



Integrierter
Datenschutz



Medical Apps: Anforderungen aus Datenschutz und IT-Sicherheit

ds² Unternehmensberatung GmbH & Co. KG

Einführung: Medizinische Apps



©fotomek - stock.adobe.com

Seminar 3 „Medical Apps: Anforderungen aus Datenschutz und IT-Sicherheit“

Einführung

1. Einstieg in die Prüfung von medizinischen Apps
2. Apps als Medizinprodukt, die nicht als DiGA zugelassen sind
3. Apps als Ergänzung einer Standardbehandlung
4. Telemedizin
5. Sekundärnutzung z.B. für Werbung

Einführung: Was wird unter medizinische Apps verstanden?

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

Klassifizierung hilft für die Zuordnung der Anforderungen nur bedingt

 keine Berücksichtigung des Schutzbedarfs der Daten aus Sicht Datenschutz / IT-Sicherheit

Einführung: Datenschutz und IT-Sicherheit in medizinischen Apps

Diverse Untersuchungen zeigen Defizite in der Erfüllung grundlegender Aspekte von Datenschutz und IT-Sicherheit auf.

Mögliche Gründe:

- Entwicklung mobiler Anwendungen wird immer einfacher: Plugins, Tools und Software Development Kits ebnen den Weg
- Vertiefte Informatik-Kenntnisse und/oder Kenntnisse der Anforderungen aus unterschiedlichen Rechtsgebieten für die reine Entwicklung nicht erforderlich
 - für den Betrieb hingegen schon
- Bekanntes Dilemma: Privacy by Design und Privacy by Default adressieren den Verwender von Apps, aber nicht unmittelbar den Hersteller von Software

Einführung: Datenschutz und IT-Sicherheit in medizinischen Apps

Akteure bei Apps :

- die Anbieter/Betreiber von Apps,
- die Entwickler der Apps
(bei Eigenentwicklung ggf. in Personalunion mit dem Anbieter),
- ggf. Plattformbetreiber, über die Apps bezogen werden können,
- ggf. weitere beteiligte Parteien, z. B. Content-Agentur (Inhalts-Lieferant),

sowie

- die Anwender/Nutzer von Apps, deren Daten von den allen oder einigen der oben genannten verarbeitet werden

Einführung: Datenschutz und IT-Sicherheit in medizinischen Apps

Allgemeine datenschutzrechtliche Anforderungen

Kein spezifisches Datenschutzrecht für Gesundheits-Apps:

DS-GVO, BDSG & TTDSG geben Rahmen für die datenschutzrechtlichen Anforderungen vor

➤ Anbieter/Betreiber der App ist regelmäßig Verantwortlicher i. S. von Art. 4 Nr. 7 DS-GVO

Einführung: Datenschutz und IT-Sicherheit in medizinischen Apps

Allgemeine datenschutzrechtliche Anforderungen

Rolle des App-Entwicklers ist abhängig von den objektiven Kriterien der Zusammenarbeit:

- ggf. nur Lizenzgeber
- i. d. R. Auftragsverarbeiter (Art. 4 Nr. 8, Art. 28 DS-GVO)
- gemeinsam Verantwortlicher, falls die Festlegung der Mittel und Zwecke der Verarbeitung gemeinsam mit dem Auftraggeber erfolgt, (Art. 4 Nr. 7, Art. 26 DS-GVO)
- ggf. Dritter, falls Empfänger von personenbezogenen Daten vom Betreiber der App zur Verarbeitung zu eigenen Zwecken (Art. 4 Nr. 9, 10 DS-GVO)

Im Regelfall:

- Anbieter muss Entwickler Vorgaben zur Sicherstellung einer datenschutzkonformen App Vorgaben machen
 - Einhaltung der Datenschutzprinzipien, insb. Implementierung von technischen und organisatorischen Sicherheitsfunktionen in der App

Einführung: Datenschutz und IT-Sicherheit in medizinischen Apps

Bedrohungen gegen (mobile) Endgeräte & Apps (IT-Sicherheit)

- Smartphones & Apps werden für Angreifer immer attraktiver
- nur wenige Betriebssysteme (ganz überwiegend nur Android und iOS)
- Spyware für Apps auf mobilen Endgeräten nimmt zu
- Verwendung von unsicherem, eigenen Code oder ungeprüfte Verwendung von Code von Drittanbietern
- Verwendung unsicherer APIs (Application Programming Interfaces) zur Interaktion mit Fremdsystemen
- Verwendung schwacher Authentifizierungen
- „Ausufernde“ Rechtevergabe
- Datenabflüsse aufgrund Vernachlässigung von unternehmerischen Sorgfaltspflichten bei Betrieb von Apps
- etc.

Einführung: Sicherheit der Verarbeitung (Art. 32 DS-GVO)

Gewährleistung eines dem Risiko angemessenen Schutzniveaus



Geeignete technische und organisatorische Maßnahmen (TOM)



Festlegung
unter
Berück-
sichtigung
von



Risikoanalyse / Schutzbedarfsanalyse



Art, Umfang, Umstände und Zwecke der Verarbeitung



Stand der Technik*, Implementierungskosten,
Wirksamkeitsprüfungen

Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO



nachweisbar





* <https://www.stand-der-technik-security.de/startseite/>

Einführung: Privacy by Design (Art. 25 (1) DS-GVO)

Art. 25 (1) DS-GVO

„Datenschutz durch Technikgestaltung“

„Unter Berücksichtigung des **Standes der Technik, der Implementierungskosten** und der **Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung** sowie der unterschiedlichen **Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken** für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche **sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung** geeignete technische und organisatorische Maßnahmen ... um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.“


-  Kriterien für angemessene Sicherungsmaßnahmen
-  Berücksichtigung von Rahmenbedingungen der Verarbeitung
-  Verpflichtung zur risikobasierten Vorgehensweise
-  im Rahmen von Planung/Entwicklung und Betrieb

Einführung: Privacy by Design (Art. 25 (2) DS-GVO)

Art. 25 (2) DS-GVO

„Datenschutz durch Voreinstellung“

„Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass **durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden**. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.“

 datenschutzfreundliche Grundeinstellung, meint den bereits bestehenden oder vorausgewählten Wert einer konfigurierbaren Einstellung, die in der App zugewiesen wird. „Voreinstellungen“ oder „Werkseinstellungen“)

Einführung: Datenschutz und IT-Sicherheit in medizinischen Apps

Technische des BSI speziell für Gesundheits-Apps

(1) TR-03161 Anforderungen an Anwendungen im Gesundheitswesen - Teil 1: **Mobile Anwendungen**
Version 2.0, Stand 18. Mai 2022.

- URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03161/BSI-TR-03161-1.pdf?__blob=publicationFile&v=11

(2) 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

(3) 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

Erwartungshaltung der DSK:

„Die Datenschutzkonferenz fordert die Betreiber von Gesundheitswebseiten und Gesundheits-Apps auf, die berechtigten Vertraulichkeitserwartungen ihrer Nutzerinnen und Nutzer zu respektieren.“

- Zitat zur Weitergabe personenbezogener Gesundheitsdaten aus der Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 06.11.2019

... und die App-Entwickler?

Einführung: Medizinische Apps

„94. Auftragsverarbeiter und Hersteller werden in Artikel 25 zwar nicht direkt erwähnt, **gelten jedoch hinsichtlich der Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als wichtige Akteure**, denen bewusst sein sollte, dass die Verantwortlichen für die Verarbeitung personenbezogener Daten nur Systeme und Techniken mit integriertem Datenschutz verwenden dürfen.

95. Bei der Verarbeitung im Namen eines Verantwortlichen oder bei der Bereitstellung von Lösungen für Verantwortliche sollten Auftragsverarbeiter und Hersteller auf ihr Fachwissen zurückgreifen, um Vertrauen aufzubauen und ihre Kunden einschließlich KMU bei der Gestaltung/Beschaffung von Verarbeitungslösungen mit integriertem Datenschutz zu beraten. Dies wiederum bedeutet, dass die **Produkte und Dienste den Erfordernissen der Verantwortlichen entsprechend gestaltet** werden sollten.“

EDPB: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Rn. 94

https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_de.pdf

Einladung zur Diskussion



©fotomek - stock.adobe.com

Weitere Empfehlungen des EDPB für die Zusammenarbeit aus den Guidelines (Auszug)

- **Verantwortlichen** sollten Datenschutz bereits in der **Anfangsphase der Planung** (noch vor der Festlegung der Verarbeitungsmittel) eines Verarbeitungsvorgangs berücksichtigen und ihre/n **DSB einbeziehen**
- **Hersteller (und Auftragsverarbeiter)** sollten bestrebt sein, den **Nachweis dafür zu erbringen**, dass der **Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen im Lebenszyklus der von ihnen entwickelten Verarbeitungslösung gewährleistet ist**.
- **Hersteller und Auftragsverarbeiter sollten aktiv dazu beitragen**, dass die Erfüllung der Kriterien in Bezug auf den Stand der Technik sichergestellt ist, und sie sollten Verantwortliche **über etwaige Änderungen des Stands der Technik, die sich auf die Wirksamkeit der von ihnen eingeleiteten Maßnahmen auswirken können, informieren**. Die **Verantwortlichen** sollten diese **Anforderung als Vertragsklausel aufnehmen**, um sicherzustellen, dass sie auf dem neusten Stand gehalten werden.

Weitere Empfehlungen des EDPB für die Zusammenarbeit aus den Guidelines (Auszug)

- **Verantwortlichen** sollten **Hersteller und Auftragsverarbeiter** dazu **aufzufordern, zu zeigen**, inwiefern ihre Geräte, Anwendungsprogramme, Dienste oder Systeme den Verantwortlichen in die Lage versetzen, **den Anforderungen der Rechenschaftspflicht in Bezug auf den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu entsprechen**; z. B. durch die Verwendung zentraler Leistungsindikatoren, die die Wirksamkeit der Maßnahmen und Garantien für die Umsetzung der Grundsätze und Rechte belegen.
- **Ältere Systeme: gleiche Pflichten** für die Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen **wie für neue Systeme**.
 - Wenn die Einhaltung nicht bereits gewährleistet ist und wenn keine Änderungen vorgenommen werden können, um den Verpflichtungen nachzukommen, **erfüllt ein solches älteres System die Verpflichtungen zur Gewährleistung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen nicht und kann folglich für die Verarbeitung personenbezogener Daten nicht eingesetzt werden**.

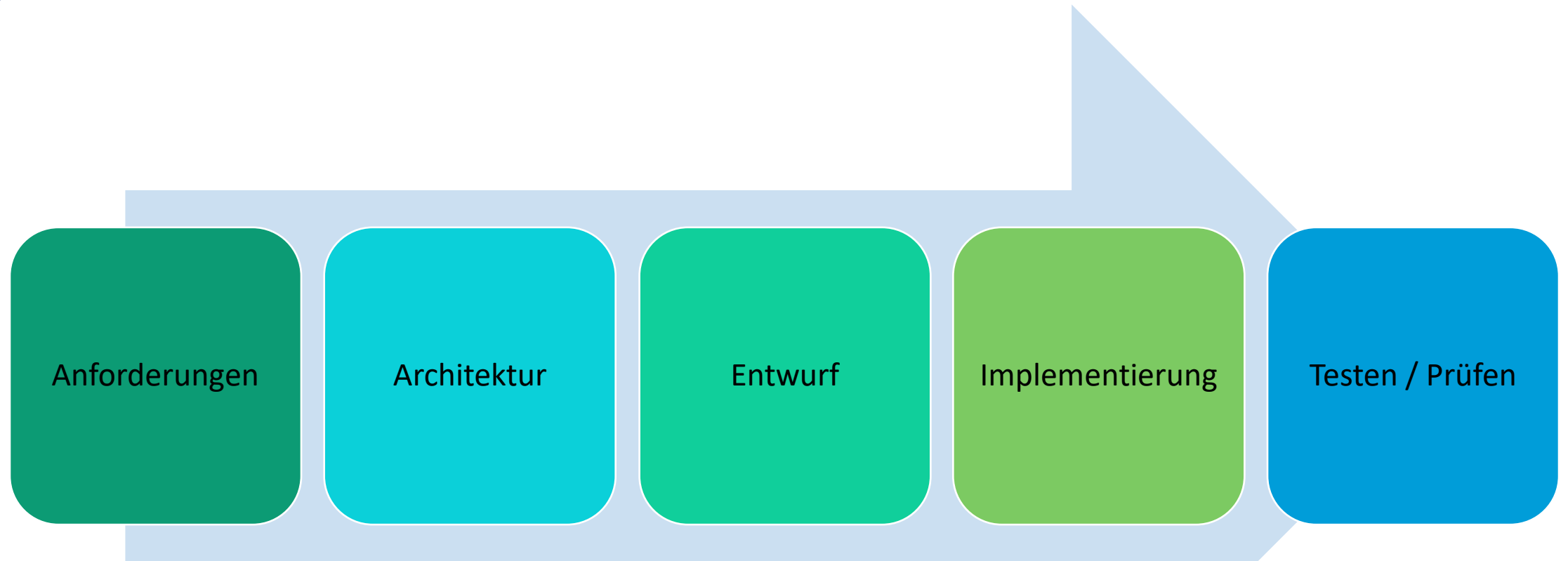
Einführung: Anforderung an medizinische Apps

- **Essenziell: Definition, Dokumentation & und Pflege der unterschiedlichen Anforderungen aus Datenschutz und IT-Sicherheit**
- **Berücksichtigung in allen Phasen des Entwicklungsprozesses**
- **Optimal: App-Entwickler, die Privacy by Design & Default sowie Security by Design zum zentralen Geschäftsziel machen** und nicht nur als technisches Merkmal begreifen.



©fotomek - stock.adobe.com

Einführung: Entwicklungsprozess von medizinischen Apps



Phasen der „guter“ App-Entwicklung

1. Einstieg in die Prüfung von medizinischen Apps

**Wie kommen die Anforderungen an den Entwickler?
Kennen die Entwickler die Schutzbedarfe der Daten?**

- Nicht nur Eigenschaften, Beschaffenheiten und Einsatzzwecke sollten festgelegt und dem Auftragnehmer (Entwickler) bekannt sein, sondern auch rechtliche Anforderungen und Schutzbedarfe
- Anbieter von Standardlösungen oftmals Experten auf eigenem Gebiet – schuldet aber keine Rechtsberatung

Fazit: Der Umfang der einzuhaltenden Anforderungen sollte klar definiert sein – wogegen soll sonst geprüft werden?

➔ Pflichtenheft für Datenschutz & IT-Sicherheit?



©fotomek - stock.adobe.com

Praxishilfe „Mobile Apps im Gesundheitswesen“ Version 1.0



©fotomek - stock.adobe.com

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	ds ² 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

➔ **„Pflichtenheft“ für Datenschutz & IT-Sicherheit!**

https://gesundheitsdatenschutz.org/html/datenschutz_ed_apps.php

Praxishilfe „Mobile Apps im Gesundheitswesen“: Ziel

Ziel der Praxishilfe:

- Hilfestellung für App-Entwickler, den Weg in die Thematik zu finden
- Unterstützung für DSB bei Beratung zu Apps und Überwachung/Prüfung von Apps im Gesundheitswesen
- Unterstützung von Verantwortlichen/Betreibern bei der „Ermutigung“ der Hersteller der Produkte, Dienste und Anwendungen, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass den Datenschutzpflichten nachgekommen werden kann.

Praxishilfe „Mobile Apps im Gesundheitswesen“: Zielgruppen

Zielgruppen der Praxishilfe:

- Software-Entwickler von mobilen Apps,
- Verantwortliche, welche Apps im Gesundheitswesen einsetzen,
- Datenschutzbeauftragte, die Software-Entwickler oder Verantwortliche beraten,
- Weitere Personen, z. B.
 - Auditoren,
 - Datenschutzbeauftragte,
 - Beschäftigte der Datenschutz-Aufsichtsbehörden oder 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

Praxishilfe „Mobile Apps im Gesundheitswesen“: Überblick

Grundlage: „Mobile Apps im Gesundheitswesen: Anforderungen aus dem Datenschutz“

Vers. 1.0, 125 Seiten

- 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.

Stand: 07.11.2022

https://gesundheitsdatenschutz.org/html/datenschutz_med_apps.php

ergänzend: „Praxishilfe zur Beachtung des TTDSG im

Bereich der Telemedizin “

Vers. 1.0, 53 Seiten

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

Stand 23.04.2022

<https://gesundheitsdatenschutz.org/html/ttdsg.php>

- Word-Datei
- Pdf-Datei
- ePub-Datei (für eBook Reader)
- Azw3-Datei (für Kindle)
- Excel-Datei mit tabellarischer Auflistung der Anforderungen (nur für Praxishilfe Apps)

Praxishilfe „Mobile Apps im Gesundheitswesen“: Begriff „App“

Begriff „App“ und Verständnis der Praxishilfe

Apps	Application Software / Anwendungssoftware oder –programm für Mobilgeräte, d.h. Software, die auf Smartphones und Tablets eingesetzt wird
Native Apps	Speziell für eine Plattform entwickelte Apps, Installation auf dem Device, eng an das Betriebssystem gebunden
Web-Apps	Browserbasierter Aufruf und Ausführung der App, nicht plattform- oder betriebssystemgebunden
Hybrid Apps	Kombination von Native App & Web App, Funktionalität weitgehend plattformunabhängig
Health Apps	Oberbegriff für Anwendungssoftware, die Gesundheitsdaten jeglicher Art verarbeitet
Medical Apps	Untergruppe von Health Apps für Anwendungssoftware, die ausschließlich Daten der medizinischen Versorgung verarbeitet, d.h. Patientendaten, die von einem health professional verarbeitet werden

Praxishilfe „Mobile Apps im Gesundheitswesen“: aus dem Inhalt

8. Mobile App i.d.R. ein Telemedium – Anforderungen aus TMG und TTDSG

- Alle elektronischen Informations- und Kommunikationsdienste sind Telemedien, soweit sie nicht
 - Telekommunikationsdienste nach § 3 Nr. 61 Telekommunikationsgesetz (TKG),
 - telekommunikationsgestützte Dienste nach § 3 Nr. 63 TKG oder
 - Rundfunk nach § 2 Rundfunkstaatsvertrag (RStV)
- mobile Apps, welche keinen Telekommunikationsdienst darstellen, müssen den Vorgaben für Telemedien genügen, d. h. insbesondere auch den Regelungen im TMG und TTDSG.

Anforderungen 1 - 38

9. Datenschutzrechtliche Anforderungen gem. DS-GVO

- Einhaltung der „Grundsätze für die Verarbeitung personenbezogener Daten“ [Anf. 39 – 70]
- Rechtsgrundlage der Verarbeitung inkl. Einwilligung [Anf. 40 – 83]
- Gewährleistung der Betroffenenrechte [Anf. 84 – 127]
- Sicherheit der Verarbeitung [Anf. 128 – 190]
- Kooperationen [Anf. 191 – 198]
- Verarbeitung in einem Drittland/Drittstaat [Anf. 199 – 200]
- Datenschutzerklärung / Datenhinweise für Apps [Anf. 201 – 210]

Anforderungen 39 - 210

4. Telemedizin

- weder TMG noch TTDSG enthalten spezifischen Regelungen für Gesundheitsdaten oder andere Art.9-Daten → datenschutzrechtliche Vorschriften gelten hier auch in gleicher Weise, keine Verdrängung der DS-GVO
- Besondere Herausforderung für Nicht-Juristen: Begriffsbestimmungsverweise
§ 2 (1) TTDSG „Die Begriffsbestimmungen des Telekommunikationsgesetzes, des Telemediengesetzes und der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) gelten auch für dieses Gesetz, soweit in Absatz 2 keine abweichende Begriffsbestimmung getroffen wird.“

Praxishilfe „Mobile Apps im Gesundheitswesen“: Anhänge

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

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

Anhang 3: Beispiel für Datenschutzerklärung / Datenhinweise für Medical Apps

Anhang 4 Hinweise zur Planung von Maßnahmen zur Umsetzung von Datenschutz und IT-Sicherheit

Anhang 4.1: Hinweise bzgl. Maßnahmen vor Beginn der Entwicklung einer App

Anhang 4.2: Hinweise zur Planung von fortlaufend erforderlichen Maßnahmen

Anhang 4.3: Hinweise zum Vorgehen bei der Erhebung von Daten

Anhang 4.4: Hinweise zum Schutz von ruhenden Daten („Data at Rest“)

Anhang 4.5: Hinweise zum Schutz von Daten während der Verarbeitung („Data in Use“)

Anhang 4.6: Hinweise zum Schutz von Daten während des Transfers („Data at Transit“)

Praxishilfe „Mobile Apps im Gesundheitswesen“: Anhänge

Anhang 5: Beispiele für Maßnahmen hinsichtlich IT-Sicherheit

Anhang 5.1: Allgemeines

Anhang 5.2: Anwendung/Frontend

Anhang 5.3: Server/Backend

Anhang 5.4: Kommunikation

Anhang 6: Checkliste Einwilligung

Anhang 7: Checkliste „Erfüllung der Anforderungen“

Anhang 7.1: Aufbau der Excel-Tabelle

Anhang 7.2: Anforderungen, die in Beziehung zueinanderstehen

Praxishilfe „Mobile Apps im Gesundheitswesen“: Anforderungen

Praxishilfe verwendet sog. „Muss-, Soll-, Kann- und Darf-Vorschriften“ bei der Darstellung der Anforderungen (aus Sicht der Autoren):

MUSS / MÜSSEN	Die Anforderung ist zwingend, d. h. in jedem Fall einzuhalten
SOLL / SOLLTEN	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.

Nicht jede Anforderung muss immer erfüllt werden – es hängt von den Voraussetzungen ab

Praxishilfe „Mobile Apps im Gesundheitswesen“: Anforderungen

- Beschränkung auf die Beschreibung von Anforderungen aus dem Umfeld von Datenschutz und IT-Sicherheit,
 - die bei der Entwicklung und Bereitstellung von „Medical Apps“ anzuwenden sind
 - die auch für „Health Apps“ „ gelten können, aber nicht zwingend gelten müssen.
- keine abschließende Darstellung aller möglichen Anforderung
 - Darstellung der wichtigsten Anforderungen
 - Einzelfallbewertung des konkreten Verarbeitungsbedarfs notwendig

1. Einstieg in die Prüfung von medizinischen Apps

Wie soll die Prüfung geplant werden?

Was soll geprüft werden?



1. Einstieg in die Prüfung von medizinischen Apps

Anhang 7: Checkliste „Erfüllung der Anforderungen“

- alle Anforderungen der Praxishilfe in einer Excel-Tabelle

Seite	Nr. Anforderung	Erfüllungsgrad-Kriterium	Text Anforderung	Grundlage Anforderung in der DS-GVO	Thematische Zuordnung	Anforderung (ja/nein/aus)
21	1	Muss	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.	Art. 7, Art. 9 Abs. 2 lit. a DS-GVO: Einwilligung	Standortdaten	
21	2	Muss	Die Genauigkeit der Lokalisierung MUSS sich am Zweck des Service orientieren.	Art. 5 Abs. 1 lit. b DS-GVO: Zweckbindung	Standortdaten	
21	3	Muss	Die Verarbeitung von Standortdaten MUSS in den Datenschutzhinweisen dargestellt werden.	Art. 12 DS-GVO: Transparenzpflicht	Standortdaten	
21	4	Kann	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.	Art. 7 Abs. 3 DS-GVO: Einwilligung	Standortdaten	
21	5	Muss	Erteilte Einwilligungen für die Lokalisierung des Nutzerstandortes MÜSSEN jederzeit temporär oder permanent für die Zukunft widerrufen werden können.	Art. 7 Abs. 3 DS-GVO: Einwilligung	Standortdaten	
21	6	Muss	Die personenbezogenen Daten MÜSSEN gegen die Kenntnisnahme unberechtigter Dritter geschützt werden.	Art. 32 Abs. 1 lit. b DS-GVO: Vertraulichkeit	Vertraulichkeit	
21	7	Muss	Das System MUSS es Benutzern ermöglichen, sich von ihrer laufenden Sitzung abzumelden.	Art. 32 Abs. 1 lit. b DS-GVO: Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit	Vertraulichkeit	
22	8	Muss	Benutzerkonten MÜSSEN mit mindestens einem geeigneten Authentisierungsmerkmal geschützt werden.	Art. 5 Abs. 1 lit f, Art. 32 Abs. 1 lit. b DS-GVO: Vertraulichkeit	Authentifizierung	
22	9	Muss	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 .	Art. 32 Abs. 1 lit. b DS-GVO: Integrität	Authentifizierung	
22	10	Darf nicht	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.	Art. 32 Abs. 1 lit. b DS-GVO: Vertraulichkeit	Authentifizierung	
22	11	Muss	Falls Passwörter als Authentisierungsmerkmal genutzt werden, MUSS eine Änderung des	Art. 32 Abs. 1 lit. b DS-GVO:	Authentifizierung	

1. Einstieg in die Prüfung von medizinischen Apps

Anhang 7: Checkliste „Erfüllung der Anforderungen“

- thematische Sortierung oder Filterung der Anforderungen der Praxishilfe möglich
- Generierung spezifischer Checklisten für Entwickler, DSB und andere
- Immer beachten: Anforderungen können auch mehrere Stellen innerhalb der DS-GVO betreffen
 - z. B. Anforderungen zur Einwilligung:
 - Art. 5 Abs. 1 lit. a DS-GVO Rechtmäßigkeit
 - Art. 7 DS-GVO: allg. Anforderungen,
 - Art. 8 DS-GVO: Kinder bzgl. Dienste der Informationsgesellschaft
 - Art. 9 Abs. 2 lit. a DS-GVO: besondere Kategorien / health data



©fotomek - stock.adobe.com

1. Einstieg in die Prüfung von medizinischen Apps

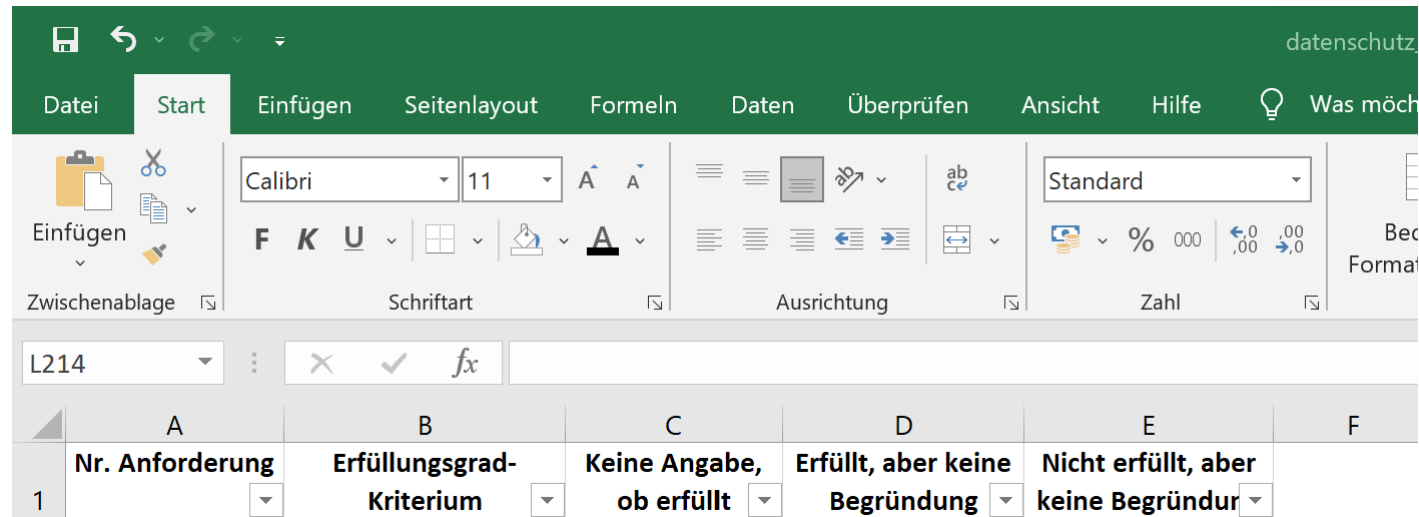
Aufbau der Checkliste „Erfüllung der Anforderungen“, hier Tabellenblatt „Anforderungsliste“

Spalte	
1	Seitenzahl der entsprechenden Anforderung in der Praxishilfe
2	Nummer der Anforderung aus der Praxishilfe
3	Erfüllungsgrad der Anforderung
4	Text der Anforderung
5	Zuordnung der Anforderung zu einer relevanten Stelle der DS-GVO
6	thematische Zuordnung der Anforderung zur Ermöglichung einer Sortierung oder Filterung (in der Tabelle)
7	Erfüllungsstatus der Anforderung (ja/nein)
8	Angabe, wodurch diese Anforderung erfüllt wird
9	Angabe, wodurch diese Anforderung <u>nicht</u> erfüllt wird
10	Prüfvermerk, idealerweise mit Begründung (des Prüfers)

1. Einstieg in die Prüfung von medizinischen Apps

Aufbau der Checkliste „Erfüllung der Anforderungen“, hier Tabellenblatt „Auffälligkeiten“

- Übersicht, welche Anforderungen bzgl. des Kriteriums „erfüllt“ bzw. „nicht erfüllt“ bearbeitet wurden, bzw. welche Antworten noch offen sind.
- Prüfung, ob vorhandener Text zur Darstellung, wie das Kriterium behandelt wurde, vorhanden ist.



The screenshot shows the Microsoft Excel interface with the 'Start' ribbon selected. The table below is a checklist for 'Auffälligkeiten' (Issues/Findings). The table has columns for 'Nr. Anforderung' (Requirement No.), 'Erfüllungsgrad-Kriterium' (Compliance Level-Criterion), 'Keine Angabe, ob erfüllt' (No indication if fulfilled), 'Erfüllt, aber keine Begründung' (Fulfilled, but no justification), and 'Nicht erfüllt, aber keine Begründung' (Not fulfilled, but no justification). The first row is numbered '1'.

	A	B	C	D	E	F
L214	Nr. Anforderung	Erfüllungsgrad-Kriterium	Keine Angabe, ob erfüllt	Erfüllt, aber keine Begründung	Nicht erfüllt, aber keine Begründung	
1						

1. Einstieg in die Prüfung von medizinischen Apps

Aufbau der Checkliste „Erfüllung der Anforderungen“, hier Tabellenblatt „Prüfkriterien“

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?

1. Einstieg in die Prüfung von medizinischen Apps: Szenarien

a) DSB möchte Einhaltung von Privacy by Design und Privacy by Default prüfen,

Checkliste „Erfüllung der Anforderungen“							
Seite	Nr. Anforderung	Erfüllungsgrad-Kriterium	Text Anforderung	Grundlage Anforderung in der DS-GVO	Thematische Zuordnung	Anforderung erfüllt (ja/nein auswählen)	Anforde (Kurze)
32	60	Muss	Alle Personen, welche auf die gespeicherten Gesundheitsdaten zugreifen können, MÜSSEN vor dem erstmaligen Zugriff auf die Wahrung des Datengeheimnisses verpflichtet worden sein.	Art. 5 Abs. 1 lit. f DS-GVO: Vertraulichkeit	Verpflichtung		
58	169	Muss	Bei der Planung von Apps MÜSSEN von Anfang an die Anforderungen der Datenschutz-Grundverordnung berücksichtigt werden. Die Dokumentation der App-Entwicklung MUSS dies darstellen.	Art. 25 Abs. 1 DS-GVO: Privacy by Design/Default	Rechtmäßigkeit		
58	170	Muss	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.	Art. 25 Abs. 1 DS-GVO: Privacy by Design/Default	Security Development Lifecycle		
58	172	Muss	Apps MÜSSEN die in Kapitel 3 Datenschutz-Grundverordnung enthaltenen Betroffenenrechte gewährleisten. In der Dokumentation der App MUSS die Gewährleistung der Betroffenenrechte nachvollziehbar dargestellt sein.	Art. 25 Abs. 1 DS-GVO: Privacy by Design/Default	Betroffenenrechte		
58	173	Muss	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.	Art. 25 Abs. 1 DS-GVO: Privacy by Design/Default	Beachtung Grundsätze bei der Verarbeitung		
58	174	Muss	In einer APP MUSS die Grundeinstellung der App den maximal möglichen Datenschutz darstellen. Ein Benutzer KANN den Datenschutz durch Änderung der Einstellungen aktiv herabsenken.	Art. 25 Abs. 2 DS-GVO: Privacy by Design/Default	Datenschutzfreundliche Voreinstellungen		
59	175	Darf nicht	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.	Art. 25 Abs. 2 DS-GVO: Privacy by Design/Default	Datenminimierung		

1. Einstieg in die Prüfung von medizinischen Apps: Szenarien

a) DSB möchte Einhaltung von Privacy by Design und Privacy by Default prüfen

Checkliste „Erfüllung der Anforderungen“

Seite	Nr. Anforderung	Erfüllungsgrad-Kriterium	Text Anforderung	Grundlage Anforderung in der DS-GVO	Thematische Zuordnung	Anforderung erfüllt (ja/nein auswählen)	Anforderung erfüllt durch (Kurze Beschreibung)
32	60	Muss	Alle Personen, welche auf die gespeicherten Gesundheitsdaten zugreifen können, MÜSSEN vor dem erstmaligen Zugriff auf die Wahrung des Datengeheimnisses verpflichtet worden sein.	Art. 5 Abs. 1 lit. f DS-GVO: Vertraulichkeit	Verpflichtung	ja	Prozess für die Einholung der Vertraulichkeitsverpflichtung sowie die Erst-Unterweisung besteht. Prozessbeschreibung ist DSB bekannt.
58	169	Muss	Bei der Planung von Apps MÜSSEN von Anfang an die Anforderungen der Datenschutz-Grundverordnung berücksichtigt werden. Die Dokumentation der App-Entwicklung MUSS dies darstellen.	Art. 25 Abs. 1 DS-GVO: Privacy by Design/Default	Rechtmäßigkeit	nein	
58	170	Muss	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.	Art. 25 Abs. 1 DS-GVO: Privacy by Design/Default	Security Development Lifecycle	nein	
58	172	Muss	Apps MÜSSEN die in Kapitel 3 Datenschutz-Grundverordnung enthaltenen Betroffenenrechte gewährleisten. In der Dokumentation der App MUSS die Gewährleistung der Betroffenenrechte nachvollziehbar dargestellt sein.	Art. 25 Abs. 1 DS-GVO: Privacy by Design/Default	Betroffenenrechte	nein	
58	173	Muss	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.	Art. 25 Abs. 1 DS-GVO: Privacy by Design/Default	Beachtung Grundsätze bei der Verarbeitung	ja	Konfiguration durch den Anbieter
58	174	Muss	In einer APP MUSS die Grundeinstellung der App den maximal möglichen Datenschutz darstellen. Ein Benutzer KANN den Datenschutz durch Änderung der Einstellungen aktiv herabsenken.	Art. 25 Abs. 2 DS-GVO: Privacy by Design/Default	Datenschutzfreundliche Voreinstellungen	ja	Alle Einwilligungsschieberegler sind per Default auf "nicht eingewilligt gestellt".
59	175	Darf nicht	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.	Art. 25 Abs. 2 DS-GVO: Privacy by Design/Default	Datenminimierung	nein	

1. Einstieg in die Prüfung von medizinischen Apps

a) DSB möchte Einhaltung von Privacy by Design und Privacy by Default prüfen

Grundlage Anforderung in der DS-GVO	Thematische Zuordnung	Anforderung erfüllt (ja/nein auswählen)	Anforderung erfüllt durch (Kurze Beschreibung)	Anforderung nicht zu erfüllen weil (Kurze Begründung)
Art. 5 Abs. 1 lit. f DS-GVO: Vertraulichkeit	Verpflichtung	ja	Prozess für die Einholung der Vertraulichkeitsverpflichtung sowie die Erst-Unterweisung besteht. Prozessbeschreibung ist DSB bekannt.	
Art. 25 Abs. 1 DS-GVO: Privacy by Design/Default	Rechtmäßigkeit	nein		Hersteller / Entwickler hat eine solche Dokumentation in der Vergangenheit nicht erstellt, Pflicht war ihm nicht bekannt und entstand erst vertraglich durch Beauftragung des Auftraggebers. Es liegt lediglich eine Dokumentation des Anbieters vor.
Art. 25 Abs. 1 DS-GVO: Privacy by Design/Default	Security Development Lifecycle	nein		Lizenzmodell: Standardvertrag sieht diese Anforderungen nur zum Teil vor. Lizenzmodell und Vertragsklauseln zum Datenschutz nicht verhandelbar.
Art. 25 Abs. 1 DS-GVO: Privacy by Design/Default	Betroffenenrechte	nein		Im Standardprodukt ist keine Löschfunktion vorgesehen.
Art. 25 Abs. 1 DS-GVO: Privacy by Design/Default	Beachtung Grundsätze bei der Verarbeitung	ja	Konfiguration durch den Anbieter	
Art. 25 Abs. 2 DS-GVO: Privacy by Design/Default	Datenschutzfreundliche Voreinstellungen	ja	Alle Einwilligungsschieberegler sind per Default auf "nicht eingewilligt gestellt".	
Art. 25 Abs. 2 DS-GVO: Privacy by Design/Default	Datenminimierung	nein		Transfers an Dritte in erfolgen durch Verwendung von Fremdcode / Bibliotheken. Abschalten nicht möglich.

1. Einstieg in die Prüfung von medizinischen Apps

a) DSB möchte Einhaltung von Privacy by Design und Privacy by Default prüfen

Tabellenreiter „Auffälligkeiten“:

- Übersicht, welche Anforderungen bzgl. des Kriteriums „erfüllt“ bzw. „nicht erfüllt“ bearbeitet wurden, bzw. welche Antworten noch offen sind.
- Prüfung, ob vorhandener Text zur Darstellung, wie das Kriterium behandelt wurde, vorhanden ist.

Nr. Anforderung	Erfüllungsgrad-Kriterium	Keine Angabe, ob erfüllt	Erfüllt, aber keine Begründung	Nicht erfüllt, aber keine Begründung
60	Muss		X	
169	Muss			X
170	Muss			X
172	Muss			X
173	Muss		X	
174	Muss		X	
175	Darf nicht			X

1. Einstieg in die Prüfung von medizinischen Apps

b) Entwickler möchte Überblick zu Anforderungen an die Einwilligung:

Orientierung an **Anhang 6: Checkliste Einwilligung**

enthält detaillierte **Prüffragen** (ja/nein) zu den Aspekten:

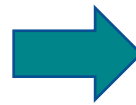
- **Allgemein**
- **Form**
- **Willensbekundung**
- **Transparenz**
- **Freiwilligkeit**
- **Informiertheit**
- **Bestimmtheit**
- **Ausdrücklichkeit**
- **Einwilligung Minderjähriger**
- **Widerrufbarkeit**
- **Nachweisbarkeit**
- **Drittlandtransfers**
- **Kopplungsverbot**
- **Broad Consent**

1. Einstieg in die Prüfung von medizinischen Apps

b) Entwickler möchte Anforderungen an Einwilligung prüfen:

Anhang 7: Checkliste „Erfüllung der Anforderungen“ mit Filter:

- Art. 5 Abs. 1 lit. a DS-GVO
- Art. 7 DS-GVO
- Art. 8 DS-GVO
- Art. 9 Abs. 2 lit. a DS-GVO



Nr. der Anforderung	Grundlage der Anforderung in der DS-GVO
21	Art. 7, Art. 9 Abs. 2 lit. a DS-GVO: Einwilligung
21	Art. 7 Abs. 3 DS-GVO: Einwilligung
21	Art. 7 Abs. 3 DS-GVO: Einwilligung
27	Art. 7, Art. 9 Abs. 2 lit. a DS-GVO: Einwilligung
27	Art. 7, Art. 9 Abs. 2 lit. a DS-GVO: Einwilligung
27	Art. 7 DS-GVO: Einwilligung
34	Art. 7, Art. 9 Abs. 2 lit. a DS-GVO: Einwilligung
34	Art. 7, Art. 9 Abs. 2 lit. a DS-GVO: Einwilligung
34	Art. 7, Art. 8 DS-GVO: Einwilligung
34	Art. 7 DS-GVO: Einwilligung
37	Art. 7 DS-GVO: Einwilligung
38	Art. 7 Abs. 3 DS-GVO: Einwilligung
38	Art. 7 Abs. 3 DS-GVO: Einwilligung
45	Art. 5 Abs. 1 lit. a, Art. 9 DS-GVO: Rechtmäßigkeit
46	Art. 7, Art. 9 Abs. 2 lit. a DS-GVO: Einwilligung
80	Art. 5 Abs. 1 lit. a, Art. 9 DS-GVO: Rechtmäßigkeit

1. Einstieg in die Prüfung von medizinischen Apps

b) Entwickler möchte Maßnahmen planen:

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

1. Einstieg in die Prüfung von medizinischen Apps

b) Entwickler möchte Maßnahmen planen:

Anhang 4.2: Hinweise zur Planung von fortlaufend erforderlichen Maßnahmen

Anhang 4.3: Hinweise zum Vorgehen bei der Erhebung von Daten

Anhang 4.4: Hinweise zum Schutz von ruhenden Daten („Data at Rest“)

Anhang 4.5: Hinweise zum Schutz von Daten während der Verarbeitung („Data in Use“)

Anhang 4.6: Hinweise zum Schutz von Daten während des Transfers („Data at Transit“)

2. Apps als Medizinprodukt (nicht als Diga zugelassen)

Begriff „Medizinprodukt“ gem. Art. 2 Ziff. 1 der Verordnung (EU) 2017/745

„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.

2. Apps als Medizinprodukt (nicht als Diga zugelassen)

Zuordnung als „**Medizinprodukt**“ ist kein Wunschkonzert:

- es liegt daher nicht im Ermessen eines Herstellers, Händlers oder Betreibers eines Softwareprodukts wie einer App, ob diese ein Medizinprodukt ist.
- trifft die Begriffsdefinition zu, so handelt es sich bei der Mobile App um ein Medizinprodukt.
- keine speziellen datenschutzrechtlichen Anforderungen in Verordnung (EU) 2017/745 – DS-GVO gilt unmittelbar sowie ergänzend die nationalen datenschutzrechtlichen Vorgaben
- Anhang I (Kap. II Ziff. 17.4, Kap. III lit. ab) der Verordnung (EU) 2017/745 verpflichtet 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“, festzulegen.
 - Keine konkrete Vorgabe, daher Stand der Technik als Maßstab

2. Apps als Medizinprodukt (nicht als Diga zugelassen)

Zuordnung als „**Medizinprodukt**“ ist kein Wunschkonzert:

- Viele Medical Apps sind vermutlich Medizinprodukte, Einordnung aber oft nicht einfach
- Hilfestellung bei der Einordnung:
 - Anhang I der Leitlinien der Medical Device Coordination Group (MDCG): Guidance MDCG 2019-11 - Qualification and classification of software. 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
 - Orientierungshilfe des BfArM https://www.bfarm.de/DE/Medizinprodukte/Aufgaben/Abgrenzung-und-Klassifizierung/_artikel.html

3. Apps als Ergänzung einer Standardbehandlung: DiGA

- Festlegung von Anforderungen an IT-Sicherheit entsprechend § 139e Abs. 10 SGB V9 von BSI im Einvernehmen mit dem BfArM und im Benehmen mit dem BfDI
- Festlegung der Prüfkriterien für die nachzuweisenden Anforderungen an den Datenschutz gemäß § 139e Abs. 11 SGB V9 durch BfArM legt im Einvernehmen mit dem BfDI und im Benehmen mit dem BSI.
- Anlage 1 „Fragebogen gemäß § 4 Abs. 6“ der DiGAV10 enthält diverse Anforderungen an Datenschutz und IT-Sicherheit, deren Einhaltung rechtlich vorgeschrieben ist.

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



©fotomek - stock.adobe.com

3. Apps als Ergänzung einer Standardbehandlung: DiPA

- Festlegung von Anforderungen an Datensicherheit entsprechend § 78a Abs. 7 SGB XI durch das BSI im Einvernehmen mit dem BfArM und im Benehmen mit dem BfDI
- Festlegung der von DiPA-Herstellern nachzuweisenden Prüfkriterien für die nachzuweisenden Anforderungen an den Datenschutz entsprechend § 78a Abs. 8 SGB XI durch das BfArM im Einvernehmen mit dem BfDI und im Benehmen mit dem BSI
- In aktuell in Ausarbeitung befindlichen Verordnung zur Erstattungsfähigkeit digitaler Pflegeanwendungen (VdiPA) werden weitergehende Anforderungen beschrieben, die voraussichtlich überwiegend den Vorgaben an eine DiGA entsprechen

Auf spezifische Anforderungen für diese sogenannten DiPA wird in der Praxishilfe nicht eingegangen.



©fotomek - stock.adobe.com

4. Telemedizin

- „Telemedizin ist ein Sammelbegriff für verschiedenartige ärztliche Versorgungskonzepte.“
- „Diese Konzepte weisen als Gemeinsamkeit den prinzipiellen Ansatz auf, dass medizinische Leistungen der Gesundheitsversorgung in den Bereichen Diagnostik, Therapie und Rehabilitation sowie bei der ärztlichen Entscheidungsberatung über räumliche Entfernungen (oder zeitlichen Versatz) hinweg erbracht werden.“
- „Hierbei werden Informations- und Kommunikationstechnologien eingesetzt.“

Bundesärztekammer

<https://www.bundesaerztekammer.de/themen/aerzte/digitalisierung/telemedizin-fernbehandlung>



Je nach Einsatzgebiet der App ist ggf. Bestandteil von Telemedizin.

4. Telemedizin

- Immer in telemedizinische Dienstleistungen beinhaltet: die Übertragung besonderer Kategorien personenbezogener Daten
- Weder TMG noch TTDSG enthalten spezifischen Regelungen für Gesundheitsdaten oder andere Art.9-Daten → datenschutzrechtliche Vorschriften gelten hier auch in gleicher Weise, keine Verdrängung der DS-GVO
- Auch hier: besondere Herausforderung für Nicht-Juristen: Begriffsbestimmungsverweise in den Gesetzen, verbunden mit dem Fehlen einer Legaldefinition für Telemedizin
 - § 2 (1) TTDSG „Die Begriffsbestimmungen des Telekommunikationsgesetzes, des Telemediengesetzes und der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) gelten auch für dieses Gesetz, soweit in Absatz 2 keine abweichende Begriffsbestimmung getroffen wird.“

5. Sekundärnutzung

Was meint Sekundärnutzung?

- Personenbezogene Daten entstehen in konkreten Anwendungskontexten, in der Regel zweckgebunden unter einem oder mehreren primären Verwendungszwecken
- Sekundärnutzung geht daher häufig mit einer Zweckänderung einher, ggf. Abwägung nach Art. 6 (4) DS-GVO durchzuführen
- Zweckbindung ist ein Hauptgrundsatz der DS-GVO gem. Art. 5 Abs. 1 lit. b:
 - Verarbeitung personenbezogener Daten darf nur im Rahmen von festgelegten, eindeutigen und legitimen Zwecken erfolgen.
 - Eine Änderung des Zweckes bedarf wiederum eines eigenen Erlaubnistatbestandes.
 - Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke nicht unvereinbar mit dem ursprünglichen Zweck,
 - für andere Zweckänderungen ggf. nachzuweisen.

5. Sekundärnutzung, hier: Bezug zur Zweckbindung

- 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.

aus S. 29 der Praxishilfe

5. Sekundärnutzung, hier: Werbung allgemein

„Ohne Werbung geht es nicht, mit aber auch nicht überall“

→ spezifische Vorgaben beachten

Gesetz über die Werbung auf dem Gebiet des Heilwesens
(Heilmittelwerbegesetz)

- macht Vorgaben für Zulässigkeit von Werbemaßnahmen
 - Werbung gegenüber Fachkreisen & Patienten (Laien) zulässig,
 - irreführende Werbung verboten

→ Check im Einzelfall erforderlich, insb. bei DiGA



WERBUNG????

5. Sekundärnutzung, hier: Werbung & pbD

Aber was ist mit berechtigten Interessen für Direktmarketingmaßnahmen?

Cave: Gesundheitsdaten!

„**Nutzung personenbezogener Daten der besonderen Kategorie von App-Anwendern aufgrund einer Interessensabwägung ist – 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.**“ (s. S. 39 der Praxishilfe)

Für jegliche Verarbeitung personenbezogener genetischer, biometrischer oder Gesundheitsdaten zu anderen Zwecken, **insbesondere zu Zwecken der Werbung in der Regel** ausdrückliche Einwilligung der jeweils betroffenen Person erforderlich sein.



WERBUNG????

Diskussion & Fragen



©fotomek - stock.adobe.com

Checkliste in Action



©fotomek - stock.adobe.com



Integrierter
Datenschutz



Herzlichen Dank für Ihre Aufmerksamkeit!

Fragen oder Anregungen? – Bitte melden Sie sich gerne:

Andrea Backer-Heuveldop

ds² Unternehmensberatung GmbH & Co. KG

Falkenstraße 10

33775 Versmold

Zentrale: +49 5423 95 993 20

andrea.heuveldop@ds-quadrat.de