung so gestaltet werden, dass die Anwendung nur starke Passwörter akzeptieren, d. h. Passwörter, welche aus alphanumerischen Zeichen sowie Sonderzeichen bestehen und eine den Empfehlungen[124] von Sicherheitsexperten entsprechende Mindestlänge aufweisen. Unbedingt zu beachten: Wichtiger als die Komplexität des Passwortes oder die Häufigkeit des Passwortwechsels ist, dass Anwender sich ihr Passwort merken können!

6. Nutzung von Technologien zur Erkennung von Manipulationen
Es gibt Verfahren, die Benachrichtigungen auslösen, wenn ein Dritter versucht, Code zu manipulieren oder bösartigen Code in eine Anwendung einzuschleusen. Aktive Manipulationserkennung kann eingesetzt werden, um zu gewährleisten, dass der Code bzw. eine Anwendung im Falle einer unerwünschten bzw. ungewollten Manipulation nicht funktioniert.

7. Der Grundsatz der geringstmöglichen Rechte (Least Privilege)
Das Prinzip der geringstmöglichen Rechte besagt, dass ein Code bzw. die daraus resultierende Anwendung nur mit den Berechtigungen ausgeführt werden sollte, welche die Anwendung unbedingt benötigt. D. h. eine Anwendung sollte niemals mehr Berechtigungen anfordern als das zum Funktionieren der Anwendung absolut erforderliche Minimum. Insbesondere dürfen keine unnötigen Netzwerkverbindungen hergestellt werden. Bei jeder Aktualisierung des Codes muss eine Bedrohungsmodellierung erfolgen und ggf. versucht werden, die Rechte der Anwendung weiter einzuschränken.

8. Ordnungsgemäßes Session Handling anwenden
„Sessions“ dauern auf mobilen Geräten i. d. R. länger als auf Desktops. Das macht die Behandlung von Sessions für Server schwieriger. Zur Identifizierung einer Sitzung sollten Token anstelle von Geräte-Identifikatoren verwendet werden. Token können jederzeit widerrufen werden, was im Falle von verlorenen oder gestohlenen Geräten mehr Sicherheit bietet. Die Fernlöschung von Daten von einem verlorenen/gestohlenen Gerät und die Fernabmeldung sollten jederzeit möglich sein.

9. Die besten Kryptographie-Tools und -Methoden verwenden
Die Verwaltung von Schlüsseln ist beim Einsatz kryptographischer Verfahren entscheidend, wenn sich Maßnahmen zur Verschlüsselung auszahlen sollen. Schlüssel dürfen insbesondere niemals fest im Code implementiert werden, denn dies macht es Angreifern leicht, Zugriff auf die Schlüssel zu erhalten.

---

[124] Z. B.
- National Institute of Standards and Technology (NIST): Special Publication 800-63-3 - Digital Identity Guidelines. Online, zitiert am 2022-07-22; verfügbar unter https://pages.nist.gov/800-63-3/
- Bundesamt für Sicherheit in der Informationstechnik (BS): IT-Grundschutz - ORP.4 Identitäts- und Berechtigungsmanagement, ORP.4.A8, ORP.4.A22, ORP.4.A23. Online, zitiert am 2022-07-22; verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html bzw. pdf-Datei https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2022.pdf?__blob=publicationFile&v=3#download=1
-

Die Schlüssel müssen in sicheren Containern aufbewahrt und dürfen niemals lokal zugreifbar auf dem mobilen Gerät gespeichert werden.

Einige weithin akzeptierte und auch heute leider noch eingesetzte Verschlüsselungsprotokolle wie MD5 und SHA1 haben sich nach modernen Sicherheitsstandards als unzureichend erwiesen.

Nur nach Ansicht von Experten der Kryptographie anerkannte und vertrauenswürdige Methoden sollten eingesetzt werden [125], aktuell gehören dazu z. B. 256-Bit-AES-Verschlüsselung sowie SHA-256 für das Hashing.

10. Regelmäßige Tests durchführen

Die Gewährleistung der Sicherheit ist ein Prozess, der nie endet. Neue Bedrohungen tauchen auf und neue (Sicherheits-)Lösungen werden dann benötigt.

Daher muss auf jeden Fall in Penetrationstests, Bedrohungsmodellierung und Emulatoren investiert werden, um Anwendungen kontinuierlich auf Schwachstellen zu testen. Gefundene Schwachstellen müssen unverzüglich Anwendern mitgeteilt und mit einem Update bzw. Patch behoben werden.

[125] Insbesondere zu beachten Technische Richtlinie 02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI. Online, zitiert am 2022-07-22; verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html

Anhang 3: Beispiel für Datenschutzerklärung / Datenhinweise für Medical Apps

Hinweis 12: Im nachfolgenden Beispiel für Datenschutzhinweise im Einsatz für eine Mobile App wird nicht auf dem Einsatz von externen Tools eingegangen, die beispielsweise zur Reichweitenmessung oder zur sicheren Identifikation (z. B. Video Ident) eingesetzt werden, aber auch nicht auf Social Media Integration. Werden Tools von Drittanbietern (oder von Auftragsverarbeitern) eingesetzt, so müssen Informationen zu diesen Verarbeitungen wie auch zu den Herstellern/Betreibern ebenfalls in die Datenschutzhinweise aufgenommen werden.

Datenschutzhinweise des Unternehmens „Treue-Datenverarbeitung gGmbH

Unser Unternehmen nimmt den Schutz Ihrer personenbezogenen Daten ernst und möchten Sie an dieser Stelle über den Datenschutz in unserem Unternehmen informieren. Uns sind im Rahmen unserer datenschutzrechtlichen Verantwortlichkeit durch das Inkrafttreten der EU-Datenschutz-Grundverordnung (Verordnung (EU) 2016/679; nachfolgend: "DS-GVO") Pflichten auferlegt worden, um den Schutz personenbezogener Daten der von einer Verarbeitung betroffenen Person (wir sprechen Sie als betroffene Person nachfolgend auch mit "Kunde", "Nutzer", "Sie", "Ihnen" oder "Betroffener" an) sicherzustellen.

Im Rahmen der Nutzung unserer App erhalten Sie folgende Leistungen von uns: [Leistungsbeschreibung der App].

Soweit wir entweder alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheiden, umfasst dies vor allem die Pflicht, Sie transparent über Art, Umfang, Zweck, Dauer und Rechtsgrundlage der Verarbeitung zu informieren (vgl. Art. 12, Art. 13 und Art. 14 DS-GVO). Mit dieser Erklärung informieren wir Sie darüber, in welcher Weise Ihre personenbezogenen Daten von uns verarbeitet werden und welche Rechte Sie haben.

1. Verantwortlicher für Datenverarbeitung

Wir stellen Ihnen eine mobile App zur Verfügung, die Sie auf Ihr mobiles Endgerät herunterladen können. Im Folgenden informieren wir über die Erhebung personenbezogener Daten bei Nutzung unserer mobilen App. Personenbezogene Daten sind alle Daten, die auf Sie persönlich beziehbar sind, z. B. Name, Adresse, E-Mail-Adressen, Nutzerverhalten.

Verantwortlicher gem. Art. 4 Abs. 7 EU-Datenschutz-Grundverordnung (DS-GVO) ist:

Name,
Ladungsfähige Anschrift,
Telefonnummer,
ggf. Faxnummer
E-Mail-Adresse

(Siehe auch unser Impressum).

2. Kontaktdaten bei Datenschutzfragen

Unseren Datenschutzbeauftragten erreichen Sie unter datenschutz@beispiel.de oder unter unserer postalischen Anschrift. Bei Nutzung unserer postalischen Anschrift verwenden sie bitte den Zusatz „Datenschutzbeauftragte“ im Adressfeld, damit die bei uns eingehende Post in unserer zentralen Postannahme entsprechend vertraulich behandelt wird.

Bei Fragen oder Anmerkungen zur Verarbeitung Ihrer personenbezogenen Daten ist unser Datenschutzbeauftragter unser kompetentester Ansprechpartner. Entsprechend den rechtlichen

Vorgaben gehört Ihre Beratung zu allen mit der Verarbeitung Ihrer personenbezogenen Daten und mit der Wahrnehmung Ihrer Rechte zusammenhängenden Fragen zu seinen direkten Aufgaben. Auch ist ein Datenschutzbeauftragter entsprechend den Vorgaben der DS-GVO bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden.

Wenden Sie sich bitte an unseren Datenschutzbeauftragten, wenn Sie die Ihnen zustehenden Rechte, die im nachfolgenden Kapitel dargestellt werden, uns gegenüber geltend machen wollen. Nur in diesem Falle ist die schnellstmögliche und sachgerechte Bearbeitung Ihrer Anfrage, die uns möglich ist, gewährleistet.

3. Ihre Rechte („Betroffenenrechte“)

Sie haben gegenüber uns folgende Rechte hinsichtlich der Sie betreffenden personenbezogenen Daten:

- Recht auf Auskunft
  Sie haben das Recht, von uns jederzeit auf Antrag eine Auskunft über die von uns verarbeiteten, Sie betreffenden personenbezogenen Daten im Umfang des Art. 15 DS-GVO zu erhalten. Hierzu können Sie einen Antrag postalisch oder per E-Mail stellen, idealerweise gerichtet an unseren Datenschutzbeauftragten.
- Recht auf Berichtigung
  Sie haben das Recht, von uns die unverzügliche Berichtigung der Sie betreffenden personenbezogenen Daten zu verlangen, sofern diese unrichtig sein sollten. Wenden Sie sich hierfür bitte postalisch oder per E-Mail an unseren Datenschutzbeauftragten.
- Recht auf Löschung
  Sie haben das Recht, in bestimmten Fällen im Rahmen des Art. 17 DS-GVO die Löschung von Daten zu verlangen, insbesondere soweit die Daten für den vorgesehenen Zweck nicht mehr erforderlich sind bzw. unrechtmäßig verarbeitet werden, oder Sie Ihre Einwilligung widerrufen oder einen Widerspruch erklärt haben. Zum Zeitraum der Datenspeicherung verweisen wir insbesondere auch auf Ziffer 10 dieser Datenschutzhinweise. Um Ihr Recht auf Löschung geltend zu machen, wenden Sie sich bitte postalisch oder per E-Mail an unseren Datenschutzbeauftragten.
- Recht auf Einschränkung der Verarbeitung
  Sie haben unter bestimmten Voraussetzungen das Recht, von uns die Einschränkung der Verarbeitung zu verlangen (Art. 18 DS-GVO). Dieses Recht besteht insbesondere, wenn
  - die Richtigkeit der personenbezogenen Daten zwischen dem Nutzer und uns umstritten ist, für die Dauer, welche die Überprüfung der Richtigkeit erfordert,
  - sowie im Fall, dass der Nutzer bei einem bestehenden Recht auf Löschung anstelle der Löschung eine eingeschränkte Verarbeitung verlangt;
  - ferner für den Fall, dass die Daten für die von uns verfolgten Zwecke nicht länger erforderlich sind, der Nutzer sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt
  - sowie, wenn die erfolgreiche Ausübung eines Widerspruchs zwischen uns und dem Nutzer noch umstritten ist.

  Um Ihr Recht auf Einschränkung der Verarbeitung geltend zu machen, wenden Sie sich bitte postalisch oder per E-Mail an unseren Datenschutzbeauftragten.
- Recht auf Datenübertragbarkeit
  Sie haben das Recht, von uns die Sie betreffenden personenbezogenen Daten, die Sie uns bereitgestellt haben, in einem strukturierten, gängigen, maschinenlesbaren Format nach Maßgabe des Art. 20 DS-GVO zu erhalten. Um Ihr Recht auf Datenübertragbarkeit geltend zu

machen, wenden Sie sich bitte postalisch oder per E-Mail an unseren Datenschutzbeauftragten.

- Recht auf Widerspruch gegen die Verarbeitung
  Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die u. a. aufgrund von Art. 6 Abs. 1 lit. e oder lit. f DS-GVO erfolgt, Widerspruch nach Art. 21 DS-GVO einzulegen. Wir werden die Verarbeitung Ihrer personenbezogenen Daten einstellen, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder wenn die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Um Ihr Recht auf Widerspruch gegen die Verarbeitung geltend zu machen, wenden Sie sich bitte postalisch oder per E-Mail an unseren Datenschutzbeauftragten.
- Recht auf Widerruf einer Einwilligung
  Sie haben das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.
- Recht auf Beschwerde bei einer Aufsichtsbehörde
  Sie haben ferner das Recht, sich bei Beschwerden an eine Aufsichtsbehörde zu wenden.

4. Keine Verpflichtung Ihrerseits zur Bereitstellung personenbezogener Daten

Wir machen den Abschluss von Verträgen mit uns nicht davon abhängig, dass Sie uns zuvor personenbezogene Daten bereitstellen. Für Sie als Kunde und Nutzer unserer App besteht grundsätzlich auch keine gesetzliche oder vertragliche Verpflichtung, uns Ihre personenbezogenen Daten zur Verfügung zu stellen, abgesehen von den Daten, die zwingend für den Abschluss eines Vertrages zum Kauf unserer App sowie deren Bezahlung erforderlich sind.

Es kann jedoch sein, dass wir bestimmte Angebote nur eingeschränkt oder gar nicht erbringen können, wenn Sie die dafür erforderlichen Daten nicht bereitstellen. Insbesondere kann unsere App bestimmte Funktionen nur bereitstellen und Ihnen entsprechende Ergebnisse liefern, wenn der App entsprechende Informationen bereitgestellt werden.

5. Verarbeitung personenbezogener Daten bei Nutzung unserer mobilen App

5.1. Datenerhebung bei der Kontaktaufnahme

Bei Ihrer Kontaktaufnahme mit uns per E-Mail oder über ein Kontaktformular wird Ihr Name und Ihre E-Mail-Adresse und, falls Sie von Ihnen angegeben werden, Ihre Telefonnummer von uns gespeichert, um Ihre Fragen zu beantworten. Die in diesem Zusammenhang anfallenden Daten löschen wir, nachdem die Speicherung nicht mehr erforderlich ist, oder – im Falle von gesetzlichen Aufbewahrungspflichten – schränken die Verarbeitung ein.

5.2. Download der App

Bei Herunterladen der mobilen App werden die erforderlichen Informationen an den App Store übertragen, also insbesondere Nutzername, E-Mail-Adresse und Kundennummer Ihres Accounts, Zeitpunkt des Downloads, Zahlungsinformationen und die individuelle Gerätekennziffer. Auf diese Datenerhebung haben wir keinen Einfluss und sind nicht dafür verantwortlich; die Verantwortung dafür liegt allein beim App Store. Wir verarbeiten die Daten nur, soweit es für das Herunterladen der mobilen App auf Ihr mobiles Endgerät notwendig ist.

Optional: Diese mobile App können Sie zudem kostenlos über unsere Website direkt auf Ihr mobiles Endgerät laden. Bei Download werden über die Website weitere Nutzerdaten verarbeitet, über die wir in der Datenschutzerklärung unserer Website, welche sie unter der URL „xyz“ einsehen können, informieren.

5.3. Datenverarbeitung bei Nutzung der App

Die Vorzüge unserer App können wir Ihnen zwangsläufig nur zur Verfügung stellen, wenn bei der Nutzung für den App-Betrieb erforderliche Daten zu Ihrer Person erhoben und verarbeitet werden. Wir erheben diese Daten nur, wenn diese Daten für die Funktionsfähigkeit der App erforderlich sind.

Für die Nutzung der App ist die Erstellung eines Nutzerkontos erforderlich. Dafür geben Sie mindestens Ihren Anmeldenamen und ein Passwort an. Das Passwort wird in Form eines sogenannten „Hash-Wertes" gespeichert. Ein Hashwert ist ein berechneter Wert, der für jedes Passwort eindeutig berechnet wird, aber aus dem selbst das Passwort selbst nicht berechnet werden kann (sog. „Einweg-Funktion"). Daher kennen wir Ihr Passwort nicht und können es im Falle eines Verlustes auch nicht wiederherstellen. Damit im Falle eines Verlustes des Passwortes das Passwort wieder zurückgesetzt werden kann, werden weitergehende Informationen abgefragt, die nur Sie kennen (z. B. den Namen einer bestimmten Bezugsperson).

Bei Nutzung der mobilen App erheben wir die nachfolgend beschriebenen personenbezogenen Daten, um die komfortable Nutzung der Funktionen zu ermöglichen. Wenn Sie unsere mobile App nutzen, erheben wir die folgenden Daten, die für uns technisch erforderlich sind, um Ihnen die Funktionen unserer mobilen App anzubieten und die Stabilität und Sicherheit zu gewährleisten, sofern Sie in diese Verarbeitung einwilligen (Rechtsgrundlage ist Art. 9 Abs. 2 lit. a DS-GVO): (Nicht Zutreffendes streichen)

- IP-Adresse
- Datum und Uhrzeit der Anfrage
- Zeitzonendifferenz zur Greenwich Mean Time (GMT)
- Inhalt der Anforderung
- Zugriffsstatus/HTTP-Statuscode
- jeweils übertragene Datenmenge
- Website, von der die Anforderung kommt
- Versions- sowie Patchstand der App,
- Betriebssystem und dessen Oberfläche,
- eindeutige Nummer des Endgerätes (IMEI = International Mobile Equipment Identity),
- eindeutige Nummer des Netzteilnehmers (IMSI = International Mobile Subscriber Identity),
- Mobilfunknummer (MSISDN),
- MAC-Adresse bei WLAN-Nutzung,
- Name Ihres mobilen Endgerätes,
- Hier die medizinischen Daten hinzufügen, die verarbeitet werden.

Falls zutreffend: Die mobile App wird ausschließlich auf Ihrem mobilen Endgerät geladen und betrieben. Die App kann ohne Zugriff auf das Internet verwendet werden. Bei ihrer Nutzung werden keine personenbezogenen Daten erhoben.

5.4. Zugriff auf Schnittstellen/Funktionen Ihres Endgerätes

Zu Beginn der Nutzung unserer mobilen App bitten wir Sie in einem Pop-up um die Erlaubnis zur Nutzung

- Internetzugriffs: Dieser wird benötigt, um (genaue Angabe, z. B. Ihre Eingaben auf unseren Servern zu speichern, Informationen von unseren Servern abzurufen).
- Kamera: Dieser wird benötigt, damit Sie Fotos anfertigen und in der App (falls zutreffend) sowie auf unseren Servern speichern können.
- Gespeicherte Dokumente: Dies wird benötigt, um auf erstellte Dokumente zugreifen und in der App anzeigen zu können.
- …

Diese Verarbeitung und Verwendung von Daten erfolgt ausschließlich zur Bereitstellung des Dienstes. Wenn Sie die Erlaubnis nicht erteilen, nutzen wir diese Daten nicht und Sie können in diesem Fall nicht alle Funktionen unserer App nutzen. Sie können die Erlaubnis später in den Einstellungen der App oder auch des Betriebssystems widerrufen oder bei erfolgtem Widerruf der App die Rechte auch wieder erteilen.

Wenn Sie den Zugriff auf diese Daten gestatten, wird die mobile App nur auf Ihre Daten zugreifen (falls zutreffend und die Daten auf unseren Server übertragen), soweit es für die Erbringung der Funktionalität der App notwendig ist, z. B., um Sie an Termine zu erinnern. Ihre Daten werden von uns vertraulich behandelt und gelöscht, wenn Sie die Rechte zur Nutzung widerrufen oder diese Daten zur Erbringung der Leistungen nicht mehr erforderlich sind und keine rechtlichen Aufbewahrungspflichten bestehen. Rechtsgrundlage ist Art. 9 Abs. 2 lit. a DS-GVO.

5.5. Zugriff auf Schnittstellen/Funktionen externer Geräte (falls zutreffend)

Über … (Beschreibung der Verbindung wie bspw. Bluetooth Pairing) wird Ihr Endgerät mit einem zusätzlichen Gerät verbunden, damit die mit diesem Zusatzgerät … (Angabe welches Gerät, beispielsweise ein Blutdruckmessgerät) erhobene Daten in Ihrer App verarbeitet werden können.

5.6. Erstellung eines Nutzeraccounts (Registrierung)

Bei Anlage eines Nutzeraccounts werden sogenannte „Pflichtangaben“ erhoben. Pflichtangaben im Rahmen der Registrierung sind mit einem Sternchen gekennzeichnet und sind für den Abschluss des Nutzungsvertrages erforderlich. Hierzu gehören insbesondere Ihre Zugangsdaten, dies sind Nutzername/E-Mail-Adresse (nicht Zutreffendes löschen) und Ihr Passwort), um Ihnen den Zugang zu Ihrem Nutzeraccount zu gewähren und diesen zu verwalten. Wenn Sie diese Pflichtangaben nicht angeben, können Sie keinen Nutzeraccount erstellen. Darüber hinaus können Sie folgende freiwillige Angaben im Rahmen der Registrierung machen.

Die Pflichtangaben verwenden wir ausschließlich, um Sie beim Login zu authentifizieren und Anfragen zur Rücksetzung Ihres Passwortes nachzugehen. Die von Ihnen im Rahmen der Registrierung oder einer Anmeldung eingegebenen Daten werden von uns nur verarbeitet,

1. um Ihre Berechtigung zur Verwaltung des Nutzeraccounts zu verifizieren;
2. die Nutzungsbedingungen der App sowie alle damit verbundenen Rechte und Pflichten durchzusetzen und
3. mit Ihnen in Kontakt zu treten, um Ihnen technische oder rechtliche Hinweise, Updates, Sicherheitsmeldungen oder andere Nachrichten, die etwa die Verwaltung des Nutzeraccounts betreffen, senden zu können.

Freiwillige Angaben verwenden wir, um diese entsprechend den von Ihnen vorgenommenen Einstellungen im Rahmen der App anzuzeigen (z. B. ein Foto zu Ihrem Namen). (Falls zutreffend) Auf Ihren Wunsch hin zeigen wir diese Informationen auch anderen Nutzern der App an.

Rechtsgrundlage ist Art. 9 Abs. 2 lit. a DS-GVO.

5.7. Verwendung von Cookies

Falls Cookies genutzt werden

Zusätzlich zu den zuvor genannten Daten werden bei Ihrer Nutzung unserer mobilen App Cookies auf Ihrem Rechner gespeichert. Bei Cookies handelt es sich um kleine Textdateien, die im Gerätespeicher Ihres mobilen Endgerätes abgelegt und der von Ihnen verwendeten mobilen App zugeordnet gespeichert werden. Durch Cookies fließen uns Informationen zu, welche die mobile App leichter bedienbar machen, z. B. um die Anmeldung an der App zu speichern und so zu verhindern, dass sie sich bei jedem Seitenwechsel neu anmelden müssen. Cookies können keine Programme ausführen oder Viren auf Ihr mobiles Endgerät übertragen. Rechtsgrundlage ist Art. 9 Abs. 2 lit. a DS-GVO.

Man unterscheidet zwischen Session-Cookies, die wieder gelöscht werden, sobald Sie die Anwendung beendet wird, und permanenten Cookies, die über die einzelne Sitzung hinaus gespeichert werden. Hinsichtlich ihrer Funktion unterscheidet man bei Cookies wiederum zwischen:

- Technischen Cookies: Diese sind zwingend erforderlich, um sich innerhalb der App zu bewegen, grundlegende Funktionen zu nutzen und die Sicherheit der App zu gewährleisten; sie sammeln weder Informationen über Sie zu Marketingzwecken noch speichern sie, welche Webseiten Sie ggf. besucht haben;
- Performance Cookies: Diese sammeln Informationen darüber, wie Sie unsere App nutzen, welche Seiten Sie besuchen und ob Fehler bei der App-Nutzung auftreten. Sie sammeln keine Informationen, die Sie identifizieren könnten – alle gesammelten Informationen sind anonym und werden nur verwendet, um unsere App zu verbessern und herauszufinden, was unsere Nutzer interessiert.
- Advertising Cookies, Targeting Cookies: Diese dienen dazu, dem Nutzer der App bedarfsgerechte Werbung innerhalb der App oder Angebote von Dritten anzubieten und die Effektivität dieser Angebote zu messen; Advertising und Targeting Cookies werden maximal 13 Monate lang gespeichert. **Falls zutreffend:** Diese Art der Cookies wird von uns nicht verwendet.
- Sharing Cookies: Diese dienen dazu, die Interaktivität unserer App mit anderen Diensten (z. B. sozialen Netzwerken) zu verbessern; Sharing Cookies werden maximal 13 Monate lang gespeichert. **Falls zutreffend:** Diese Art der Cookies wird von uns nicht verwendet.

Falls keine Cookies genutzt werden
Die mobile App setzt keine Cookies ein.

5.8. Erhebung Ihrer Standortdaten

Unsere App nutzt sogenannte Location Based Services, mit welchen wir Ihnen spezielle Angebote bieten, die auf Ihren jeweiligen Standort zugeschnitten sind. Diese Funktionen können Sie erst nutzen, nachdem Sie über ein Pop-up zugestimmt haben, dass wir zu Zwecken der Leistungserbringung Ihre Standortdaten mittels GPS und Ihre IP-Adresse erheben können. Sie können die Funktion in den Einstellungen der App oder Ihres Betriebssystems jederzeit erlauben oder widerrufen. Ihr Standort wird nur an uns übertragen, wenn Sie bei Nutzung der App Funktionen in Anspruch nehmen, die wir Ihnen nur bei Kenntnis Ihres Standortes anbieten können. Rechtsgrundlage ist Art. 9 Abs. 2 lit. a DS-GVO.

5.9. Datenverarbeitung zu Werbezwecken

Möglichkeit 1
Für Werbezwecke nutzen wir sog. „Advertising Identifier“ (IDFA). Dies ist eine einzigartige, jedoch nicht-personalisierte und nicht dauerhafte Identifizierungsnummer für ein bestimmtes Endgerät. Die über den IDFA erhobenen Daten werden nicht mit sonstigen gerätebezogenen Informationen verknüpft. Den IDFA verwenden wir, um Ihnen personalisierte Werbung bereitzustellen und Ihre Nutzung auswerten zu können. Wenn Sie in den Einstellungen Ihres Mobilgerätes die Option „kein Ad-Tracking“ aktivieren, erfolgt selbstverständlich keine Nutzung der IDFA. Sie können in den Geräteeinstellungen jederzeit den IDFA löschen („Ad-ID zurücksetzen“), dann wird ein neuer IDFA erstellt, der nicht mit den früher erhobenen Daten zusammengeführt wird. Wir weisen Sie darauf hin, dass Sie eventuell nicht alle Funktionen unserer App nutzen können, wenn Sie die Nutzung des IDFA beschränken. Rechtsgrundlage ist Art. 9 Abs. 2 lit. a DS-GVO.

Möglichkeit 2
Eine Verarbeitung Ihrer Daten zu Werbezwecken findet nicht statt.

5.10. Verarbeitung durch Dienstleister

Wie bei jedem Unternehmen, setzen auch wir zur Abwicklung unseres Geschäftsverkehrs externe in- und ausländische Dienstleister ein (z. B. für die Bereiche IT, Logistik, Telekommunikation, Vertrieb und Marketing). Diese werden nur nach unserer Weisung tätig und wurden entsprechend den Vorgaben von Art. 28 DS-GVO vertraglich dazu verpflichtet, die datenschutzrechtlichen Bestimmungen einzuhalten.

6. Empfänger, die ggf. Zugriff auf Ihre Daten bekommen

Folgende Kategorien von Empfängern, bei denen es sich im Regelfall um Auftragsverarbeiter handelt, erhalten ggf. Zugriff auf Ihre personenbezogenen Daten:

- Dienstleister für den Betrieb unserer App und die Verarbeitung der durch die Systeme gespeicherten oder übermittelten Daten wie beispielsweise für Rechenzentrumsleistungen oder Zahlungsabwicklungen. Hierbei handelt es sich grundsätzlich um eine Verarbeitung in unserem Auftrag. („Auftragsverarbeitung“)
- Staatliche Stellen/Behörden, soweit dies zur Erfüllung einer gesetzlichen Verpflichtung erforderlich ist. Rechtsgrundlage für die Weitergabe ist dann Art. 6 Abs. 1 lit. c DS-GVO bzw. Art. 9 Abs. 2 lit. g DS-GVO.

Darüber hinaus geben wir Ihre personenbezogenen Daten nur an Dritte weiter, wenn Sie eine ausdrückliche Einwilligung dazu erteilt haben.

Im Rahmen der Weiterentwicklung unseres Geschäfts kann es dazu kommen, dass sich die Struktur unseres Unternehmens wandelt, indem die Rechtsform geändert wird, Tochtergesellschaften, Unternehmensteile oder Bestandteile gegründet, gekauft oder verkauft werden. Bei solchen Transaktionen werden die Kundeninformationen gegebenenfalls zusammen mit dem zu übertragenden Teil des Unternehmens im Rahmen der sogenannten „Rechtsnachfolge“ weitergegeben. Bei jeder Weitergabe von personenbezogenen Daten an Dritte im beschriebenen Umfang tragen wir dafür Sorge, dass dies in Übereinstimmung mit diesen Datenschutzhinweisen und dem anwendbaren Datenschutzrecht erfolgt.

7. Zweckänderungen

Verarbeitungen Ihrer personenbezogenen Daten zu anderen als den beschriebenen Zwecken erfolgen nur, soweit eine Rechtsvorschrift dies erlaubt oder Sie in den geänderten Zweck der Datenverarbeitung eingewilligt haben. Im Falle einer Weiterverarbeitung zu anderen Zwecken als denen, für den die Daten ursprünglich erhoben worden sind, informieren wir Sie vor der Weiterverarbeitung über diese anderen Zwecke und stellen Ihnen sämtliche weitere hierfür maßgeblichen Informationen zur Verfügung.

8. Push-Nachrichten (falls zutreffend)

Push-Benachrichtigungen sind Nachrichten, die von der App auf Ihr Gerät gesendet und dort priorisiert dargestellt werden. Diese App verwendet Push-Benachrichtigungen im Auslieferungszustand, sofern Sie bei der App-Installation oder bei der ersten Nutzung eingewilligt haben. Rechtsgrundlage ist Art. 6 Abs. 1 lit. a DS-GVO bzw. Art. 9 Abs. 2 lit. a DS-GVO.

9. Verarbeitung in Drittländern

Möglichkeit 1

Zur Erbringung unserer Dienstleistungen im Rahmen der App-Nutzung nutzen wir auch Dienstleister außerhalb des europäischen Wirtschaftsraums (EWR), also in Drittländern. Eine derartige Verarbeitung erfolgt ausschließlich zur Erfüllung der vertraglichen und geschäftlichen Verpflichtungen und erfolgt nur im erforderlichen Umfang.

Einigen Drittländern bescheinigt die Europäische Kommission durch sog. Angemessenheitsbeschlüsse einen Datenschutz, der dem EWR-Standard vergleichbar ist (eine Liste dieser Länder sowie eine Kopie

der Angemessenheitsbeschlüsse erhalten Sie hier: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).

In anderen Drittländern, in die ggf. personenbezogene Daten übertragen werden, herrscht aber unter Umständen wegen fehlender gesetzlicher Bestimmungen kein durchgängig hohes Datenschutzniveau. Soweit dies der Fall ist, achten wir darauf, dass der Datenschutz ausreichend gewährleistet ist. Hierzu setzen wir die Standardvertragsklauseln der Europäischen Kommission ein (Die Standardvertragsklauseln zur Drittlandübermittlung finden Sie unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32021D0914).

Sie haben aufgrund Klausel 8.3 das Recht, bei Einsatz von Auftragsverarbeitern in Drittländern unter Verwendung der Standardvertragsklauseln auf Anfrage vom sogenannten Datenexporteur (die Partei, welche die Standardvertragsklauseln mit dem Dienstleister im Drittland abgeschlossen hat) eine Kopie dieser Klauseln, einschließlich der von den Parteien ausgefüllten Anlage(n), unentgeltlich zur Verfügung gestellt zu bekommen. Falls Sie eine Kopie erhalten wollen, wenden Sie sich auch für diese Anfragen bitte an unseren Datenschutzbeauftragten.

Im Rahmen der Nutzung unserer App erfolgt eine Verarbeitung in Drittstaaten. Dies betrifft im Einzelnen:

1) …

Möglichkeit 2

Eine Verarbeitung in Drittländern, d. h. eine Verarbeitung außerhalb des Europäischen Wirtschaftsraums (EWR), erfolgt nicht.

10. Speicherung und Löschung Ihrer Daten

Wir löschen oder anonymisieren Ihre personenbezogenen Daten, sobald sie für die Zwecke, für die wir sie entsprechend den Erläuterungen in diesen Datenhinweisen erhoben oder verwendet haben, nicht mehr erforderlich sind. In der Regel speichern wir Ihre personenbezogenen Daten für die Dauer des Nutzungs- bzw. des Vertragsverhältnisses über die App zzgl. eines Zeitraumes von …, während welchem wir nach der Löschung Sicherungskopien (sogenannte „Backups“) aufbewahren.

Sie selbst haben jederzeit die Möglichkeit, in der App eine Löschung zu veranlassen. Wir weisen darauf hin, dass nach einer Löschung Daten von uns nicht mehr wiederhergestellt werden können, die Daten also immer unumkehrbar gelöscht werden.

Eine Speicherung kann jedoch über die angegebene Zeit hinaus und auch im Falle einer von Ihnen veranlassten Löschung im Falle einer (drohenden) Rechtsstreitigkeit mit Ihnen oder eines sonstigen rechtlichen Verfahrens erfolgen.

Von uns eingesetzte Dritte (sog. „Auftragsverarbeiter“) werden Ihre Daten auf deren System so lange speichern, wie es im Zusammenhang mit der Erbringung der Leistung für uns entsprechend dem jeweiligen Auftrag erforderlich ist.

Rechtliche Vorgaben wie beispielsweise § 257 Handelsgesetzbuch zur Aufbewahrung und Löschung personenbezogener Daten bleiben von Vorstehendem unberührt. Wenn die durch die gesetzlichen Vorschriften vorgeschriebene Speicherfrist abläuft, erfolgt eine Sperrung oder Löschung der personenbezogenen Daten, es sei denn, dass eine weitere Speicherung durch uns erforderlich ist und dafür eine Rechtsgrundlage besteht.

Eine Speicherung Ihrer Daten erfolgt:

☐ Auf Servern in Deutschland.

- ☐ Auf Servern in der EU, ein Zugriff aus einem Drittland, auch von staatlichen Behörden eines Drittlands, ist ausgeschlossen.
- ☐ Auf Servern in der EU, ein Zugriff aus einem Drittland, auch von staatlichen Behörden eines Drittlands, ist nicht ausgeschlossen.
- ☐ auf unseren Servern in Drittstaaten.

11. Datensicherheit

Wir bedienen uns geeigneter technischer und organisatorischer Sicherheitsmaßnahmen, um Ihre Daten gegen zufällige oder vorsätzliche Manipulationen, teilweisen oder vollständigen Verlust, Zerstörung oder gegen den unbefugten Zugriff Dritter zu schützen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für Sie bzw. den Auswirkungen von Sicherheitsvorfällen wie beispielsweise Datenpannen für Sie.

Unsere Sicherheitsmaßnahmen werden entsprechend der technologischen Entwicklung fortlaufend weiterentwickelt.

Nähere Informationen hierzu erteilen wir Ihnen auf Anfrage gerne. Wenden Sie sich hierzu bitte an unseren Datenschutzbeauftragten.

12. Von Drittanbietern eingesetzte Tools

Um die Funktionalität unserer App bereitstellen zu können, nutzen wir von anderen (sogenannte „Drittanbieter“) bereitgestellte Möglichkeiten wie Software-Tools oder Hardware-Geräte. Im Einzelnen setzen wir ein:

Firma	Zweck	Speicherdauer	Ort der Verarbeitung	Zugriff auf Daten möglich

13. Änderung der Datenschutzhinweise

Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen werden unsere Datenschutzhinweise regelmäßig auf Anpassungs- oder Ergänzungsbedarf hin überprüft. Über Änderungen werden Sie unterrichtet.

Diese Datenschutzhinweise haben den Stand von ..... (Monat und Jahr der Veröffentlichung der Datenschutzhinweise).

Anhang 4: Hinweise zur Planung von Maßnahmen zur Umsetzung der Anforderungen von Datenschutz und IT-Sicherheit

Anlage 4.1. Hinweise bzgl. Maßnahmen vor Beginn der Entwicklung einer App

Vorgehen/Maßnahme	(Kurz-) Beschreibung	Adressierte Anforderung
Identifizierung von - Art, - Umfang, - Umstände und - Zwecke der Verarbeitung	Die konkreten Merkmale der Verarbeitung personenbezogener Daten sollte analysiert und dokumentiert werden.	Grundlage für das gesamte weitere Vorgehen
Identifizierung der erforderlichen Datenarten	Basierend auf der Identifizierung von Art, Umfang, Umstände und Zwecke der Verarbeitung sollten die zwingend erforderlichen Datenarten bestimmt werden. Die erforderlichen Datenarten sowie die Begründung der Erforderlichkeit sollten dokumentiert werden. Besonders sensible Daten, insbesondere in Art. 9 Abs. 1 DS-GVO genannte Datenkategorien, sollten identifiziert und entsprechend gekennzeichnet werden, damit der besonders hohe Schutzbedarf immer direkt gesehen und bei Planung sowie Implementierung entsprechend berücksichtigt wird. Hinweis: Erforderlich bedeutet „ohne diese Daten kann Anwendung nicht Funktion nicht erfüllen“	Rechtmäßigkeit, Zweckbindung, Datenminimierung, Rechenschaftspflicht
Identifizierung der Rechtsgrundlage der Verarbeitung	Es sollte die Rechtsgrundlage identifiziert werden, aufgrund derer personenbezogene Daten verarbeitet werden dürfen. Das Ergebnis sollte dokumentiert werden.	Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Rechenschaftspflicht
Durchführung einer Analyse der gesetzlichen Vorgaben	Es sollten die geltenden rechtlichen Anforderungen analysiert und in Bezug auf die geplante Anwendung bewertet werden.	Rechtssicherheit, Rechtmäßigkeit
Dokumentation aller Aktivitäten zur Einhaltung der gesetzlichen Vorgaben	Es sollten die Compliance-Aktivitäten dokumentiert werden, um der Rechenschaftspflicht zu genügen.	Rechenschaftspflicht
Bewertung des Stands der Technik	Es sollte evaluiert werden, was für die geplante Anwendung dem Stand der Technik entspricht.	Unter Berücksichtigung des Stands der Technik
Risikoanalyse	Es sollten die Risiken für die Rechte und Freiheiten der von der Verarbeitung betroffenen Personen analysiert und bewertet werden. Die Erforderlichkeit einer Datenschutz-Folgenabschätzung sollte beurteilt und dokumentiert werden, ggf. eine Datenschutz-Folgenabschätzung durchgeführt werden.	Verarbeitung nach Treu und Glauben, Sicherheit der Verarbeitung, insbesondere Integrität und Vertraulichkeit, Datenschutz-

Vorgehen/Maßnahme	(Kurz-) Beschreibung	Adressierte Anforderung
		Folgenabschätzung
Budgetierung	Es sollten die Kosten für die Planung und Umsetzung der Anforderungen aus den Bereichen Datenschutz und IT-Sicherheit abgeschätzt und entsprechende Ressourcen für die Durchführung der Maßnahmen bereitgestellt werden.	
Prüfung, ob Auftragsverarbeiter eingesetzt werden (müssen)	Es sollte geprüft werden, ob Auftragsverarbeiter eingesetzt werden, z. B. für die Bereitstellung von Serverleistungen. Ist dies der Fall, müssen Verträge zur Auftragsverarbeitung abgeschlossen werden.	Auftragsverarbeitung, Rechenschaftspflicht
Audit der Verarbeiter und Dritter	Werden Auftragsverarbeiter oder Dritte eingesetzt, sollte festgelegt werden, wie und in welchen Abständen die Einhaltung der gesetzlichen Vorschriften sowie der vertraglich vereinbarten Bedingungen geprüft werden.	Rechenschaftspflicht
Prüfung auf „gemeinsam Verantwortliche“	Es sollte geprüft werden, ob ggf. eine gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO vorliegt. Ist dies der Fall, muss ein entsprechender Vertrag abgeschlossen werden.	Gemeinsam Verantwortliche, Rechenschaftspflicht
Benennung des Datenschutzbeauftragten	Es sollte geprüft werden, ob ein Datenschutzbeauftragter benannt werden muss oder ob auch ohne Verpflichtung eine Benennung erfolgen sollte, damit eine entsprechende Datenschutzberatung erfolgen kann.	Datenschutzbeauftragter
Festlegung von Verantwortlichkeiten und Aufgaben	Es sollten Beschäftigte oder Dritte mit dem Datenschutz- und IT-Sicherheitsmanagement betraut werden.	Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Sicherheit der Verarbeitung, Rechenschaftspflicht
Erstellung und Pflege eines Verzeichnisses der Verarbeitungstätigkeiten	Es sollte ein Verzeichnis der Verarbeitungstätigkeiten erstellt und aktuell gehalten werden.	Verzeichnis von Verarbeitungstätigkeiten, Rechenschaftspflicht
Durchführung angemessener Schulungen	Es sollten alle mit der Verarbeitung personenbezogener Daten beteiligte Personen bezüglich der Vorgaben von Datenschutz und IT-Sicherheit geschult werden.	Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Sicherheit der Verarbeitung, Rechenschaftspflicht
Aktualisierung des Ausbildungsniveaus beachten	Es sollte festgelegt werden, wann Schulungen zu wiederholen sind.	Rechenschaftspflicht
Berechtigungskonzept erstellen	Es sollte in einem Berechtigungskonzept festgelegt werden, wer wann unter welchen Umständen auf welche Daten zugreifen darf. Hierzu gehört auch die Festlegung, unter welchen Bedingungen ein Entzug von Privilegien wie Zugriffsrechten entzogen werden. Entsprechend dem Berechtigungskonzept sollten die Zugangs- und Zugriffsrechte im System implementiert und durchgesetzt werden. Das Berechtigungskonzept muss in regelmäßigen Abständen überprüft und bei Bedarf (z. B.	Rechenschaftspflicht, Transparenz, Sicherheit der Verarbeitung, insbesondere Gewährleistung der Vertraulichkeit und Integrität

Vorgehen/Maßnahme	(Kurz-) Beschreibung	Adressierte Anforderung
	geänderter gesetzlicher Vorgaben) angepasst werden.	
Protokollierungskonzept erstellen	Es sollte in einem Protokollierungskonzept festgehalten werden, was wann aus welchen Gründen protokolliert wird, wer Protokolldateien ansehen und auswerten darf sowie die Zeitdauer, für die Protokolldaten aufbewahrt werden. Das Protokollierungskonzept muss in regelmäßigen Abständen überprüft und bei Bedarf (z. B. geänderter gesetzlicher Vorgaben) angepasst werden.	Rechenschaftspflicht, Transparenz, Auskunft
Passwortrichtlinie	Es sollte auch eine Richtlinie für Passwörter festgelegt werden, d. h. wie Passwörter gestaltet werden müssen und mit Passwörtern umgegangen wird.	Sicherheit der Verarbeitung, insbesondere Gewährleistung der Vertraulichkeit und Integrität
Datenschutzrichtlinie erstellen	Es sollte eine Datenschutzrichtlinie erstellt werden.	Transparenz
Erstellung einer Richtlinie für die Speicherdauer und Löschung	Es sollte festgelegt werden, aus welchen Gründen und aufgrund welcher Rechtsgrundlage welche Daten wie lange gespeichert werden und wann die Daten gelöscht werden.	Speicherbegrenzung
Erstellung einer Richtlinie für die Ausübung der Rechte der betroffenen Person	Es sollten Verfahren für die Bearbeitung und Umsetzung von Anträgen der betroffenen Personen zur Wahrnehmung ihrer Betroffenenrechte festgelegt und umgesetzt werden.	Rechtmäßigkeit, Rechenschaftspflicht, Betroffenenrechte
Planung und Implementierung mehrerer Module zur Darstellung von Daten in der Schnittstelle	Es sollte auf Schnittstellenebene immer zwischen verschiedenen Arten von Daten unterschieden werden, sodass für Verwaltungsdaten wie bspw. Daten zur Abrechnung einer App andere Vorgaben wie bspw. Zugriffe umgesetzt werden können als für sensible Daten. Auf sensible Daten darf ein Hersteller einer App bspw. keinen Zugriff haben, hingegen muss auf die zur Abrechnung erforderlichen Daten zugegriffen werden können.	Zweckbindung, Datenminimierung, Vertraulichkeit
Pseudonymisierung von Daten	Besonders sensible Daten, insbesondere in Art. 9 Abs. 1 DS-GVO genannte Datenarten, sollten pseudonymisiert werden, um das Risiko einer unbefugten Kenntnisnahme zu minimieren.	Sicherheit der Verarbeitung, insbesondere Gewährleistung der Vertraulichkeit
Planung und Implementierung einen Mechanismus zur Abgabe einer Einwilligung	Es sollte ein Verfahren zur Einholung von Einwilligungen vorhanden sein. Dieses Verfahren muss allen gesetzlichen Anforderungen genügen und die Erfüllung auch nachweisen können.	Rechtmäßigkeit, Einwilligung

Vorgehen/Maßnahme	(Kurz-) Beschreibung	Adressierte Anforderung
Planung und Umsetzung einer Eingabeaufforderung für den Rechtsgrund in Schnittstellen	Bei Nutzung von Schnittstellen, d. h. immer dann, wenn nicht der Patient selbst auf die Daten zugreift, sollte vom System der Rechtsgrund des Zugriffs protokolliert werden. Hierfür muss das zugreifende System bzw. zugreifende andere Nutzer außer dem Patienten nach der rechtlichen Grundlage des Zugriffs gefragt werden.	Rechtmäßigkeit
Planung und Umsetzung einer Funktion zur Beauskunftung berechtigter Personen	Es sollte ein sicherer Mechanismus vorhanden sein, um betroffenen Personen Zugang zu den Daten und eine Kopie dieser Daten davon zu gewähren.	Rechenschaftspflicht, Recht auf Auskunft
Planung und Umsetzung einer Funktion zur Sperrung von Daten	Es sollte eine sichere Funktion zur Sperrung von Daten vorhanden sein, d. h. gesperrte Daten dürfen nicht verarbeitet werden. Eine Sperrung darf nur nach Information der betroffenen Person aufgehoben werden.	Rechenschaftspflicht, Recht auf Sperrung
Erstellung einer Richtlinie für den Umgang mit Datenpannen	Es sollten Verfahren und Strategien für den Umgang mit Datenpannen festgelegt und umgesetzt werden. Dies muss die ggf. erforderliche Benachrichtigung von Datenschutz-Aufsichtsbehörden sowie betroffener Personen über eine Datenschutzverletzung umfassen.	Rechenschaftspflicht, Transparenz, Verletzungen des Schutzes personenbezogener Daten
Planung und Umsetzung einer Funktion zur Datenübertragbarkeit	Es sollte eine Möglichkeit existieren, Daten auf Veranlassung betroffener Personen in elektronischer Form an andere in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln.	Rechenschaftspflicht, Recht auf Datenübertragbarkeit
Festlegung der Umsetzung Korrektur und Ergänzung vorhandener Daten	Es sollten Verfahren und Strategien zur Gewährleistung der Richtigkeit der personenbezogenen Daten festlegt und umgesetzt werden.	Richtigkeit
Erstellung eines IT-Sicherheitskonzeptes	Es sollten Verfahren und Strategien für die Sicherheit festgelegt und in einem IT-Sicherheitskonzept dokumentiert werden. Das IT-Sicherheitskonzept muss in regelmäßigen Abständen überprüft und bei Bedarf (z. B. geänderter gesetzlicher Vorgaben) angepasst werden.	Sicherheit der Verarbeitung, Rechenschaftspflicht
Erstellung von Richtlinien für die Beantwortung von behördlichen Anfragen, insbesondere von Datenschutzbehörden	Es sollten Verfahren festgelegt und umgesetzt werden, wie und von wem Anfragen von Datenschutzbehörde oder anderer Behörden bearbeitet werden.	Rechenschaftspflicht, Berücksichtigung der Befugnisse

Vorgehen/Maßnahme	(Kurz-) Beschreibung	Adressierte Anforderung
Dokumentation der gesetzlichen Offenlegungspflichten	Es sollten die gesetzlich vorgeschriebene Offenlegungspflichten analysiert und dokumentiert werden, sodass einerseits betroffene Personen in den Datenschutzhinweisen informiert werden, andererseits Beschäftigte bei Nachfragen von Behörden eine Möglichkeit zum Nachschlagen haben.	Rechenschaftspflicht, Rechtmäßigkeit

Anlage 4.2. Hinweise zur Planung von fortlaufend erforderlichen Maßnahmen

Vorgehen/Maßnahme	(Kurz-) Beschreibung	Adressierte Anforderung
Überprüfung der gewählten Lösungen	Die geplanten bzw. implementierten Lösungen sollten regelmäßig auf ihre Wirksamkeit überprüft werden, insbesondere ob die Lösungen noch technisch angemessen sind sowie ob sie dem Stand der Technik entsprechen.	Rechenschaftspflicht, Verarbeitung nach Treu und Glauben, Sicherheit der Verarbeitung, insbesondere Integrität und Vertraulichkeit
Aktualisierung aller Richtlinie, Konzepte sowie aller anderen Datenschutz- und IT-Sicherheitsdokumente	Alle Dokumente sollten in regelmäßigen Abständen überarbeitet werden.	Transparenz
Implementierung von Sicherungs- und Wiederherstellungsmechanismen	Es sollten Sicherungs- und Wiederherstellungsmechanismen eingeplant und umgesetzt werden, sodass bei einem Vorfall Daten angemessen schnell wieder hergestellt werden.	Sicherheit der Verarbeitung, insbesondere Gewährleistung der Verfügbarkeit und Belastbarkeit
Regelmäßige Durchführung von Penetrationstests	Es sollten regelmäßig Penetrationstests durchführt werden.	Sicherheit der Verarbeitung, insbesondere Gewährleistung der Vertraulichkeit und Integrität

Anlage 4.3. Hinweise zum Vorgehen bei der Erhebung von Daten

Vorgehen/Maßnahme	(Kurz-) Beschreibung	Adressierte Anforderung
Darstellung der Rechtsgrundlage für die Erhebung	Es sollte für jede Verarbeitungstätigkeit bzw. für den damit verbundenen Zweck die Rechtsgrundlage festlegt werden.	Rechtmäßigkeit, Rechenschaftspflicht
Information der betroffenen	Es sollten betroffenen Personen alle Informationen und insbesondere auch die	Transparenz, Informationspflicht

Vorgehen/Maßnahme	(Kurz-) Beschreibung	Adressierte Anforderung
Person	Datenschutzrichtlinien zur Verfügung gestellt werden. Personen sind insbesondere auch über die Rechtsgrundlage der Verarbeitung zu informieren.	
Ggf. ausdrückliche Einwilligung einholen	Ist die Rechtsgrundlage eine Einwilligung der betroffenen Person, so sind die Vorgaben der DS-GVO einzuhalten und die Einhaltung nachgewiesen werden. Bei den in Art. 9 Abs, 1 genannten Datenarten ist insbesondere die Ausdrücklichkeit der Einwilligung zu beachten und nachzuweisen.	Einwilligung, Rechtmäßigkeit, Rechenschaftspflicht
Grenzen für die Datenerhebung festlegen und beachten	Es sollten nur die Daten erhoben werden, die für die Erreichung der festgelegten Zwecke erforderlich sind.	Zweckbindung, Datenminimierung

Anlage 4.4. Hinweise zum Schutz von ruhenden Daten („Data at Rest“)

Vorgehen/Maßnahme	(Kurz-) Beschreibung	Adressierte Anforderung
Darstellung der Datenflüsse für die geplante Verarbeitung	Die Verantwortlichen müssen die Datenflüsse kennen, um zu wissen, welche Daten von wem/welcher Anwendung wann wie genutzt wird, damit hierbei angemessene Schutzmaßnahmen geplant und umgesetzt werden können. Dies muss vorab geplant und dokumentiert werden.	Rechenschaftspflicht und Sicherheit der Verarbeitung
Trennung von personenbezogenen Verwaltungsdaten und sensiblen Daten auf Datenbankebene	Durch Trennung der Daten können gezielt Maßnahmen zum umfangreicheren Schutz besonders sensibler Daten, insbesondere der in Art. 9 Abs. 1 DS-GVO genannten Daten, ergriffen werden. Zugleich erhält ein Angreifer, der Zugriff auf Verwaltungsdaten (wie bspw. Abrechnungsdaten der App) erhält, keinen Zugriff auf die sensiblen Daten.	Sicherheit der Verarbeitung, insbesondere Gewährleistung der Vertraulichkeit
Verschlüsselung der Datenbank	Zum Schutz der Daten sollten Daten nur verschlüsselt im Dateisystem abgelegt werden sowie die Datenbank(en) verschlüsselt werden. Beides muss dem Stand der Technik entsprechen.	Sicherheit der Verarbeitung, insbesondere Gewährleistung der Vertraulichkeit
Implementierung eines Intrusion-Detection-Systems	Es sollte ein effizientes System zur Kontrolle der Datenflüsse vorhanden sein, welches insbesondere erlaubt, auch nicht geplante und nicht gewünschte Abflüsse von Daten (z. B. Zugriffe durch Hersteller der Betriebssysteme) zu erkennen.	Sicherheit der Verarbeitung, insbesondere Gewährleistung der Vertraulichkeit und Integrität
Implementierung einer angemessenen Protokollierung	Es sollte ein effizientes Protokollierungssystem geplant und umgesetzt werden, welches zumindest Auskunft gibt über: - ID-Nummer zur eindeutigen Identifizierung des Ereignisses, - ID-Nummer zur Identifizierung des Zugreifenden, sei es eine Person oder auch ein	Rechenschaftspflicht, Transparenz der Verarbeitung, Ermöglichung einer Auskunft, Sicherheit der Verarbeitung, insbesondere Gewährleistung der

Vorgehen/Maßnahme	(Kurz-) Beschreibung	Adressierte Anforderung
	System, - ID-Nummer zur Identifizierung des Patienten - Datum und Uhrzeit des Zugriffs, - Auf welche Datenkategorien zugegriffen wurde, - Den Grund für den Zugriff.	Vertraulichkeit und Integrität

Anlage 4.5. Hinweise zum Schutz von Daten während der Verarbeitung („Data in Use“)

Vorgehen/Maßnahme	(Kurz-) Beschreibung	Adressierte Anforderung
Nur bekannte Nutzer können System nutzen	Es sollten angemessene und effiziente Mechanismus zur eindeutigen Identifizierung der Nutzer vorhanden sein, die gewährleisten, dass nur sicher identifizierte und dem System bekannte Nutzer eine Anmeldung am System durchführen können.	Sicherheit der Verarbeitung, insbesondere Integrität und Vertraulichkeit
Nur berechtigte Zugriffe	Es sollten angemessene und effiziente Zugangskontrollmechanismus existieren, die sicherstellen, dass ausschließlich dem Berechtigungskonzept entsprechend autorisierte Zugriffe möglich sind.	Sicherheit der Verarbeitung, insbesondere Integrität und Vertraulichkeit
Implementierung eines Mechanismus zur Anomalie-Erkennung	Die Protokolldaten sollten regelmäßig auf Anomalien kontrolliert werden, um unberechtigte Zugriffe zu erkennen.	Sicherheit der Verarbeitung, insbesondere Integrität und Vertraulichkeit
Hinweis, wenn Rechtsgrund abgelaufen ist	Wenn die Rechtsgrundlage nicht mehr gilt (z. B. weil die Einwilligung zurückgezogen wurde), sollte das Ereignis im System gekennzeichnet werden. Zugriffe aufgrund dieses Rechtsgrunds dürfen nicht mehr erfolgen. Zugreifende sollten einen Hinweis über den Ablauf des Rechtsgrunds erhalten.	Rechtmäßigkeit

Entschlüsselung nur auf dem Endgerät	Werden Daten auf einem Server gespeichert, auf dem ein Zugriff nicht berechtigter Personen auf den Arbeitsspeicher nicht sicher ausgeschlossen werden kann, sollten verschlüsselte Daten nur auf dem Smartphone/Tablet entschlüsselt werden, um so das Risiko von unberechtigten Zugriffen zu minimieren,	Rechtmäßigkeit, Sicherheit der Verarbeitung, insbesondere Vertraulichkeit

Anlage 4.6. Hinweise zum Schutz von Daten während eines Transfers („Data at Transit“)

Vorgehen/Maßnahme	(Kurz-) Beschreibung	Adressierte Anforderung
Datenübertragungen ausschließlich verschlüsselt	Es sollte nur nach dem Stand der Technik Ende-zu-Ende verschlüsselte Übertragungen erfolgen.	Sicherheit der Verarbeitung, insbesondere Integrität und Vertraulichkeit
Überwachung der Sicherheit einer Übertragung	Es sollten Mechanismen zur Überwachung der sicheren Übertragung wie bspw. Zertifikatsprüfungen eingesetzt werden.	Sicherheit der Verarbeitung, insbesondere Integrität und Vertraulichkeit

Anhang 5: Beispiel für Maßnahmen hinsichtlich IT-Sicherheit

Nachfolgend finden sich einige Anforderungen ohne Anspruch auf Vollzähligkeit, welche einige wichtige Elemente zur Gewährleistung der IT-Sicherheit darstellen.

Weiterhin sind unbedingt die Empfehlungen der Betriebssystemhersteller hinsichtlich der IT-Sicherheit bei der Entwicklung von mobilen Apps zu beachten, insbesondere die Guides unter

- Google: Android and Security (Stand 2012-02-02): https://googlemobile.blogspot.com/2012/02/android-and-security.html
- Android Develobers → Guides → Security (Stand: 2022-02-23): https://developer.android.com/topic/security/best-practices
- Apple: Documentation Security: https://developer.apple.com/documentation/security?language=de

Anlage 5.1. Allgemeines

- Datenschutzhinweise/-richtlinien berücksichtigen, die für den Benutzer leicht zu lesen und zu verstehen sind, insbesondere enthaltend
  - Eindeutige Regelung zur Datenspeicherung sowie Datenlöschung
  - Falls zutreffend: Einfügen eines Abschnitts für Minderjährige mit der Verpflichtung zur Genehmigung durch einen gesetzlichen Vertreter
- Regelmäßige Sicherheitsaktualisierungen durch Patches gewährleisten
- Kontaktmöglichkeiten anbieten, um Probleme mit der App zu melden
- Ermöglichung der Fernlöschung oder Deaktivierung der Anwendung und ihrer Inhalte
- Statische Code-Analysatoren und Fuzzer bei der Entwicklung der App verwenden
- Daten nicht an Dritte weitergeben oder andernfalls den Benutzer informieren

Anlage 5.2. Anwendung/Frontend

- Möglichst keine Bibliotheken von Drittanbietern nutzen; falls unumgänglich nur von vertrauenswürdigen Drittanbietern
  - Kriterien der Beurteilung der Vertrauenswürdigkeit vorab festlegen
  - Beurteilung der Vertrauenswürdigkeit transparent auch für Nutzer einsehbar dokumentieren
  - Alle Drittanwender-Bibliotheken klar und übersichtlich aufführen
  - Ein effektives Monitoring bzw. ggf. auftretender Sicherheitslücken bei den Drittanbieterbibliotheken durchführen.
- Kontrolle des Zugriffs auf Daten/Informationen durch restriktive Vergabe von Berechtigungen
  - Anwendungen testen, indem diese mit der niedrigsten Berechtigungsstufe ausgeführt werden
- Überprüfung der Identität des Nutzers über ein Authentifizierungssystem oder biometrische Parameter
- Speichern Sie Passwörter nicht in Dateien und überprüfen Sie deren Entropie
- Insbesondere keine hart kodierten Passwörter im Code speichern
- Erstellung, Pflege und Löschung von Sitzungs-Tokens (lang, komplex und quasi-zufällig) durch OAuth
- Vermeidung, dass Anmeldeinformationen oder andere persönliche Daten im Cache oder im Code sichtbar sind
- Verwenden Sie AES mit mindestens 256 Bit zur Verschlüsselung der personenbezogenen Daten
- Deaktivierung der Anwendung im Hintergrund zulassen

- Auf Mobilgeräten mit SD-Karte: Auf der SD-Karte personenbezogene oder personenbeziehbare Daten nur verschlüsselt speichern
- Die App sollte keine Cookies speichern, damit Dritte die darin gespeicherten Informationen nicht abgreifen können
- Icon in der App, welches bei einer Übertragung von Daten den Benutzer über die Übertragung informiert
- Absicherung der Code-Integrität durch kryptographische Maßnahmen wie beispielsweise Nutzung von Hash-Codes und elektronischer Signatur, insbesondere auch zur Prüfung bei Einspielung eines Updates/Patches
- Verwendung abgesicherter Funktionen zur Vermeidung von Buffer Overflow
- Vermeidung von einfachen Angriffen wie SQL-Injection
- Vermeidung von Cross-Site-Scripting-Angriffen
- Vermeidung von Cross-Application-Scripting-Angriffen
- Beendung der Ausführung der Anwendung im Falle einer Verletzung der Code-Integrität
- Reverse Engineering der App vermeiden, Anti-Debugging-Techniken anwenden
- Verschleierung/Verschlüsselung des App-Codes
- Validierung aller Informationen, die in die App ein- und ausgegeben werden, um Fälle wie beispielsweise QR-Code-Leaks zu vermeiden

Anlage 5.3. Server/Backend

- Analysieren Sie den Server in regelmäßigen Abständen und halten Sie ihn auf dem neuesten Stand
- Abhärtung des Servers, insbesondere Vermeidung von Injections auf dem Server
- Ergreifung von Maßnahmen zur Vermeidung von Denial-of-Service-Angriffen
- Sicherstellen, dass der Server alle unverschlüsselten Anfragen zurückweist
- Die Validierung der Sitzung muss vom Server durchgeführt werden
- Überprüfung der Identität des Benutzers vor der Ausführung des von der Anwendung angebotenen Dienstes
- Cookies von früheren Sitzungen dürfen nicht akzeptiert werden
- Löschen von personenbezogenen Daten auf dem Server, sobald die Daten auf dem Server nicht mehr benötigt werden (beispielsweise nach Abschluss rechenintensiver Auswertungen, die nur serverseitig ausgeführt werden können)

Anlage 5.4. Kommunikation

- Einrichten eines sicheren Datenübertragungskanals wie z. B. Nutzung von TLS
- Verwendung von Virtual Private Networks und/oder HTTPS-Logins
- Verwendung kryptographischer Methoden zur Erlangung von Informationen eines Body Sensor Network (BSN) im Falle von Wearables

Anhang 6: Checkliste Einwilligung

Zu prüfen…	Ja	Nein
Allgemein		
Ist eine Einwilligung erforderlich? (D. h. es gibt keine andere Rechtsgrundlage für die Verarbeitung?)		
Existiert eine andere Rechtsgrundlage, aber die Einwilligung wird in Kenntnis der Anforderungen und Folgen dennoch gewählt?		
Ist die Einsichtsfähigkeit der betroffenen Personen gegeben? Wenn nicht: Wird vom gesetzlichen Vertreter die Einwilligung eingeholt?		
Wird die Einwilligung zeitlich vor der Erhebung und Verwendung von personenbezogenen Daten eingeholt?		
Ist die Identität der einwilligenden Person eindeutig festgestellt?		
Form		
Wurden nationale Form-Vorgaben für die Einwilligung wie bspw. „Schriftform“ beachtet?		
Ist die Einwilligung „Teil eines größeren Dokuments“? Wenn ja, dann muss sie von den anderen Sachverhalten des Dokuments klar zu unterscheiden sein: Werden Anforderungen an die „optische“ Hervorhebung der datenschutzrechtlichen Einwilligung eingehalten?		
Ist an eine zweifache Ausfertigung des Dokumentes gedacht? (Verbleib des Originals beim Verantwortlichen, Kopie beim/bei der betroffenen Person)		
Wurde eine Gelegenheit für Rückfragen vor Abgabe der Einwilligung gegeben?		
Wird dokumentiert, ob Rückfragen vorhanden waren oder nicht sowie der Umgang mit Rückfragen?		
Wurde darauf geachtet, dass die Informationen keine Unterschrift zur Bestätigung der Kenntnisnahme enthalten?		
Willensbekundung		
Ist für die Abgabe der Einwilligung ein aktiver Prozess (z. B. Häkchen setzen oder unterschreiben) erforderlich?		
Wurden vorangekreuzte Kästchen oder andere Arten von Vorauswahl hinsichtlich Einwilligung vermieden?		
Transparenz		
Werden Informationen in einer einfachen und klaren Sprache, die für jedermann verständlich ist, gegeben?		
Werden Daten zu unterschiedlichen Zwecken und auf unterschiedliche Weise verarbeitet: Werden separate Einwilligungen eingeholt?		
Ist für die betroffene Person eindeutig ersichtlich, welche Texte informativ und welche Bestandteile der Einwilligung sind?		
Wurde bei Einholung zusammen mit anderen Erklärungen auf eine Hervorhebung geachtet?		
Freiwilligkeit		
Hatte die betroffene Person eine echte Wahl zwischen Zustimmung und Ablehnung?		
Wurde darüber aufgeklärt, dass die betroffene Person die Einwilligung ohne Nachteil für sie verweigern kann? Wenn ein Nachteil besteht: Gibt es einen (verständlichen) Hinweis auf die Folgen, die die Verweigerung der Einwilligung für den Betroffenen haben kann?		
Ist gewährleistet, dass die Erfüllung eines Vertrages oder die Erbringung einer Dienstleistung nicht von der Einwilligung abhängig gemacht wurde, wenn die Einwilligung nicht zwingend zur Erfüllung benötigt wird (Kopplungsverbot)?		

Zu prüfen…	Ja	Nein
Wie wurde – wenn zutreffend - ein Ungleichgewicht zwischen Verantwortlichem und betroffenen Personen berücksichtigt?		
Informiertheit		
Hat der Betroffene alle erforderlichen Informationen (inkl. Vor- und Nachteile) erhalten? Insbesondere: – Personenkreis, der auf Daten Zugriff erlangen darf, – Datenverwendung (Zweck, Ziel, Nutzen, Chancen und Risiken), – die (Art der) Daten, die erhoben und verwendet werden, – das Bestehen eines Rechts, die Einwilligung zu widerrufen, – gegebenenfalls Informationen über die Verwendung der Daten für eine automatisierte Entscheidungsfindung gemäß Art. 22 Abs. 2 lit. c, – Datenweitergabe (an wen, ggfs. Speicherung an welchem Ort, Land), – Angaben zu möglichen Risiken von Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien		
Werden alle in Art. 13 DS-GVO bzw. Art 14 DS-GVO genannten Informationen bereitgestellt? Insbesondere: – Ansprechpartner sowie Kontaktdaten (Verantwortlicher, Datenschutzbeauftragter, …) – Rechtsgrundlage der Vereinbarung – Empfänger – Speicherdauer – Rechte des Betroffenen (Einsichtnahme, Korrektur, Löschen, Widerruf Einwilligung)		
Werden die Informationen so klar und eindeutig bereitgestellt, dass kein Zwang oder Täuschung z. B. durch Fehlinterpretation seitens der betroffenen Person entstehen kann?		
Sind der Verantwortliche sowie seine Vertreter eindeutig benannt? Stehen alle benötigten Kontaktdaten dem Betroffenen zur Verfügung?		
Bezieht sich bei der Verarbeitung besonderen Kategorien von Daten (Art. 9 DS-GVO) die Einwilligungserklärung ausdrücklich auch auf diese Daten?		
Bestimmtheit		
Bezieht sich die Einwilligung auf einen konkret benannten Zweck? (Bzw. auf mehrere konkret benannte Zwecke „für den bestimmten Fall“?) Hinweis: Generaleinwilligungen sind unwirksam; für verschiedene Zwecke müssen separate Einwilligungen eingeholt / abgegeben werden		
Ist die Einwilligungserklärung von etwaigen sonstigen (datenschutzrelevanten) Hinweisen deutlich getrennt? Es ist zu vermeiden, dass der Betroffene auf Grund Unübersichtlichkeit des Dokumentes nicht erkennt, ob und gegebenenfalls in was er eigentlich einwilligt bzw. einwilligen soll.		
Ausdrücklichkeit		
Beinhaltet die Verarbeitung genetische oder Gesundheitsdaten (bzw. andere in Art. 9 Abs. 1 DS-GVO genannten Kategorien) und wurden dies ausdrücklich angegeben?		
Wurde die Einwilligung ausdrücklich auch auf diese Daten erteilt? (Hinweis: Keine Einwilligung nur durch schlüssiges Verhalten)		
Einwilligung Minderjähriger		
Bei Verarbeitungen, die Art. 8 DS-GVO berühren: Alter jünger als 16?		
Bei der Verarbeitung mittels „Dienste der Informationsgesellschaft“ - Art. 8 beachtet?		
Wenn Einwilligung der Eltern vorliegt: Spätestens bei Volljährigkeit des Betroffenen ist weitere Verarbeitung nur mit Einwilligung des Betroffenen selbst möglich. Gibt es Mechanismus, um die Verarbeitung der Daten zum Zeitpunkt „x“ zu stoppen?		

Zu prüfen…	Ja	Nein
Widerrufbarkeit		
Ist auf den jederzeit möglichen Widerruf der Einwilligung im Einwilligungsformular hingewiesen?		
Ist im Einwilligungsformular Kontaktdaten für einen Widerruf angegeben?		
Ist im Einwilligungsformular darauf hingewiesen, dass ein Widerruf immer nur für die nach dem Widerruf erfolgende geplante Verarbeitung gilt?		
Ist der Widerruf der Einwilligung (mindestens) so einfach möglich wie das Erteilen der Einwilligung selbst?		
Gibt es einen (verständlichen) Hinweis auf die Folgen des Widerrufs?		
Nachweisbarkeit		
Werden Einwilligungen für die Zeitdauer der jeweiligen Verarbeitung archiviert, sodass ein Nachweis jederzeit möglich ist?		
Ist der Nachweis gegeben, dass die Einwilligung von der betroffenen Person abgegeben wurde?		
Ist der Nachweis gegeben, dass die Einwilligung den Anforderungen der DS-GVO genügend abgegeben wurde? Dies beinhaltet insbesondere den Nachweis von: – Einsichtsfähigkeit – Bestimmtheit – Zweckbindung – Freiwilligkeit – Informiertheit – (Ausdrückliche) Willensbekundung – Hinweis auf Widerrufbarkeit		
Werden erteilte Einwilligungen protokolliert? Wenn ja: Sind ausreichende technische und organisatorische Maßnahmen zum Schutz der Protokolle getroffen? (Beweisfestigkeit)		
Sind erteilte Einwilligungen jederzeit abrufbar?		
Drittlandtransfer		
Wurde geprüft, ob das Recht des Bestimmungsdrittlands den übermittelten personenbezogenen Daten nach Maßgabe des Unionsrechts einen angemessenen Schutz gewährleistet?		
Wurden geeignete Maßnahmen vorgesehen, mit denen ein der DS-GVO gleichwertiges Schutzniveau erreicht wird?		
Wurde geprüft, ob die Maßnahmen ein der DS-GVO gleichwertiges Schutzniveau gewährleisten?		
Kopplungsverbot		
Wurde die Behandlung bzw. eine andere Leistung nicht davon abhängig gemacht, dass der Patient in eine Datenverarbeitung einwilligt, welche mit der Behandlung bzw. der Leistung nicht im Zusammenhang steht?		
Broad Consent		
Nachweis wissenschaftliche Forschung		
Angabe des Forschungszweckes (Cave: keine „General“-Erlaubnis statthaft)		
Überprüfbare und nachvollziehbare Darstellung, warum der Forschungszweck zum Zeitpunkt der Erhebung der Daten nicht <u>vollständig</u> angegeben werden kann		
Nachweis der Einhaltung der anerkannten ethischen Standards (i. d. R. durch vorliegendes Ethik-Votum)		
Betroffenen Personen ist es möglich sein, ihre Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten zu erteilen		

Anhang 7: Checkliste „Erfüllung der Anforderungen“

Um Entwicklern und DSB eine Prüfliste zu bieten, wurden alle Anforderungen dieser Praxishilfe in einer Excel-Tabelle abgebildet. Dadurch können die Anforderungen thematisch sortiert oder gefiltert und insbesondere auch in Form einer Checkliste abgearbeitet werden. Dabei ist zu beachten, dass Anforderungen natürlich immer auch mehrere Stellen innerhalb der DS-GVO betreffen können. So werden beispielsweise Anforderungen zur Einwilligung nicht nur Art. 7 DS-GVO betreffen, sondern auch die in Art. 5 Abs. 1 lit. a DS-GVO enthaltene Rechtmäßigkeit adressieren.

Checkliste_Apps_Anforderungen.xlsx

Anlage 7.1. Aufbau der Excel-Tabelle

- Aufbau des Tabellenblatts „Anforderungsliste“
  - Spalte 1: Hier wird die Seitenzahl angegeben, auf welcher die entsprechende Anforderung in der Praxishilfe zu finden ist. Dies kann hilfreich sein, wenn man die Anforderung im Kontext nachlesen möchte.
  - Spalte 2: Hier wird die Nummer der Anforderung aus der Praxishilfe angegeben. Dadurch kann z. B. eine Sortierung innerhalb der Tabelle durchgeführt werden.
  - Spalte 3: Hier wird angegeben, welchen Erfüllungsgrad die Anforderung aufweist.
  - Spalte 4: Der Text der Anforderung ist in dieser Spalte zu finden.
  - Spalte 5: Hier wird eine Zuordnung der Anforderung zu einer relevanten Stelle der DS-GVO angegeben. Häufig gibt es noch weitere Stellen in der DS-GVO, die mit der Anforderung in Zusammenhang stehen. Aus Gründen der Übersicht wurde jedoch eine aus Sicht der Autoren relevante Regelung ausgewählt.
  - Spalte 6: Die Spalte ist eine thematische Zuordnung der Anforderung, um eine Sortierung oder Filterung (beispielsweise nach Text „Einwilligung“) in der Tabelle zu ermöglichen.
  - Spalte 7: Hier wird angegeben, ob die Anforderung erfüllt ist oder nicht. Antwortmöglichkeiten sind „ja“ und „nein“, denn letztlich wird auch eine nicht zutreffende Anforderung nicht erfüllt, sodass diese beiden Antwortmöglichkeiten ausreichen.
  - Spalte 8: In dieser Spalte wird in aller Kürze dargestellt, wodurch diese Anforderung erfüllt wird. Hier kann auch ein Verweis auf begleitende Dokumente wie z. B. ein IT-Sicherheitskonzept oder ein Protokollierungskonzept erfolgen.
  - Spalte 9: In dieser Spalte wird in aller Kürze dargestellt, wodurch diese Anforderung nicht erfüllt wird. Dies kann beispielsweise auch der Fall sein, weil eine Anforderung auf den konkreten Fall nicht zutrifft.
  - Spalte 10: In dieser Spalte kann ein Prüfer (z. B. ein Auditor) eintragen, ob die Anforderung aus seiner Sicht erfüllt wurde oder nicht, idealerweise mit Begründung.
- Tabellenblatt „Auffälligkeiten“
  - Im Tabellenblatt „Auffälligkeiten“ findet sich eine Übersicht, welche Anforderungen bzgl. des Kriteriums „erfüllt“ bzw. „nicht erfüllt“ bearbeitet wurden, bzw. welche Antworten noch offen sind. Gleichermaßen wird geprüft, ob vorhandener Text zur Darstellung, wie das Kriterium behandelt wurde, vorhanden ist.
- Tabellenblatt „Prüfkriterien“
  - Einige Anforderungen stehen in Beziehung zueinander (siehe Anlage 7.2). Ist eine Anforderung erfüllt, eine andere aber nicht, so bietet sich in diesen Fällen eine Überprüfung an, ob die Angaben zum Erfüllungsgrad der jeweiligen Anforderungen richtig dokumentiert wurden. Das Tabellenblatt „Prüfkriterien“ bietet hier Hinweise, wenn Auffälligkeiten entsprechend den vorgegebenen Kriterien gefunden wurden.

- In den Spalten A und B des Tabellenblattes „Prüfkriterien“ stehen die zueinander in Beziehung stehenden Anforderungen, in den Spalten H bis K des Tabellenblatts „Hilfstabelle“ wird überprüft, ob die Kriterien zutreffen und welcher Text ggf. angezeigt werden soll.

– Tabellenblatt „Hilfstabelle“
  - Das Tabellenblatt "Hilfstabelle" enthält Parameter für Auswahlzellen und stellt Auswertungen für andere Tabellenblätter zur Verfügung. Damit nicht aus Versehen unbeabsichtigte Änderungen durchgeführt werden, ist das Tabellenblatt ausgeblendet. Es existiert jedoch kein Passwortschutz, sodass nach einem Einblenden des Tabellenblattes Änderungen und Anpassungen für die eigenen Bedürfnisse vorgenommen werden können.

Anlage 7.2. Anforderungen, die in Beziehung zueinanderstehen

Anforderung		**Prüfhinweise**
Erfüllt	**Nicht erfüllt**	
10	32	Passwörter als Hash gespeichert (Anf. 10), aber nicht verschlüsselt?
14	10	Eingabe Passwort wird verschleiert (Anf. 14), aber Darstellung erfolgt im Klartext?
12	13	Schutz vor Brute-Force-Attacken ist vorhanden (Anf. 12), aber Maßnahmen gegen Ausprobieren von Passwörtern sind nicht vorhanden?
13	12	Maßnahmen gegen Ausprobieren von Passwörtern integriert (Anf. 13), aber kein Schutz vor Brute-Force-Attacken vorhanden?
16	15	Biometrie ist nicht alleiniger Authentifizierungsmechanismus (Anf. 16), aber es wird keine eigene Authentifizierung in der App angeboten?
15	16	Es wird eine eigene Authentifizierungsmethode angeboten (Anf. 15), aber Biometrie ist alleiniger Authentifizierungsmechanismus?
17	15	Eine Einwilligung in die Nutzung von biometrischen Authentifizierungsmethoden wurde eingeholt (Anf. 14), aber eine Zustimmung liegt nicht vor?
15	17	Eine Zustimmung des Nutzers zur Nutzung von biometrischen Authentifizierungsmöglichkeiten liegt vor (Anf. 15), aber eine Einwilligung ist nicht vorhanden?
92	89	Datenschutzhinweise sind mit maximal zwei Klicks von der Startseite aus erreichbar (Anf. 92), aber sind von der Startseite der App aus nicht aufrufbar bzw. nicht erreichbar?
89	92	Datenschutzhinweise sind unmittelbar von der Startseite der App aus aufrufbar bzw. erreichbar (Anf. 89), aber nicht mit maximal zwei Klicks von der Startseite aus erreichbar?
85	41	Datenschutzhinweise enthalten alle in Artikel 13, 14 der Datenschutz-Grundverordnung genannten Informationen (Anf. 85), aber betroffene Personen erhalten nicht alle Informationen, die für die Gewährleistung einer transparenten Verarbeitung erforderlich sind?
41	85	Betroffene Personen erhalten alle Informationen, die für die Gewährleistung einer transparenten Verarbeitung erforderlich sind (Anf. 41), aber die Datenschutzhinweise enthalten nicht alle in Artikel 13, 14 der Datenschutz-Grundverordnung genannten Informationen?
85	79	Datenschutzhinweise enthalten alle in Artikel 13, 14 der Datenschutz-Grundverordnung genannten Informationen (Anf. 85), aber betroffenen Personen werden vor der Erteilung einer Einwilligung nicht alle erforderlichen Informationen bereitgestellt?
41	79	Betroffene Personen erhalten alle Informationen, die für die Gewährleistung einer transparenten Verarbeitung erforderlich sind (Anf. 41), aber

Anforderung		Prüfhinweise
Erfüllt	Nicht erfüllt	
		betroffenen Personen werden vor der Erteilung einer Einwilligung nicht alle erforderlichen Informationen bereitgestellt?
36	37	In die Verarbeitung von Unique Identifier des Endgerätes bzw. des Betriebssystems wurde eingewilligt (Anf. 36), aber es liegt keine ausdrückliche Einwilligung vor?
37	36	Für die Verarbeitung von Unique Identifier des Endgerätes bzw. des Betriebssystems liegt eine ausdrückliche Einwilligung vor (Anf. 37), aber es wurde keine Einwilligung eingeholt?
54	99	Gespeicherte Daten können korrigiert sowie aktualisiert werden (Anf. 54), aber es existiert keine Möglichkeit, auf Aufforderung des Betroffenen Daten zu seiner Person zu korrigieren?
54	100	Gespeicherte Daten können korrigiert sowie aktualisiert werden (Anf. 54), aber es existiert keine geeignete Funktion, um erhobene und/oder verarbeitete Daten zu aktualisieren oder zu ergänzen?
100	54	Es existiert eine geeignete Funktion, um erhobene und/oder verarbeitete Daten zu aktualisieren oder zu ergänzen (Anf. 100), aber gespeicherte Daten können nicht korrigiert bzw. nicht aktualisiert werden?
100	99	Es existiert eine geeignete Funktion, um erhobene und/oder verarbeitete Daten zu aktualisieren oder zu ergänzen (Anf. 100), aber es existiert keine Möglichkeit, auf Aufforderung des Betroffenen Daten zu seiner Person zu korrigieren?
99	100	Es existiert eine Möglichkeit, auf Aufforderung des Betroffenen Daten zu seiner Person zu korrigieren (Anf. 99), aber es existiert keine geeignete Funktion, um erhobene und/oder verarbeitete Daten zu aktualisieren oder zu ergänzen?
99	54	Es existiert eine Möglichkeit, auf Aufforderung des Betroffenen Daten zu seiner Person zu korrigieren (Anf. 99), aber gespeicherte Daten können nicht korrigiert bzw. nicht aktualisiert werden?
58	110	Daten, deren Speicherfrist abgelaufen ist, werden schnellstmöglich gelöscht (Anf. 58), aber Daten werden nicht unverzüglich gelöscht, wenn der Verwendungszweck entfällt und keine gesetzliche Grundlage zur Speicherung der Daten vorliegt?
110	58	Daten werden unverzüglich gelöscht, wenn der Verwendungszweck entfällt und keine gesetzliche Grundlage zur Speicherung der Daten vorliegt (Anf. 110), aber Daten, deren Speicherfrist abgelaufen ist, werden nicht schnellstmöglich gelöscht?
205	206	Für jedes Drittland wird ein eigenes Transfer-Impact-Assessment erstellt (Anf. 205), aber es wird kein Transfer-Impact-Assessment durchgeführt, wenn die Datenverarbeitung in einem Drittland durchgeführt wird oder ein Zugriff auf die Daten aus einem Drittland nicht ausgeschlossen werden kann?
206	205	Es wird immer ein Transfer-Impact-Assessment durchgeführt, wenn die Datenverarbeitung in einem Drittland durchgeführt wird oder ein Zugriff auf die Daten aus einem Drittland nicht ausgeschlossen werden kann (Anf. 206), aber es wird nicht für jedes Drittland ein eigenes Transfer-Impact-Assessment erstellt?
135	158	Bei der Rollen- und Rechtevergabe im Berechtigungs- und Rollenkonzept wird das Need-to-know-Prinzip angewendet (Anf. 135), aber die Berechtigungen von Benutzern und Anwendungen werden nicht auf ein für deren Aufgaben notwendiges Minimum reduziert?

Anforderung		Prüfhinweise
Erfüllt	**Nicht erfüllt**	
158	1385	Die Berechtigungen von Benutzern und Anwendungen werden auf ein für deren Aufgaben notwendiges Minimum reduziert (Anf. 158), aber bei der Rollen- und Rechtevergabe im Berechtigungs- und Rollenkonzept wird das Need-to-know-Prinzip nicht angewendet?
137	136	Eine Kombination von Rollen bzw. Zugriffsrechten für eine Person, welche der Person mehr Rechte auf Datenzugriffe erteilt, als für ihre Aufgabe nötig ist, wird verhindert (Anf. 137), aber es werden keine Maßnahmen getroffen, um die Kombination von nicht miteinander vereinbare Funktionsrollen zu verhindern?
136	137	Es werden Maßnahmen getroffen, um die Kombination von nicht miteinander vereinbare Funktionsrollen zu verhindern (Anf. 136), aber eine Kombination von Rollen bzw. Zugriffsrechten für eine Person, welche der Person mehr Rechte auf Datenzugriffe erteilt, als für ihre Aufgabe nötig ist, wird nicht verhindert?
80	5	Eine Einwilligung ist für den Betroffenen jederzeit mit Wirkung für die Zukunft temporär oder permanent widerrufbar (Anf. 80), aber erteilte Einwilligungen für die Lokalisierung des Nutzerstandortes können nicht jederzeit temporär oder permanent für die Zukunft widerrufen werden?
20	150	Für kryptographische Operationen werden nur geprüfte Standardbibliotheken verwendet, aber für die Implementierung von kryptografischen Verfahren werden keine etablierten und dem aktuellen Stand der Technik entsprechende Krypto-Bibliotheken genutzt?
24	23	Bei Erkennung eines ungültigen TLS-Server-Zertifikat wird die Verbindung unterbrochen (Anf. 24), aber bei Ungültigkeit oder Verbindungs-Timeout zum Revocation- oder OCSP-Server wird der Verbindungsaufbau nicht abgebrochen?
81	4	Der Widerruf ist mindestens so einfach, wie die Erteilung der Einwilligung (Anf. 81), aber der Widerruf der Einwilligung ist nicht so einfach wie die Erteilung der Einwilligung?