Bundesgesundheitsbl 2021 · 64:1254–1261
https://doi.org/10.1007/s00103-021-03412-y
Eingegangen: 19. April 2021
Angenommen: 20. August 2021
Online publiziert: 15. September 2021

André Zilch · Martin Tschirsich
ZFT.COMPANY GmbH, Eppstein, Deutschland

Datenschutz und Informationssicherheit bei digitalen Gesundheitsanwendungen (DiGA)

Einleitung

Mut zur Lücke beim Thema Datenschutz und Sicherheit? Ganz im Gegenteil. Die Erfahrung aus einem knappen Jahr digitale Gesundheitsanwendungen (DiGA) zeigt, dass sich nahezu alle Hersteller der Bedeutung sicherer und datenschutzkonformer Apps auf Rezept bewusst sind und mit der gebotenen Sensibilität vorgehen. Und das hat neben dem Schutz der Anwender vor Datenmissbrauch viele weitere gute Gründe. So genießt das Thema insbesondere bei den Ärzten, die die Apps letztendlich verschreiben, einen hohen Stellenwert. Zudem trägt der Hersteller eine wichtige Gesamtverantwortung für den Erfolg der DiGA an sich, wie sie der Spitzenverband der gesetzlichen Krankenversicherung (GKV) treffend beschreibt: „Bei DiGA steht und fällt mit dem Datenschutz und der Datensicherheit die Reputation und somit auch die Erfolgswahrscheinlichkeit der neuen Leistungskategorie der DiGA“ [1].

Wie schnell die Reputation verspielt ist, hat zuletzt wieder einmal ein Hackerangriff gezeigt, ausgerechnet in Finnland, einem Land, das weltweit als E-Health-Vorreiter gilt. So wurde Ende 2020 bekannt, dass Angreifer Zugriff auf über 40.000 digitale Patientenakten des Psychotherapieanbieters Vastaamo genommen hatten, von denen mittlerweile mehr als 30.000 frei im Internet für jeden verfügbar sind [2]. Der Schaden für die Betroffenen ist immens, sind doch auch die einzelnen Aufzeichnungen zugänglich, die innerhalb der Sitzungen durch die Therapeuten erstellt wurden. Der Schaden für das betroffene Unternehmen war so groß, dass Vastaamo mittlerweile seinen Betrieb wegen Insolvenz eingestellt hat.

Trotz der unstrittig hohen Bedeutung und der mahnenden Negativbeispiele ist in der Praxis ein riskantes Auseinanderklaffen von Anspruch und Wirklichkeit in Sachen Datenschutz und Informationssicherheit zu beobachten, aller Beteuerungen zum Trotz. Dabei ist festzustellen, dass nicht nur Fehler in der Umsetzung auftreten, sondern auch schon zuvor bei der Anforderungsanalyse und im Prozessdesign systematisch Fehler gemacht werden.

Doch was sind die Ursachen für diese Diskrepanz? Ein Blick auf die im DiGA-Verzeichnis des Bundesinstituts für Arzneimittel und Medizinprodukte (BfArM) vertretenen Hersteller offenbart überwiegend Unternehmen mit einem geringen Reifegrad in der Organisation von Anwendungsentwicklung. Diese Unternehmen sind zum großen Teil sehr jung oder wenig erfahren in der Entwicklung von Anwendungen mit hohem oder sehr hohem Schutzbedarf.

Einige Hersteller haben diesen Bedarf aber erkannt und haben, sofern nicht auf internes Fachpersonal zurückgegriffen werden konnte, externe Expertise eingekauft. Doch auch bei der Wahl des Dienstleisters zeigt sich Verbesserungspotenzial. Ein zu technischer Fokus deckt die bestehenden Fehler bei Anforderungsanalyse und Prozessdesign nicht auf. Unternehmen, die Zertifizierungen unter Berücksichtigung der Datenschutz-Grundverordnung (DSGVO) oder im Rahmen der für DiGA-Hersteller bisher angewendeten Medizinprodukterichtlinie (MDD) anbieten, richten ihr Hauptaugenmerk auf die Anforderungen der MDD oder der DSGVO, nicht aber auf die darüber hinausgehenden Anforderungen der Digitale-Gesundheitsanwendungen-Verordnung (DiGAV). Im Ergebnis wenden DiGA-Hersteller viel Kapital und Ressourcen auf, ohne das geforderte Informationssicherheits- und Datenschutzniveau zu erreichen, und gehen damit ungewollt hohe Risiken ein.

Ganz im Sinne eines *How-to* wollen wir daher zeigen, wo wir als Experten für Informationssicherheit Nachholbedarf sehen. Ebenso wie DiGA-Hersteller schon bei der Planung die Anforderungen der MDD berücksichtigen müssen, so müssen auch Informationssicherheit und Datenschutz nach DiGAV von Anfang an mit geplant werden. Da deren Einhaltung zum Teil erheblich in die Gestaltung von Geschäftsprozessen eingreift, können diese Anforderungen nicht erst nachträglich betrachtet werden.

Nachfolgend geben wir zunächst den gesetzlichen Rahmen wieder, leiten beispielhaft konkrete Anforderungen ab und schließen mit einem *How-to* für Hersteller, um so die häufigsten Informationssicherheits- und Datenschutzmängel direkt zu adressieren.

Gesetzlicher Rahmen

Während die Herleitung der Datenschutzanforderungen an eine DiGA noch relativ nachvollziehbar auf Grund-

lage der Datenschutzgesetzgebung wie der DSGVO erfolgt, blieb zumindest bis zum Inkrafttreten der Medizinprodukteverordnung (MDR) im Jahr 2017 die Suche nach dem Begriff Informationssicherheit in den gängigen Gesetzbüchern mit Bezug zu digitalen Gesundheitsanwendungen ergebnislos.

Begriffserklärung. Zielführend ist zunächst eine Begriffsklärung. So fordert die DSGVO die Sicherheit der Verarbeitung während das Digitale-Versorgung-Gesetz (DVG) nach Datensicherheit verlangt. In der Praxis wird dagegen oft auf die IT-Sicherheit abgezielt. Doch die Begriffe sind nicht synonym und ein falsches Verständnis häufig die Ursache von kritischen Auslassungen im Gesamtprozess einer DiGA. So zielt die Informationssicherheit übergeordnet auf den Schutz sämtlicher Informationswerte und betrachtet Daten sowie Prozesse sowohl analog als auch digital [3]. Daten- und IT-Sicherheit beleuchten die jeweiligen Teilaspekte.

Grundlegende Regelungen. Übergeordneter rechtlicher Rahmen für die Verarbeitung personenbezogener Daten ist nicht das DVG und auch nicht die DiGAV, welche „nur ein Instrument … beim BfArM ist" [4], sondern die DSGVO und das Bundesdatenschutzgesetz (BDSG). Gefordert werden ganz allgemein dem Risiko angemessene technische und organisatorische Maßnahmen unter Berücksichtigung von *Stand der Technik*, Implementierungskosten und vieler weiterer Faktoren. Die Trennlinie zwischen gerade noch angemessenen und regelwidrigen Maßnahmen ist aufgrund dieser vielen Freiheitsgrade oft unscharf. Als untere Grenze gelten jedoch die *anerkannten Regeln der Technik*, welche in nationalen oder internationalen Standards und Normen festgeschrieben sind [5]. Zu berücksichtigen ist, dass sowohl *Stand der Technik* sowie die *anerkannten Regeln der Technik* keinesfalls nur rein technische Aspekte, sondern gerade auch organisatorische Maßnahmen umfassen.

Standards und Normen. Ebenfalls zu berücksichtigen ist, dass sich viele der bekannten Standards auf Unternehmen beziehen und nicht auf ein Produkt wie eine DiGA selbst. Am Bekanntesten darunter sind die Werke der ISO/IEC-27000-Reihe [6] oder auch der IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik (BSI), welche das Management der Informationssicherheit anhand strukturierter Vorgaben zur Aufbau- und Ablauforganisation im Unternehmen beschreiben. Der Fokus liegt dabei auf der innerbetrieblichen Datenverarbeitung und internen Anwendern. Weitere Richtlinien, darunter die VdS-Richtlinie 10000 [7] und ISIS12 [8], zielen noch mehr als schon der BSI-Grundschutz auf die IT-Sicherheit als Untermenge eines ganzheitlichen prozessorientierten Informationssicherheitsmanagements ab. Die vorgenannten Richtlinien sollen den Anwendern zwar als Hilfestellung dienen, weisen jedoch neben den zuvor genannten Schwachpunkten auch keine Verbindlichkeit auf. Das Informationssicherheitsmanagement eines DiGA-Herstellers sollte sich daher nicht allein auf diese Richtlinien stützen. Zur Erfüllung der Anforderungen an das Produkt DiGA selbst mit seinen vielfältigen Prozessen zwischen internen und externen Akteuren empfiehlt es sich, zunächst ein Sicherheitskonzept ausgehend von der nach DiGAV vorgeschriebenen Schutzbedarfsanalyse mit eigener Risikobewertung z. B. nach BSI-Standard 200-3 auszuarbeiten. Relevant sind dabei fast immer die weniger bekannten Standards zum Identitätsmanagement (IdM). Die Berücksichtigung des Stands der Technik nach der DSGVO [5] verlangt von den Verantwortlichen u. a. die Beschäftigung mit den Regelwerken ISO/IEC 24760 1–3 („A framework for identity management"), ISO/IEC 29115 („Entity authentication assurance framework") oder ISO/IEC 29003 („Identity proofing").

Die Medizinprodukterichtlinie (Medical Device Directive [MDD]). Der Bestimmung der Datenschutz- und Sicherheitsanforderungen an ein Medizinprodukt wird nach Erfahrung der Autoren von einzelnen Herstellern die Risikoeinstufung nach der inzwischen veralteten MDD zugrunde gelegt. Doch selbst DiGA, die nach MDD der Risikoklasse 1 zuzuordnen waren, erfordern aufgrund der Verarbeitung von Gesundheitsdaten, die nach Artikel 9 DSGVO besonderen Kategorien personenbezogener Daten zuzuordnen sind, einen erheblichen Aufwand im Bereich der Informationssicherheit, um den o. g. Anforderungen zu genügen.

In Summe ergeben sich zahlreiche Abhängigkeiten über die verschiedenen Regelwerke hinweg, die zu einer massiven Komplexitätserhöhung im Bereich der Informationssicherheit führen.

Ableitung konkreter Anforderungen

Schutzbedarf der DiGA bestimmen

Zunächst gilt es, den Schutzbedarf einer DiGA in Bezug auf die Grundwerte der Informationssicherheit wie Vertraulichkeit, Integrität und Verfügbarkeit in den Kategorien *normal, hoch* oder *sehr hoch* zu bestimmen. Da DiGA generell Gesundheitsdaten verarbeiten, muss von einem mindestens *hohen* Schutzbedarf ausgegangen werden. Dies leitet sich aus Artikel 4 Nr. 15 und Artikel 9 DSGVO und der Ermittlung der Schutzbedarfskategorie beispielsweise nach Roßnagel et al. ab [9]. Häufig ist allein „die Information, dass eine DiGA verwendet wird, schon aus sich heraus eine Gesundheitsinformation" [10]. Werden durch DiGA Informationen verarbeitet, „deren Bekanntwerden der betroffenen Person in besonderem Maße unangenehm sind oder zu einer gesellschaftlichen [Stigmatisierung] der betroffenen Person führen können", wie beispielsweise bei einer Offenbarung psychotherapeutischer Informationen analog zum Fall von Vastaamo, so ist der Schutzbedarf nach Roßnagel et al. *sehr hoch* [11].

Nachdem die Schutzbedarfskategorie einer DiGA bestimmt wurde, sind im nächsten Schritt die konkreten Anforderungen auf Stand der Technik an Prozesse und technische Lösungen für Registrierung, Authentisierung und Einwilligung der Endnutzer abzuleiten. Dazu müssen zunächst die entsprechenden Definitionen von Schutzbedarfskategorie, Ver-

Bundesgesundheitsbl 2021 · 64:1254–1261 https://doi.org/10.1007/s00103-021-03412-y

A. Zilch · M. Tschirsich

Datenschutz und Informationssicherheit bei digitalen Gesundheitsanwendungen (DiGA)

Zusammenfassung

Die Gewähr von Datenschutz- und Informationssicherheit stellt Hersteller digitaler Gesundheitsanwendungen (DiGA) regelmäßig vor Schwierigkeiten. Ursächlich sind häufig ein geringer Reifegrad in der Organisation der Anwendungsentwicklung und fehlende Expertise an der Schnittstelle zwischen regulatorischen Vorgaben und angewandter Informationssicherheit. Im Ergebnis werden sowohl in der Umsetzung als auch bei der Anforderungsanalyse und im Prozessdesign kritische Fehler gemacht, die es zu vermeiden gilt.

Vorliegend werden Anforderungen und Lösungswege aufgezeigt, die sich aus der Datenschutz-Grundverordnung (DSGVO), dem Stand der Technik, anderen zu berücksichtigenden Vorschriften sowie dem Digitale-Versorgung-Gesetz (DVG) und der entsprechenden Verordnung ergeben. Zur Herleitung konkreter Anforderungen nach Stand der Technik und unter Berücksichtigung des ermittelten Schutzbedarfs in Bezug auf die Schutzziele der Informationssicherheit wie Vertraulichkeit, Integrität und Verfügbarkeit wird auf wichtige Standards und Normen verwiesen. Im Sinne eines *How-to* für Hersteller adressieren die Autoren anschließend direkt die wichtigsten Mängel aus den Bereichen Authentisierung, Einwilligung und Autorisierung und geben entsprechende Empfehlungen.

Eine wichtige Brücke zur Überwindung der aufgezeigten Kluft zwischen Anspruch und Wirklichkeit in Sachen Datenschutz und Informationssicherheit sehen die Autoren in der weiteren Unterstützung der Hersteller durch das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM), beispielsweise in Form von Handreichungen. Gleichzeitig ist auch von Herstellern eine weitere Reifung der Anwendungsentwicklungsorganisation zu erwarten. Auch nimmt die Informationssicherheit mit der Ablösung der Medizinprodukterichtlinie (MDD) durch die Medizinprodukteverordnung (MDR) eine bedeutendere Stellung ein.

Schlüsselwörter

Schutzbedarf · Anforderungen · Mängel · Empfehlungen · How-to

Data protection and information security of digital health applications (DiGA)

Abstract

Ensuring data privacy and information security frequently poses a challenge for manufacturers of digital health applications (DiGA). This is often caused by a low level of maturity of the application development organization and a lack of expertise in the intersection between regulatory requirements and applied information security. As a result, critical mistakes are made during implementation, requirement analysis, and process design. These must be avoided.

This paper presents the requirements and solutions derived from and in compliance with the General Data Protection Regulation, the state of the art, other regulations that must be taken into account, the Digital Healthcare Act (DVG), and the corresponding ordinance. In order to derive specific requirements according to the state of the art and considering the identified level of protection with regard to the fundamental objectives of information security, such as confidentiality, integrity and availability, reference is made to important standards and norms. In the spirit of a *how-to* for manufacturers, the authors then directly address the most important deficiencies regarding authentication, consent, and authorization and give appropriate recommendations.

The authors see further support for manufacturers from the Federal Institute for Drugs and Medical Devices (BfArM), for example in the form of specific guidelines, as an important pillar in overcoming the gap between requirements and reality in matters of data protection and information security. At the same time, further maturation of the manufacturer's application development organization is required and expected. At the same time, with the replacement of the Medical Device Directive (MDD) with the Medical Device Regulation (MDR), information security gains more importance.

Keywords

Protection needs · Requirements · Deficiencies · Recommendations · How-to

trauensniveau der Prozesse und Level of Assurance (Maß an Gewissheit) der unterschiedlichen Standards wie in **Tab. 1** dargestellt miteinander abgeglichen werden.

Authentisierungsmittel und datenschutzrechtliche Einwilligungserklärung

Aus **Tab. 1** können zugleich Anforderungen zur Auswahl der Authentisierungsmittel individuell abgeleitet werden. So ist nach den Vorgaben der ISO/IEC 29115 [12] und der BSI TR-03107-1 [13] ab einer Schutzbedarfskategorie *hoch* ein zweiter Authentisierungsfaktor (2FA) vorzusehen und nicht erst für die Kategorie *sehr hoch*. Beide Werke sind bei der Berücksichtigung des Stands der Technik nach der DSGVO [5] und insbesondere der DiGAV zu beachten, wobei Letztere zudem auf eine Abwägung bezüglich der Implementierungskosten verzichtet. Auf die BSI TR-03107-1 verweist auch der Leitfaden des BfArM in seiner nichtabschließenden Aufzählung.

Auch wenn der Titel der BSI TR-03107-1 „Elektronische Identitäten und Vertrauensdienste im E-Government" lautet, wird bereits in der Einleitung der technischen Richtlinie (TR) darauf verwiesen, dass die Kriterien und Zuordnungen weitgehend unabhängig davon sind, ob die Verfahren für E-Government oder E-Business eingesetzt werden. Bei der Bewertung rechtlicher Vorgaben können sich Unterschiede ergeben. Im Falle von DiGA stellt der Schutzbedarf der zu schützenden Daten die wesentliche Kenngröße zur Auswahl geeigneter

Tab. 1 Vergleich der Definitionen von Schutzbedarfskategorien, Vertrauensniveau der Prozesse und Level of Assurance (Maß an Gewissheit) nach unterschiedlichen Standards

BSI-Grundschutz Schutzbedarfskategorie BSI 200-2	Vertrauensniveau BSI TR-03107	Level of Assurance (LoA) ISO/IEC 29115	Definition	eIDAS Vertrauensniveau EU 2015/1502	Definition
–	–	Low (LoA 1)	Little or no confidence in the asserted identity. This LoA is used when minimum risk is associated with erroneous authentication	–	–
Normal	Normal	Medium (LoA 2)	Some confidence in the asserted identity. This LoA is used when *moderate risk* is associated with *erroneous authentication*. *Single-factor authentication is acceptable*	Niedrig	Es kann davon ausgegangen werden, dass die Person im Besitz eines Beweismittels ist, das von dem Mitgliedstaat, in dem das elektronische Identifizierungsmittel beantragt wird, anerkannt wird und die beanspruchte Identität repräsentiert
Hoch	Substanziell	High (LoA 3)	High confidence in the asserted identity. This LoA is used where *substantial risk* is associated with *erroneous authentication*. *This LoA shall*[a] *employ multi-factor authentication*	Substanziell	Es ist überprüft worden, dass die Person im Besitz eines Beweismittels ist, das von dem Mitgliedstaat, in dem das elektronische Identifizierungsmittel beantragt wird, anerkannt wird und die beanspruchte Identität repräsentiert, …
Sehr hoch	Hoch	Very high (LoA 4)	Very high confidence in the asserted identity. *This LoA is used when a high risk is associated* with *erroneous authentication*. LoA 4 provides the highest level of entity authentication assurance defined by this Recommendation/Standard	Hoch	Ist überprüft worden, dass die Person im Besitz eines mit Foto oder biometrischen Merkmalen versehenen Identitätsnachweises ist, der von dem Mitgliedstaat, in dem das elektronische Identifizierungsmittel beantragt wird, anerkannt wird, und dass der Identitätsnachweis die beanspruchte Identität repräsentiert, so wird das Beweismittel geprüft, um festzustellen, ob es laut einer verlässlichen Quelle gültig ist, …

[a] „Shall" indicates a requirement

Verfahren dar. Eine 2FA ist hiernach auch Voraussetzung einer DSGVO-konformen Einwilligung in die Datenverarbeitung. Demgegenüber kann eine Einwilligung, die mittels Nutzerinteraktion wie dem Anklicken eines Kästchens durch einen Nutzer erteilt wird, der sich zuvor nur anhand Benutzername und Passwort authentisiert hat, lediglich ein *normales* und kein *hohes* Vertrauensniveau erreichen [14]. Auch der in Artikel 7 Nr. 1 DSGVO geforderte Nachweis, „dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat", scheitert für den elektronischen Fall einer Einwilligungserklärung regelmäßig ohne Nutzung einer 2FA.

DSGVO-Betroffenenrechte und Support

Eine weitere Anforderung, deren Nichtbeachtung rasch zu massiven Defiziten in der Informationssicherheit führt, ist die sichere Umsetzung der Prozesse zur Ausübung der Betroffenenrechte nach DSGVO. Wurden Betroffene zuvor nicht entsprechend der Schutzbedarfskategorie sicher registriert, können deren Identitäten nicht mit denen der rechteausübenden Personen abgeglichen werden und es darf z. B. keine Auskunft nach Artikel 15 DSGVO erteilt werden. Dies gilt für alle möglichen Kommunikationskanäle, sei es per E-Mail, Telefon, schriftlich oder gar persönlich.

Aber auch innerbetrieblich gibt es für DiGA-Anbieter, z. B. in Hinblick auf den Produktsupport, wichtige Punkte zu beachten. Ebenso wie für Endkunden sind auch für interne Mitarbeiter, die im Rahmen ihrer Tätigkeiten Zugriffe auf gespeicherte Informationen haben oder im Informationsaustausch mit Endkunden stehen, die Anforderungen der Informationssicherheit umzusetzen. Aus der Schutzbedarfskategorie ergeben sich die Anforderungen an die Registrierung und Authentisierung von Mitarbeitern gegenüber der Anwendung, aber auch gerade die gegenseitige Authentisierung im Kontakt mit Endkunden: Woher weiß der Supportmitarbeiter, dass es sich um den „richtigen" Kunden handelt, und

woher weiß der Kunde, dass es sich um den richtigen „Supportmitarbeiter" handelt? Hierbei sind sowohl organisatorische als auch technische Aspekte zu berücksichtigen.

Hinweise aus der Praxis

Sind die in Summe zahlreichen Anforderungen an eine DiGA hergeleitet, stellt sich die Frage nach deren Umsetzung und Kontrolle. In der täglichen Praxis beobachten die Autoren hierbei eine Häufung von ganz konkreten Mängeln am Produkt. Im Sinne eines *How-to* sind nachfolgend die am häufigsten beobachteten Datenschutz- und Informationssicherheitsmängel sowie Abhilfemaßnahmen aufgeführt.

Problemfeld Authentisierung

An erster Stelle der am häufigsten identifizierten Sicherheitsmängel – zudem mit dem höchsten Risiko für Betroffene und Betreiber – steht ganz eindeutig die Authentisierung der verschiedenen Akteure rund um die App. Im Einzelnen sind zu nennen:

Unzureichendes Vertrauensniveau. Wie im vorherigen Kapitel dargelegt, ist eine Authentisierung mittels Benutzername und Passwort unter Berücksichtigung des Stands der Technik in der DSGVO [5] ohne zweiten Authentisierungsfaktor nicht ausreichend.

Unsichere Account-Wiederherstellung. Aus der Wahl ungenügender Authentisierungsmittel ergibt sich die unsichere Account-Wiederherstellung als Folgefehler im Prozedere für den Fall vergessener Zugangangsdaten, wie etwa Passwörter. Häufig werden Einmalpasswörter (Reset-Token) per SMS oder E-Mail an das Postfach des Nutzers versandt. Neben der Problematik des unsicheren Übertragungskanals werden hierbei oft handwerkliche Fehler gemacht. Eine zu geringe Entropie (Informationsgehalt) des Tokens und ein fehlender Schutz vor Zugriffen durch systematisches Ausprobieren von Passwörtern (Online-Brute-Force-Angriff) bieten eine einfache Gelegenheit zur Account-Übernahme. Der offene Branchenverband FIDO-Allianz (Fast IDentity Online) sieht zur Lösung dieses Problems zwei generelle Ansätze [15]: erstens eine Reidentifizierung des Nutzers und zweitens die Vergabe von zusätzlichen Authentisierungsmitteln.

Schlupfloch DSGVO-Betroffenenrechte. Jede Datenschutzerklärung beinhaltet einen Passus, der Nutzer über ihre Rechte bzgl. Auskunftsersuchens über die verarbeiteten personenbezogenen Daten informiert. In fast allen Fällen beantworten DiGA-Betreiber derartige Auskunftsersuchen per E-Mail oder gar telefonisch. Aus zwei Gründen ist dies brandgefährlich: Zum einen ist die E-Mail ein unsicherer Kommunikationskanal und zum anderen lässt sich überhaupt nicht prüfen, ob die um Auskunft ersuchende Person tatsächlich auch die betroffene Person ist, die sie zu sein behauptet. Die oft geforderte Vorlage eines Ausweisdokumentes führt nur dann zum Erfolg, wenn die Nutzerregistrierung der DiGA ebenfalls eine Identitätsfeststellung beinhaltet.

Unsicherere E-Mail. Der geläufigste Kommunikationskanal zum Nutzer ist die E-Mail, auch bei DiGA. Sei es zur Bestätigung der Registrierung, zum Versand von Zugangsdaten wie Passwort-Reset-Token oder zum Export von Gesundheitsdaten. Was dabei nicht beachtet wird: Sowohl die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (kurz: Datenschutzkonferenz, DSK) als auch jüngst das Verwaltungsgericht Mainz gehen von „dem Erfordernis einer Ende-zu-Ende-Verschlüsselung oder einer qualifizierten Transportverschlüsselung" [16] für Daten nach Art. 9 DSGVO aus, für die „in jedem Fall besondere Schutzmaßnahmen zu ergreifen sind, da insoweit schon aufgrund der allgemeinen datenschutzrechtlichen Wertung stets von einem hohen Risiko ausgegangen werden muss" [17]. Enthält – wie im vorherigen Abschnitt dargelegt – bereits die Information, dass eine DiGA verwendet wird, eine Gesundheitsinformation, so stellt der E-Mail-Versand in den vorgenannten Fällen einen Verstoß gegen datenschutzrechtliche Vorgaben dar und ist ein Risikospiel mit der Datenschutzaufsicht. Neben den Nutzern sind aber auch die Mitarbeiter der DiGA-Hersteller und Betreiber selbst gefährdet. Nicht von ungefähr ist die E-Mail das bei Angreifern beliebteste Einfallstor in Unternehmensnetze.

Öffentlich erreichbare Administration. Unstrittig ist auch der gegenüber einem einfachen Nutzer einer DiGA nochmals gestiegene Schutzbedarf von administrativen Zugängen, über welche die eigenen Mitarbeiter auf die medizinischen Inhalte sowie Nutzerdaten zugreifen können. Dazu gehören Webportale oder privilegierte Programmierschnittstellen sowohl auf eigener Infrastruktur als auch betrieben durch Auftragsverarbeiter. Die DiGAV fordert daher konsequent, „dass Zugriffe auf Funktionen und Daten der digitalen Gesundheitsanwendung durch Betriebspersonal des Herstellers nur über sichere Netze und Zugangspunkte möglich sind". In der Praxis bleibt diese Forderung häufig unbeachtet.

Angesichts der Vielzahl an Mängeln rund um das Thema Authentisierung ist die Frage nach den Ursachen berechtigt. Eine wichtige Rolle spielt dabei sicher die fehlende Verfügbarkeit allgemeiner elektronischer Identitäten und entsprechender Infrastruktur. Die elektronische Gesundheitskarte scheidet aufgrund bekannter Mängel als Identitätsnachweis aus [18], die eID (der elektronische Identitätsnachweis des Personalausweises) ist nicht geläufig genug und derzeitige Überlegungen zur Einführung gänzlich neuer elektronischer Identitäten im Gesundheitswesen können frühestens in einigen Jahren Früchte tragen. Daher sind die Hersteller angewiesen, eigene Ansätze zu entwickeln.

Problemfeld datenschutzrechtliche Einwilligung

Nicht auf äußere Umstände zurückführbar ist dagegen eine ganze Reihe von regelmäßig anzutreffenden Mängeln im Zusammenhang mit der datenschutzrechtlichen Einwilligung. Im Einzelnen sind hier zu nennen:

Unzureichendes Vertrauensniveau und fehlender Nachweis der Einwilligung. DiGA-Betreiber müssen nach Art. 7 Abs. 1 DSGVO „im Einzelfall den Nachweis der tatsächlich erteilten Einwilligung" erbringen können [19]. Erteilt der Nutzer die Einwilligung elektronisch, ohne dabei auf ausreichendem Vertrauensniveau authentifiziert worden zu sein, ist das Sicherheitsziel der *Nichtabstreitbarkeit* verletzt und der Nachweis nicht zu erbringen. Für weitere umzusetzende Anforderungen bei Abgabe einer Willenserklärung auf hohem oder sehr hohem Vertrauensniveau, darunter die sog. Warnfunktion, wird auf die auch im DiGA-Leitfaden referenzierte technische Richtlinie des BSI TR-03107-1 verwiesen.

Unzulässiger Verarbeitungszweck. Eine Einwilligung darf „nur für die in § 4 Absatz 2 Satz 1 der DiGAV genannten Zwecke" eingeholt werden, eine entsprechende Abfrage „für den Empfang eines Newsletters" oder zu Werbezwecken scheidet damit grundsätzlich aus [20]. Wer dennoch Newsletter versenden oder anderweitig Daten zu Werbezwecken verarbeiten möchte, kann eine Einwilligung hierzu außerhalb der Grenzen der DiGA einholen.

Kopplung der Einwilligungen. Für Hersteller sind Daten zur „dauerhaften Gewährleistung der technischen Funktionsfähigkeit, der Nutzerfreundlichkeit und der Weiterentwicklung" der DiGA unabdingbar. Verständlich ist also der Wunsch, eine Einwilligung hierzu einzuholen. Doch die DiGA „muss auch ohne eine Einwilligung nach Nummer 4 [Anm.: § 4 Absatz 2 Nummer 4 DiGAV] nutzbar sein. Eine Koppelung an die anderen Einwilligungen oder gar eine vollständige Nicht-Nutzbarkeit der DiGA ohne eine Einwilligung nach Nummer 4 wäre unzulässig" [21].

Umfassendes Tracking. Auch mit freiwillig erteilter Einwilligung zur Weiterentwicklung der DiGA bleibt ein umfassendes Tracking untersagt. Das gilt auch dann, wenn die Daten ausschließlich durch den DiGA-Betreiber und nicht durch Dritte verarbeitet werden. Nur „fehlerspezifische Datenerfassung und Reportings" sind erlaubt [21]. Unproblematisch ist demnach der Betrieb eines Fehlertrackers wie *Sentry* auf eigener Infrastruktur. Wichtig ist aber, das Tracking auch wirklich erst nach erteilter Einwilligung zu aktivieren.

Ungenaue Datenschutzerklärung. Teils wird in DiGA-Datenschutzerklärungen auf ein berechtigtes Interesse des Verantwortlichen nach Art. 6 Abs. 1 lit. f) DSGVO verwiesen, beispielsweise zur Gewährleistung der Funktionsfähigkeit und des fehlerfreien Betriebs, obgleich nach § 4 Abs. 2 DiGAV nur eine Einwilligung Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen einer DiGA sein kann. Des Weiteren ist die Liste der Auftragsverarbeiter häufig unvollständig oder nicht aktuell. Auch eine Bezugnahme auf das bereits seit 2020 durch den EuGH gekippte Privacy Shield oder unzulässige Standardvertragsklauseln sind oft noch im Erklärungstext anzutreffen. Die Erklärung sollte daher regelmäßig auf Aktualität geprüft werden.

Verarbeitung im Drittland ohne Angemessenheitsbeschluss. „DiGA-Hersteller und deren Auftragsverarbeitende dürfen keine personenbezogenen Daten in den USA verarbeiten" [22]. Selbst die Verarbeitung in europäischen Rechenzentren der großen US-Cloud-Anbieter wie Amazon oder Microsoft ist nur unter Auflagen zulässig [23]. Dennoch scheint es bislang nahezu keinem Hersteller gelungen zu sein, gänzlich auf eine rechtswidrige Weitergabe personenbezogener Daten zu verzichten. Sei es der E-Mail-Versender, der im Auftrag wiederum bei einem US-Cloud-Anbieter verarbeiten lässt, oder die eingebundene externe Schriftart von Google. Hier empfiehlt es sich, die Verträglichkeit sämtlicher Auftragsverarbeitungsverträge auf Konformität mit DiGAV sowie die Datenverbindungen der eigenen Anwendung zu überwachen, beispielsweise mittels gängiger Werkzeuge zum Protokollieren ausgehender Datenpakete (Packet Capture Tools).

Ursächlich für die vorgenannten Mängel ist häufig ein Verlust an Übersicht über die Vielzahl der zu beachtenden Anforderungen, die über die bekannten Anforderungen nach DSGVO und MDD hinausgehen, sowie eine fehlende Kontrolle der Umsetzung. Diese erfolgt am besten auf dem Prüfstand, beispielsweise innerhalb eines Sicherheitstests (Pentest), wobei die Sicherheitsanalysten keinesfalls „wie immer" vorgehen und gerade in Bezug auf die speziellen Anforderungen der DiGAV auf dem neuesten Stand sein sollten.

Weitere Mängel

Weiterhin scheinen auch DiGA vielfach nicht gefeit vor Sicherheitsmängeln, wie sie auch in der bekannten Top-10-Liste des gemeinnützigen „Open Web Application Security Project" (OWASP) zu finden sind [24]. Darunter sind auffallend häufig kritische Mängel in der Autorisierungskomponente anzutreffen, beispielsweise die sog. Insecure Direct Object References. Auch die ungewollte Offenlegung der Existenz von Nutzerkonten anhand von E-Mail-Adressen oder mittels *Browsable Intent* unter Android ist eher der Regelfall als die Ausnahme. Ein solcher Verstoß scheint harmlos, doch handelt es sich auch hierbei meist um unbefugtes Offenbaren von Gesundheitsdaten.

In Summe ist zu konstatieren, dass eine externe sicherheitsanalytische Betrachtung in der Mehrzahl der Fälle neben Rechtsverstößen auch kritische Sicherheitsmängel aufdeckt, deren Ausnutzung einem Angreifer über das Internet und ohne Benutzerinteraktion vollständigen Zugang zu Nutzerkonten und den darin gespeicherten Gesundheitsdaten ermöglicht hätten.

Fazit

- Wie aufgezeigt sind die Anforderungen an Datenschutz und Informationssicherheit an digitale Gesundheitsanwendungen (DiGA) umfangreich. Es gilt, den noch vorhandenen Abstand zwischen Anspruch und Wirklichkeit zu überwinden.
- Vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) wurden hierzu bereits die oben aufgezeigten Erfahrungen aufgenommen

und sinnvolle Verbesserungen im Antragsprozess umgesetzt. Ziel muss es auch weiterhin sein, die Einhaltung der vorgeschriebenen Mindeststandards zu forcieren. Blinde Flecken im Antragsprozess dagegen führen in einen Unterbietungswettbewerb hin zur „DiGA auf Lücke". Die eingangs angeführte gemeinschaftliche Verantwortung für die neue Leistungskategorie DiGA würde damit unterlaufen. Sehr hilfreich hat sich bisher die Unterstützung des BfArM für Hersteller in Form des DiGA-Leitfadens sowie der Auslegungen bzw. Handreichungen zu Vorgaben der Digitale-Gesundheitsanwendungen-Verordnung (DiGAV) mit hohem Interpretationsspielraum erwiesen. Auf diese Weise können Hersteller eigene Wege zur technischen Umsetzung der Anforderungen wählen. Eine Fortführung ist unbedingt wünschenswert.

- Hoffnungsvoll stimmt ein Blick auf die erfolgte Ablösung der Medizinprodukterichtlinie (MDD) durch die Medizinprodukteverordnung (MDR) und die unterstützenden Arbeiten der Koordinierungsgruppe Medizinprodukte (MDCG), die sich in der entsprechenden „Guidance on Cybersecurity for Medical Devices" [25] niedergeschlagen haben. So wurde der Begriff der „Informationssicherheit" in der MDR explizit als „zu berücksichtigen" aufgenommen, während er in der MDD noch keine Erwähnung fand. Der Informationssicherheit wird also ein deutlich höherer Stellenwert als zuvor eingeräumt. Spannend bleibt, inwieweit sich auch hier die Erkenntnis durchsetzen wird, dass Informationssicherheit weit mehr ist als die Absicherung der IT. Letztendlich aber liegt der Ball aufseiten der Hersteller. Dort ist davon auszugehen, dass die eigenen Ansprüche an sichere und rechtskonforme Umsetzung umso eher erfüllt werden, desto weiter der Herstellungsprozess auf einen höheren Reifegrad gehoben wird. DiGA-Hersteller sollten hier, dem eigenen Reifegrad entsprechend, im Anwendungsentwicklungsprozess aktiv werden, beispielsweise mithilfe des „Building Security In Maturity Model" (BSIMM; [26]). Wer als DiGA-Hersteller nicht über ein internes Sicherheitsteam verfügt, kann hier, wie auch bei der regelmäßigen Umsetzungskontrolle, auf externe Beratung zurückgreifen.

Korrespondenzadresse

Dr. André Zilch
ZFT.COMPANY GmbH
Burgstraße 2, 65817 Eppstein, Deutschland
andre.zilch@zft.company

Einhaltung ethischer Richtlinien

Interessenkonflikt. A. Zilch und M. Tschirsich geben an, dass kein Interessenkonflikt besteht.

Für diesen Beitrag wurden von den Autoren keine Studien an Menschen oder Tieren durchgeführt. Für die aufgeführten Studien gelten die jeweils dort angegebenen ethischen Richtlinien.

Literatur

1. GKV-Spitzenverband (2021) Positionspapier des GKV-Spitzenverbandes: Anforderungen und Kriterien an Digitale Gesundheitsanwendungen. https://www.gkv-spitzenverband.de/media/dokumente/krankenversicherung_1/telematik/digitales/Positionspapier_DiGA_2021-01-07_barrierefrei.pdf. Zugegriffen: 25. Apr. 2021
2. Reinvere J (2021) Patientenakten als Waffe. https://www.faz.net/aktuell/feuilleton/datenskandal-in-finnland-dehnt-sich-aus-patientenakten-als-waffe-17177721.html. Zugegriffen: 25. Apr. 2021
3. BSI (2021) Glossar der Cybersicherheit. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/glossar-der-cyber-sicherheit_node.html. Zugegriffen: 14. Juni 2021
4. Brönneke JB, Debatin JF, Hagen J, Kircher P, Matthies H (2020) DiGA VADEMECUM: Was man zu Digitalen Gesundheitsanwendungen wissen muss. MWV, Berlin, S 91
5. Bartels KU, Backer M (2018) Die Berücksichtigung des Stands der Technik in der DSGVO. Datenschutz Datensicherh 42:214–219
6. International Organization for Standardization (2018) ISO/IEC 27000:2018: Information technology—security techniques—information security management systems—overview and vocabulary
7. VdS-Verlag (2018) VdS 10000:2018–12 (02) – Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU), Anforderungen
8. IT-Sicherheitscluster (2020) ISIS12-2.02: Informationssicherheit für KMU und KMO Handbuch und Katalog für Unternehmen. V 2.02
9. Roßnagel A, Sunyaev A, Lins S, Maier N, Teigeler H (2019) AUDITOR-Schutzklassenkonzept – Entwurfsfassung 0.2. 3.2.1.2 Datenarten mit hohem Schutzbedarfs (Schutzbedarfsklasse 2). https://www.auditor-cert.de/wp-content/uploads/2019/03/Schutzklassenkonzept_v2_final.pdf. Zugegriffen: 14. Juni 2021
10. Brönneke JB, Debatin JF, Hagen J, Kircher P, Matthies H (2020) DiGA VADEMECUM: Was man zu Digitalen Gesundheitsanwendungen wissen muss. MWV, Berlin, S 88
11. Roßnagel A, Sunyaev A, Lins S, Maier N, Teigeler H (2019) AUDITOR-Schutzklassenkonzept – Entwurfsfassung 0.2. 3.2.1.3 Datenarten mit sehr hohem Schutzbedarf (Schutzbedarfsklasse 3). https://www.auditor-cert.de/wp-content/uploads/2019/03/Schutzklassenkonzept_v2_final.pdf. Zugegriffen: 14. Juni 2021
12. International Organization for Standardization (2013) ISO/IEC 29115:2013: Information technology—security techniques—entity authentication assurance framework
13. BSI (2019) Technische Richtlinie TR-03107-1: Elektronische Identitäten und Vertrauensdienste im E-Government. Teil 1: Vertrauensniveaus und Mechanismen. Version 1.1.1. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.html. Zugegriffen: 25. Apr. 2021
14. BSI (2019) Technische Richtlinie TR-03107-1: Elektronische Identitäten und Vertrauensdienste im E-Government. Teil 1: Vertrauensniveaus und Mechanismen. Version 1.1.1. S 37. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.html. Zugegriffen: 25. Apr. 2021
15. FIDO Alliance (2020) FIDO Alliance white paper: multiple authenticators for reducing account recovery needs for FIDO-enabled consumer accounts. https://media.fidoalliance.org/wp-content/uploads/2020/06/FIDO_White_Paper_Multiple_Authenticators_CDWG.pdf. Zugegriffen: 25. Apr. 2021
16. VG Mainz. Urteil vom 17. Dez. 2020 (Az. 1 K 778/19.MZ)
17. DSK (2020) Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail. Orientierungshilfe des Arbeitskreises „Technische und organisatorische Datenschutzfragen". https://www.datenschutzkonferenz-online.de/media/oh/20200526_orientierungshilfe_e_mail_verschluesselung.pdf. Zugegriffen: 25. Apr. 2021
18. Zilch A, Tschirsich M, Brodowski C (2019) „Hacker hin oder her": Die elektronische Patientenakte kommt! https://media.ccc.de/v/36c3-10595-hacker_hin_oder_her_die_elektronische_patientenakte_kommt. Zugegriffen: 25. Apr. 2021
19. DSK (2019) Kurzpapier Nr. 20. Einwilligung nach der DS-GVO. https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf. Zugegriffen: 25. Apr. 2021
20. BfArM (2020) Das Fast Track Verfahren für digitale Gesundheitsanwendungen (DiGA) nach § 139e SGB V. Ein Leitfaden für Hersteller, Leistungserbringer und Anwender. https://www.bfarm.de/SharedDocs/Downloads/DE/Service/Beratungsverfahren/DiGA-Leitfaden.pdf?__blob=publicationFile. Zugegriffen: 25. Apr. 2021
21. Brönneke JB, Debatin JF, Hagen J, Kircher P, Matthies H (2020) DiGA VADEMECUM: Was man zu Digitalen Gesundheitsanwendungen wissen muss. MWV, Berlin, S 97
22. Brönneke JB, Debatin JF, Hagen J, Kircher P, Matthies H (2020) DiGA VADEMECUM: Was man

zu Digitalen Gesundheitsanwendungen wissen muss. MWV, Berlin, S 100
23. BfArM (2021) Informationen zur Zulässigkeit der Datenverarbeitung außerhalb Deutschlands im Zusammenhang mit dem Prüfverfahren des BfArM gemäß § 139e Fünftes Buch Sozialgesetzbuch (SGB V). https://www.bfarm.de/SharedDocs/Downloads/DE/Medizinprodukte/Datenverarbeitung_au%C3%9Ferhalb_Deutschlands_FAQ.pdf. Zugegriffen: 25. Apr. 2021
24. The OWASP Foundation (2017) OWASP top 10 – 2017. The ten most critical web application security risks. https://owasp.org/www-project-top-ten/. Zugegriffen: 25. Apr. 2021
25. Medical Device Coordination Group (2019) MDCG 2019-16: Guidance on cybersecurity for medical devices
26. Migues S, Steven J, Mike W (2021) Building security in maturity model (BSIMM) – version 11. https://www.bsimm.com/. Zugegriffen: 25. Apr. 2021