Beschluss

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. November 2023

Positionspapier zu cloudbasierten digitalen Gesundheitsanwendungen

Einleitung

Seit 2020 ist für die erstattungsfähigen digitalen Gesundheitsanwendungen gemäß § 33a SGB V die Digitale Gesundheitsanwendungen-Verordnung (DiGAV) in Kraft. Sie regelt, dass digitale Gesundheitsanwendungen die gesetzlichen Vorgaben des Datenschutzes und die Anforderungen an die Datensicherheit nach dem Stand der Technik unter Berücksichtigung der Art der verarbeiteten Daten und der damit verbundenen Schutzstufen sowie des Schutzbedarfs gewährleisten (§ 4 Abs. 1 DiGAV) müssen.

Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) führt gemäß § 139e Abs. 1 SGB V ein Verzeichnis erstattungsfähiger digitaler Gesundheitsanwendungen (DiGA) nach § 33a SGB V und entscheidet auch über die Anträge der DiGA-Hersteller zur Aufnahme in das Verzeichnis.

Dabei weisen die Hersteller digitaler Gesundheitsanwendungen die Erfüllung der datenschutzrechtlichen Anforderungen gemäß § 139e Abs. 2 Satz 2 Nummer 2 SGB V derzeit unter Verwendung der Erklärung nach Anlage 1 zur Digitale Gesundheitsanwendungen-Verordnung (DiGAV) nach. Die Herstellererklärung (Selbsterklärung) ist jedoch kein sicheres Mittel, um die Einhaltung der datenschutzrechtlichen Anforderungen nachzuweisen. Daher wurden diesbezüglich die gesetzlichen Anforderungen angepasst:

- Ab dem 1. Januar 2025 müssen digitale Gesundheitsanwendungen abweichend von den Anforderungen an die Datensicherheit nach § 4 Abs. 6 DiGAV die von dem Bundesamt für Sicherheit in der Informationstechnik nach § 139e Abs. 10 SGB V festgelegten Anforderungen an die Datensicherheit erfüllen (§ 4 Abs. 7 DiGAV).

- Gemäß der derzeit geltenden rechtlichen Regelung müssen ab dem 1. August 2024 digitale Gesundheitsanwendungen, abweichend von den Anforderungen an den Datenschutz nach Absatz 6, die von dem Bundesinstitut für Arzneimittel und Medizinprodukte nach § 139e Abs. 11 SGB V festgelegten Prüfkriterien für die von digitalen Gesundheitsanwendungen nachzuweisenden Anforderungen an den Datenschutz umsetzen (§ 4 Abs. 8 DiGAV).

Neben diesen gesetzlich geregelten DiGA gibt es jedoch eine Vielzahl weiterer Gesundheitsanwendungen, die nicht von diesen Regelungen erfasst sind. Für den Einsatz dieser Vielzahl der weiteren Anwendungen ist aus Sicht der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) Folgendes zu bedenken:

I. Verantwortlichkeiten

Die Feststellung der datenschutzrechtlichen Verantwortlichkeit ist für die nicht unter § 139e SGB V fallenden digitalen Gesundheitsanwendungen ausgesprochen komplex, insbesondere da sich daran verschiedene Aufgaben und Pflichten ausrichten. Grundsätzlich kommen verschiedene Konstellationen der datenschutzrechtlichen Verantwortlichkeit in Betracht.

Die DS-GVO verpflichtet Verantwortliche und Auftragsverarbeiter, Art. 4 Nrn. 7 und 8 DS-GVO. Hersteller nehmen die Rolle eines Verantwortlichen ein, wenn sie neben der Herstellung der digitalen Gesundheitsanwendung zugleich über die Zwecke und Mittel der Datenverarbeitung entscheiden. Sie kommen abweichend hiervon als Auftragsverarbeiter in Betracht, wenn sie für einen Verantwortlichen personenbezogene Daten nach Maßgabe von Artikel 28 und 29 DS-GVO weisungsgebunden verarbeiten. Erschöpft sich die Beteiligung dagegen in der Herstellung der Gesundheitsanwendung, sodass die Hersteller keine personenbezogenen Daten der Nutzer verarbeiten, sind die Hersteller weder Verantwortliche noch Auftragsverarbeiter.

Neben den Herstellern kommen hinsichtlich der Verarbeitung personenbezogener Daten der digitalen Gesundheitsanwendungen weitere Beteiligte in Betracht, wie etwa Ärztinnen und Ärzte und andere medizinische Leistungserbringer sowie Anbieter von Cloud-Diensten. Dabei ist im Einzelfall zu prüfen, welche Rolle diese Beteiligten aus Datenschutzsicht wahrnehmen. Hierfür sind ggf. Formen der alleinigen oder gemeinsamen Verantwortlichkeit oder eine Auftragsverarbeitung von Bedeutung.

Nähere Erläuterungen enthalten die Leitlinien 07/2020 des Europäischen Datenschutzausschusses (EDSA) zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO[1], z. B. in Rn. 26:

> „Die Notwendigkeit einer Beurteilung der Faktenlage bedeutet auch, dass sich die Rolle des Verantwortlichen nicht aus der Art der Organisation ergibt, die Daten verarbeitet, sondern aus ihren konkreten Tätigkeiten in einem bestimmten Kontext. Anders ausgedrückt kann ein und dieselbe Organisation gleichzeitig hinsichtlich bestimmter Verarbeitungen als Verantwortlicher und hinsichtlich anderer Verarbeitungen als Auftragsverarbeiter handeln; die Einstufung als Verantwortlicher oder als Auftragsverarbeiter muss jeweils im Hinblick auf den konkreten Datenverarbeitungsvorgang bewertet werden.“

Bei dieser Beurteilung sollte auch berücksichtigt werden, ob es sich um einen einheitlichen Lebenssachverhalt handelt, in dem die verschiedenen Aspekte der Verarbeitung nur als Ganzes einen Sinn ergeben.[2]

Entsprechend dem Transparenzgrundsatz der DS-GVO ist zudem der Zweck der Verarbeitung personenbezogener Daten und der jeweilige Verantwortliche in der Datenschutzerklärung kenntlich zu machen.

II. Verwendung der Gesundheitsanwendung ohne Nutzung der Cloudfunktionen

Die Verwendung der Gesundheitsanwendung (z. B. einer App zum Auslesen und Speichern der Glukosewerte) muss nach dem Grundsatz „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ nach Art. 25 Abs. 1 DS-GVO auch ohne Nutzung der Cloudfunktionen und ohne Verknüpfung mit einem Benutzerkonto möglich sein, es sei denn, die Cloudfunktion ist unbedingt für die Erreichung eines therapeutischen Nutzens erforderlich und die Funktion wird von der betroffenen Person ausdrücklich gewünscht.

Die betroffene Person muss hierzu eine entsprechende Auswahlmöglichkeit erhalten (z. B. im Registrierungsprozess) und über etwaige bestehende Vorteile und Risiken, die

[1] EDSA: Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0, angenommen am 07.07.2021, https://edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_de.pdf.

[2] Siehe Beschluss der DSK vom 12.05.2020 zu Google Analytics unter https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_google_analytics.pdf.

mit der Cloudanwendung verbunden sind, informiert werden. Die Daten dürfen im Falle der Entscheidung gegen eine cloudbasierte Verarbeitung allenfalls lokal auf dem Endgerät gespeichert werden.

III. Nutzung personenbezogener Daten zu Forschungszwecken und zur Qualitätssicherung

Für die Nutzung personenbezogener Daten zu Forschungszwecken ist eine datenschutzrechtliche Rechtsgrundlage erforderlich. Hier kommt regelmäßig die ausdrückliche Einwilligung nach Art. 9 Abs. 2 Buchst. a DS-GVO i. V. m. Art. 6 Abs. 1 Buchst. a DS-GVO in Betracht.

Für die Verarbeitung anonymisierter Daten ist keine Rechtsgrundlage erforderlich. Nur Informationen, die sich nicht auf identifizierte oder identifizierbare natürliche Personen beziehen, sind keine personenbezogenen Daten im Sinne von Art. 4 Nr.1 DS-GVO. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind (Erwägungsgrund 26 Satz 3, 4 DS-GVO). Soll eine digitale Gesundheitsanwendung unter Nutzung solch anonymisierter Daten erfolgen, wäre in einer Datenschutz-Folgenabschätzung (DSFA) darzulegen, wie die Anonymisierung durchgeführt wird, und nachzuweisen, dass die Aufhebung des Personenbezugs tatsächlich gewährleistet wird.[3]

Hersteller von Medizinprodukten sind nach der EU-Medizinprodukte-Verordnung 2017/745 (MPV) zur Qualitätssicherung und zum Risikomanagement verpflichtet. Eine Verarbeitung personenbezogener Daten zu Zwecken der danach vorgeschriebenen Qualitätssicherung kann auf Grundlage des Art. 6 Abs. 1 Buchst. c i. V. m. Art. 9 Abs. 2 Buchst. i DS-GVO und § 22 Abs. 1 Nr. 1 Buchst. c BDSG erfolgen.

[3] Derzeit werden vom EDSA Leitlinien zu Anonymisierung erstellt. Nach Veröffentlichung wären diese Leitlinien von den Verantwortlichen bei der Beurteilung der Anonymisierung zu berücksichtigen.

Hierbei ist die Verarbeitung der Daten auf das erforderliche Maß zu beschränken. Es sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen (§ 22 Abs. 2 BDSG). Hierzu gehört beispielweise eine zeitlich begrenzte Speicherung und eine Löschung der zum alleinigen Zweck der Qualitätssicherung verarbeiteten Daten nach Abschluss der durchgeführten Qualitätssicherung.

Die häufig implementierten Mechanismen der Reichweitenanalyse und Software-Fehlerverfolgungsmechanismen, die typischerweise in Software-Entwicklungs-Umgebungen integriert sind und zusammen mit Apps und Webanwendungen ausgeliefert werden, überprüfen das Installationsverhalten und allgemeine Funktionalitätsaspekte der Software (Telemetrie). Diese Datenverarbeitung ist grundsätzlich nicht mit dem Zweck der Anwendung vereinbar.

IV. Betroffenenrechte

Die Hersteller bzw. Betreiber von cloudbasierten Gesundheitsanwendungen müssen Prozesse zur effektiven und unverzüglichen Erfüllung der Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit etablieren.

Da hierbei besonders sensible Gesundheitsdaten betroffen sind, muss zunächst eine sichere Authentifizierung der Antragsteller erfolgen.

V. Sicherheit der Verarbeitung

Weil eine Verarbeitung personenbezogener Daten immer mit Risiken für die davon betroffenen Personen einhergeht, müssen der Verantwortliche und Auftragsverarbeiter durch die wirksame Umsetzung technischer und organisatorischer Maßnahmen (TOM) ein dem Risiko angemessenes Schutzniveau gewährleisten und den Nachweis dafür erbringen können.

Die Verantwortlichen müssen stets prüfen, ob sie eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO durchführen müssen. Dies ist regelmäßig der Fall, wenn eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten gemäß

Art. 9 Abs. 1 DS-GVO vorliegt.[4] Eine Datenschutz-Folgenabschätzung ist vor Aufnahme der Verarbeitungsvorgänge durchzuführen.[5]

Im Einzelfall können beispielsweise (hier nur auszugsweise genannt) folgende TOM dazu beitragen, die gesetzlichen Anforderungen (vgl. Artikel 5, 24, 25, 32 DS-GVO und § 22 Abs. 2 BDSG) zu erfüllen:[6]

- Berücksichtigung von Technischen Richtlinien des BSI zur Informationssicherheit (vgl. folgender Absatz) und Best-Practice-Guidelines zur sicheren Implementierung von Anwendungen (z. B. OWASP[7]);
- sichere Authentifizierungsverfahren (in der Regel Multi-Faktor-Authentifizierung);
- Zugriffskontrolle mit „least privilege policy“ und regelmäßiger Überprüfung von Benutzerkonten und Zugriffsrechten;
- automatische zeitbasierte Sperrung von Benutzeranwendungen (u. a. bei Nichtverwendung oder Verschiebung der Anwendung in den Hintergrund einer Oberfläche);
- wirksame Verschlüsselungsmechanismen, insbesondere bei der Speicherung auf Mobilgeräten;
- Richtlinien und Weisungen an Beschäftigte zur datenschutzrechtlichen Sensibilisierung;
- Protokollierungen von Zugriffen mit anlasslosen Prüfungen;

[4] Zur Prüfung, ob eine Datenschutz-Folgenabschätzung erforderlich ist, siehe die „Leitlinien zur Datenschutz-Folgenabschätzung …“ (WP 248 Rev. 01) der Artikel-29-Arbeitsgruppe (https://www.datenschutzkonferenz-online.de/media/wp/20171004_wp248_rev01.pdf). Sie wurden vom EDSA bestätigt.

[5] Siehe hierzu die Kurzpapiere der DSK Nr. 18 „Risiko für die Rechte und Freiheiten natürlicher Personen“ (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf) und Nr. 5 „Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO“ (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf).

[6] Zu weiteren technischen und organisatorischen Maßnahmen siehe das Standard-Datenschutzmodell Version 3.0, dort insbesondere Abschnitt „D1 Generische Maßnahmen“ (https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/).

[7] Open Web Application Security Project (OWASP), https://owasp.org/; dort beispielsweise „OWASP Mobile Application Security”, https://owasp.org/www-project-mobile-app-security/.

- Schaffung einer Redundanz von Infrastrukturkomponenten und Hintergrundsystemen bei technischen Betreibern;
- Überprüfung von Sicherheitsmaßnahmen in Anwendungsprogrammen und Hintergrundsystemen durch Sicherheits- und Penetrationstests.

Auch sollte die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte Technische Richtlinie (TR) „Sicherheitsanforderungen an digitale Gesundheitsanwendungen“ (BSI TR-03161)[8] für alle mobilen Anwendungen, die sensible Daten verarbeiten und speichern, herangezogen werden. Grundsätzlich fordert das BSI, Sicherheitsanforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit von Anfang an bei der Software-Entwicklung mit zu betrachten. Diese Technische Richtlinie soll als Leitfaden dienen, um Entwickler von Anwendungen bei der Erstellung sicherer Lösungen zu unterstützen. Sie gliedert sich in drei Teile:

- BSI TR-03161 Anforderungen an Anwendungen im Gesundheitswesen – Teil 1: Mobile Anwendungen
- BSI TR-03161 Anforderungen an Anwendungen im Gesundheitswesen – Teil 2: Web-Anwendungen
- BSI TR-03161 Anforderungen an Anwendungen im Gesundheitswesen – Teil 3: Hintergrundsysteme

Die getroffenen technischen und organisatorischen Maßnahmen sind gemäß Art. 5 Abs. 2 i. V. m. Art. 32 Abs. 1 Buchst. d DS-GVO regelmäßig und anlassbezogen zu überprüfen, zu bewerten sowie zu evaluieren.

VI. Internationaler Datentransfer

Bei Datenübermittlungen an Verantwortliche und Auftragsverarbeiter in Drittländern sind die Maßgaben des Kapitel V der DS-GVO zu berücksichtigen. Falls eine Übermittlung auf Grundlage des Art. 46 DS-GVO erfolgt, müssen zusätzliche Maßnahmen ergriffen werden, die geeignet sind, bei dieser Übermittlung ein Schutzniveau herzustellen, das mit dem bei einer Verarbeitung innerhalb der EU/des EWR vergleichbar ist. Die

[8] BSI: BSI veröffentlicht Sicherheitsanforderungen für Gesundheits-Apps, Pressemitteilung vom 15.04.2020, https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/TR-Gesundheitsapps_150420.html.

entsprechenden Anforderungen an solche Maßnahmen sind in den EDSA-Empfehlungen 01/2020[9] und 02/2020[10] konkretisiert.

Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten, die nach Art. 28 DS-GVO im Auftrag innerhalb der EU/des EWR verarbeitet werden, ist der Beschluss der DSK vom 31.01.2023[11] zu beachten.

[9] EDSA: Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0, angenommen am 18.06.2021, https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_de.pdf.

[10] EDSA: Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, angenommen am 10.11.2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_de.pdf.

[11] DSK: Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten, Beschluss vom 31.01.2023, https://www.datenschutzkonferenz-online.de/media/dskb/20230206_DSK_Beschluss_Extraterritoriale_Zugriffe.pdf.