Bundesinstitut
für Arzneimittel
und Medizinprodukte

Datenschutz und Datensicherheit Anforderungen und Erfahrungen

04.05.2022

Fachgebiet DiGA-Fast-Track

Vorstellung der Referenten

Dr. Michael Berensmann
Wissenschaftlicher Mitarbeiter
Aktive Medizinprodukte und
In-vitro-Diagnostika

Lina Bünger
Sachbearbeiterin
DiGA-Fast-Track

Dr. Armin Grünewald
Wissenschaftlicher Mitarbeiter
DiGA-Fast-Track

Florian Strauch
Wissenschaftlicher Mitarbeiter
DiGA-Fast-Track

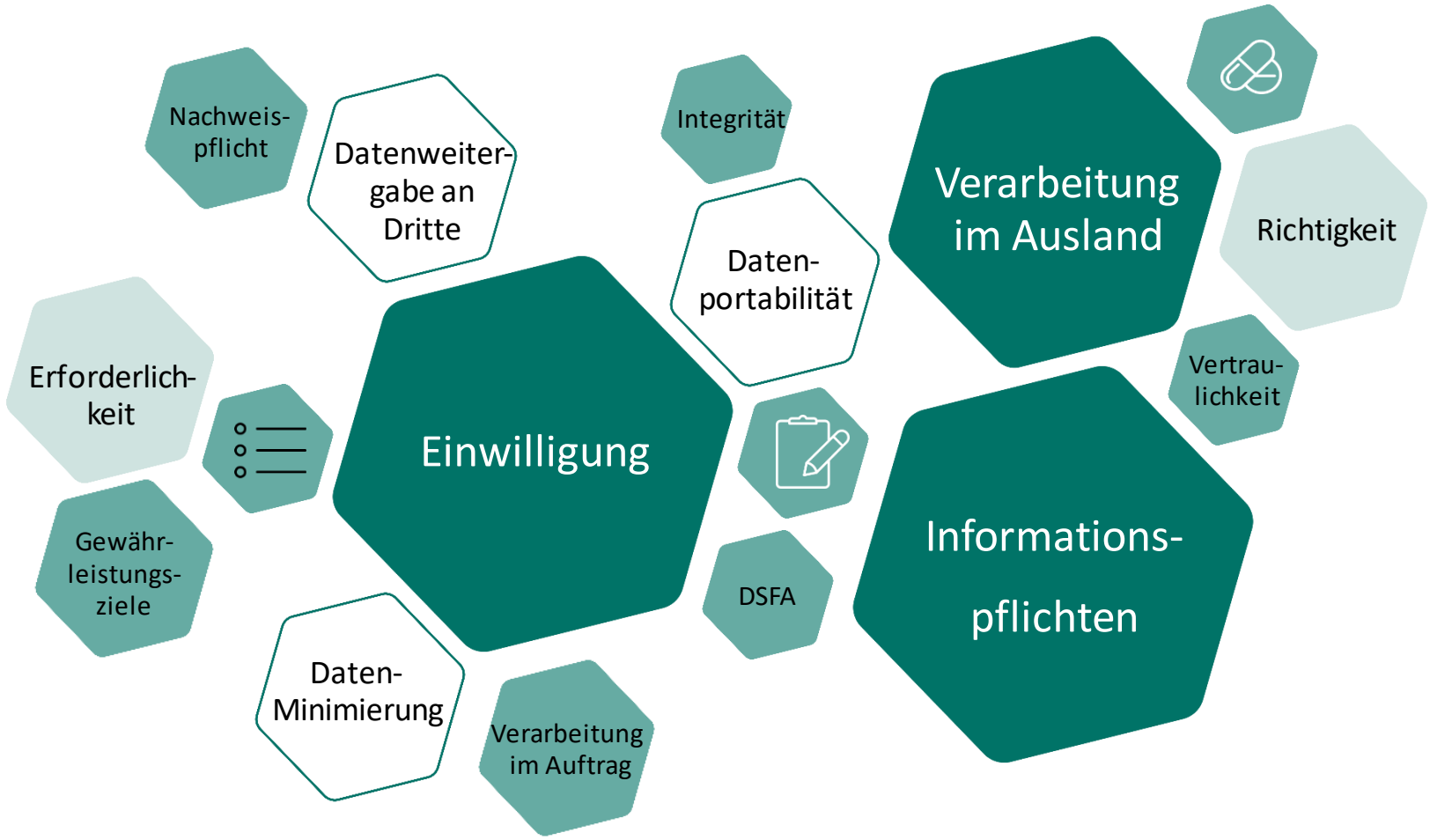
Bundesinstitut
für Arzneimittel
und Medizinprodukte

Agenda

09:30 Uhr – 09:45 Uhr	**Begrüßung und kurze Einführung** zum Thema Datenschutz und Datensicherheit
09:45 Uhr – 11:00 Uhr	**Themenblock 1: Datenschutz** Rechtliche Vorgaben aus der DiGAV „Lessons learned“ aus bisherigen Beratungs- und Antragsverfahren Eingereichte Fragen zum Thema
11:00 Uhr – 11:15 Uhr	**Kaffeepause**
11:15 Uhr – 12:25 Uhr	**Themenblock 2: Datensicherheit** Rechtliche Vorgaben aus der DiGAV „Lessons learned“ aus bisherigen Beratungs- und Antragsverfahren Eingereichte Fragen zum Thema
12:25 Uhr – 12:30 Uhr	**Abschluss**

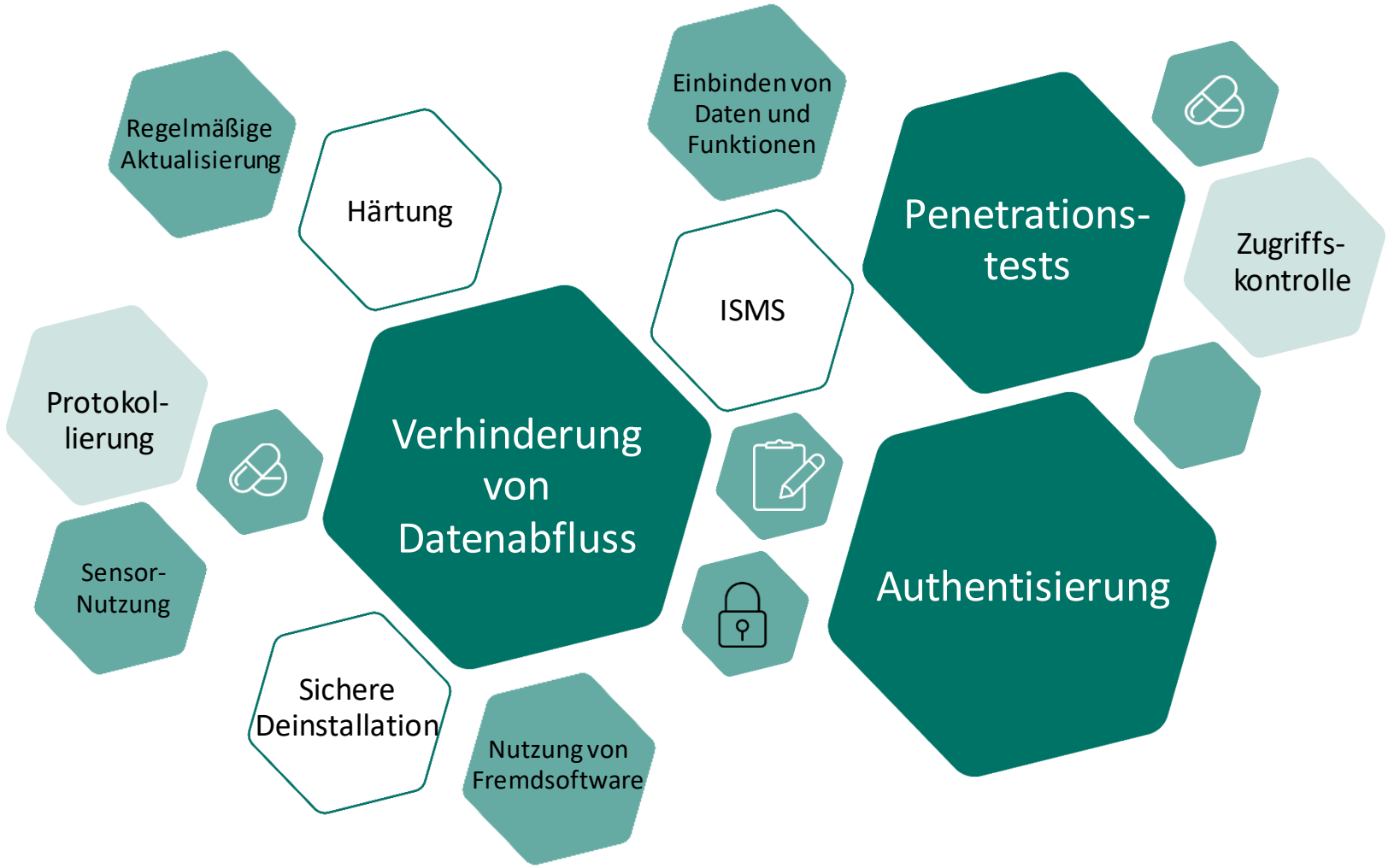
Bundesinstitut
für Arzneimittel
und Medizinprodukte

Themen Datenschutz



Bundesinstitut
für Arzneimittel
und Medizinprodukte

Themen Datensicherheit



Ziele des Webinars

Die Ziele des Webinars sind:

- Entwicklung eines besseren Verständnisses der Anforderungen an Datenschutz und Datensicherheit im DiGA-Verfahren
- Klarheit über die Anforderungen nach Anlage 1 der Digitale Gesundheitsanwendungen-Verordnung (DiGAV)
- Vermittlung des grundsätzlichen Rüstzeugs für eine erfolgreiche Umsetzung in der Praxis

Gegenstand des Webinars ist nicht:

- Klärung von produktspezifischen Fragen zum Thema Datenschutz und Datensicherheit
- Klärung regulatorischer Fragen (z. B. Daten aus anderen Medizinprodukten, Medizinprodukterecht)
- Details zu dem zukünftigen Datenschutzzertifikat sowie dem zukünftigen Datensicherheitszertifikat

Bundesinstitut
für Arzneimittel
und Medizinprodukte

Für produktspezifische Fragen zum Datenschutz und zur Datensicherheit empfehlen wir ein Beratungsgespräch

Anlaufstelle für DiGA-Beratungen:
Innovationsbüro des BfArM

https://www.bfarm.de/DE/Das-BfArM/Aufgaben/Beratungsverfahren/Innovationsbuero/_node.html

E-Mail: innovation@bfarm.de

Tel.: +49 228 99 307-4053

Bundesinstitut
für Arzneimittel
und Medizinprodukte

Wichtige Hinweise für das Webinar

- Fragen können im Chat gestellt werden
  - ✓ Bitte stellen Sie Ihre Frage nicht doppelt
  - ✓ Bitte senden Sie die Fragen im Chat an alle und nicht an einzelne Personen
  - ✓ Verständnisfragen zu den Folien gerne während des Vortrags stellen

  - Nicht beantwortete Fragen werden nach dem Webinar im Rahmen von FAQ beantwortet und auf der Webseite veröffentlicht

- Veröffentlichung der Folien nach dem Webinar auf der Webseite zur Veranstaltung

Überblick:

DiGA, Anforderungen und das Antragsverfahren

Was ist eine DiGA?

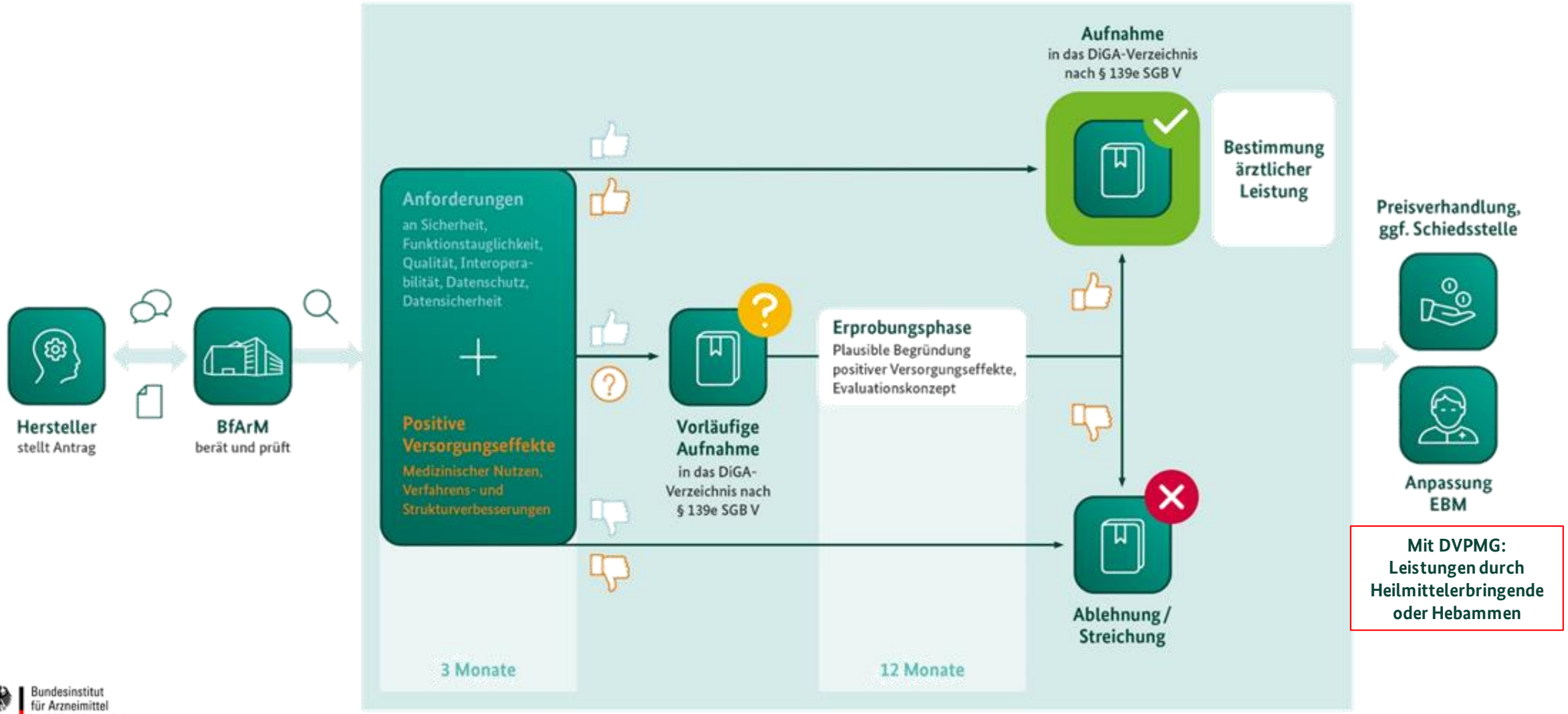
- Medizinprodukt
- niedrige Risikoklasse (I oder IIa)
- digitale Hauptfunktion
- medizinische Zweckbestimmung
- positiver Versorgungseffekt
- DiGA wird vom Patient oder von Leistungserbringer und Patient gemeinsam genutzt

Und was nicht?

- Primärpräventive digitale Anwendungen
- „Praxisausstattung“ / Telemedizinische Anwendungen

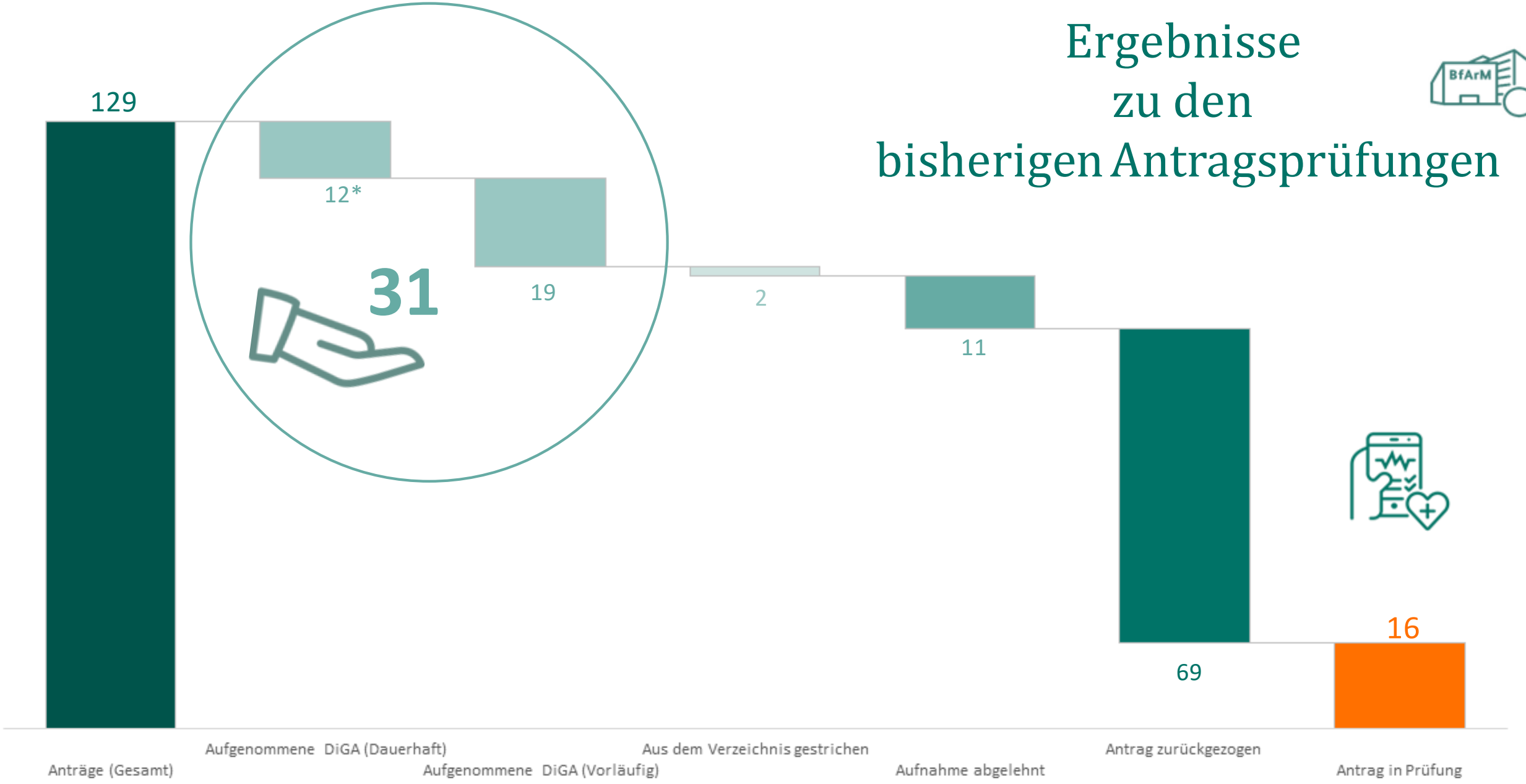
Bundesinstitut für Arzneimittel und Medizinprodukte

Der DiGA-Fast-Track zur „App auf Rezept“ im Überblick



Bundesinstitut für Arzneimittel und Medizinprodukte

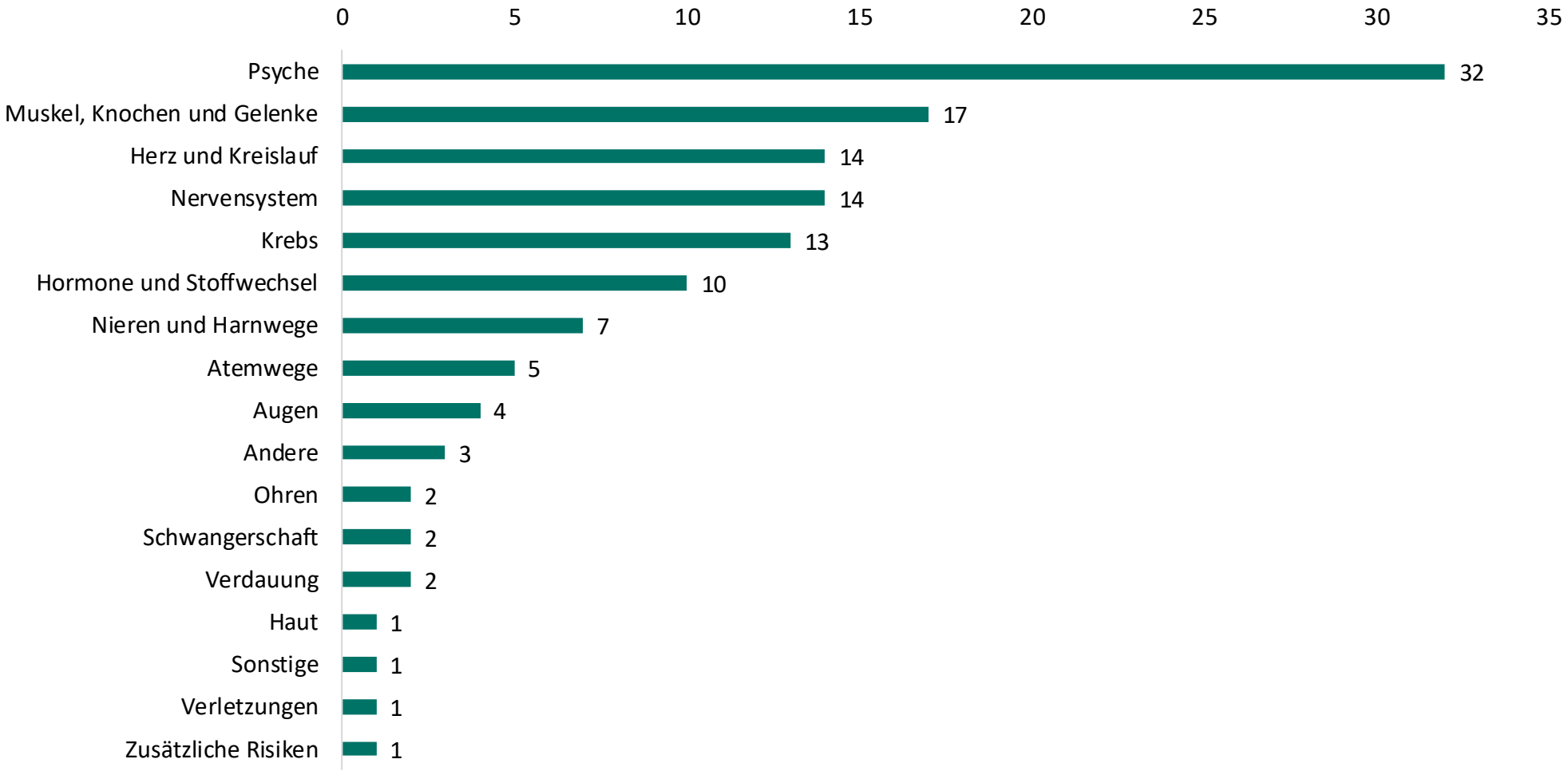
Ergebnisse zu den bisherigen Antragsprüfungen



Bundesinstitut für Arzneimittel und Medizinprodukte

*Von den 12 dauerhaft aufgenommenen, erbrachten 3 Ihre Nachweise in der Erprobungszeit

Kategorien der DiGA-Anträge



Bundesinstitut
für Arzneimittel
und Medizinprodukte

Anforderungen an eine DiGA

Sicherheit und
Funktionstauglichkeit
§ 3 DiGAV

Datenschutz und
Datensicherheit
§ 4 DiGAV

Voraussetzung aus dem SGB V und der DiGAV

Qualität, insbesondere
Interoperabilität
§§ 5 und 6 DiGAV

Positive Versorgungseffekte
§§ 8 bis 15 DiGAV

Bundesinstitut
für Arzneimittel
und Medizinprodukte

Grundlagen zu Datenschutz und Datensicherheit

§ 4 Absatz 1 DiGAV:

*Digitale Gesundheitsanwendungen müssen 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.*

Datenschutz:

- Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO) (siehe Anlage 1, Anforderung 1 Datenschutz der DiGAV)
- Vorgaben aus der DiGAV, insbesondere der Anlage 1

Aufbau der Checklisten für die Anforderungen an eine DiGA

DiGAV

Anlage 1: Fragebogen gemäß § 4 Absatz 6 DiGAV

Anforderungen an:
- Datenschutz
- Datensicherheit

Anlage 2: Fragebogen gemäß den §§ 5 und 6 DiGAV

Anforderungen an:
- Interoperabilität
- Robustheit
- Verbraucherschutz
- Nutzerfreundlichkeit
- Unterstützung von Leistungserbringenden
- Qualität medizinischer Inhalte
- Patientensicherheit

Ja-Nein-Aussagen

Eine nicht zur Auswahl vorgegebene „Nicht zutreffend“-Antwort erfordert eine schriftliche Begründung, warum das der Aussage übergeordnete Kriterium dennoch erfüllt wird.

Bundesinstitut für Arzneimittel und Medizinprodukte

Aufbau der Checklisten für die Anforderungen an eine DiGA

DiGAV

Anlage 1: Fragebogen gemäß § 4 Absatz 6 DiGAV

Nr.	Themenfeld	Anforderung	zutreffend	Nicht zutreffend	Zulässige Begründung für „nicht zutreffend“
Datenschutz					
1-40					
Datensicherheit					
Basisanforderungen, die für alle digitalen Gesundheitsanwendungen gelten					
1-37					
Zusatzanforderungen bei digitalen Gesundheitsanwendungen mit sehr hohem Schutzbedarf					
1-9					

Bundesinstitut für Arzneimittel und Medizinprodukte

Prüfung der Checklisten durch das BfArM

DiGAV

Anlage 1: Fragebogen gemäß § 4 Absatz 6 DiGAV

Erfahrungen:

Leider müssen wir immer wieder feststellen, dass die Anlagen nicht wahrheitsgemäß ausgefüllt werden.

Bitte setzen Sie sich mit den Anforderungen ausführlich auseinander und kommen Sie bei Fragen gerne auf uns zu (z. B. im Rahmen einer Beratung).

Bitte nehmen Sie alle Anforderungen ernst und stellen Sie sicher, dass jede entsprechende Anforderung vollumfänglich erfüllt ist, bevor Sie „*zutreffend*“ auswählen!

Bundesinstitut
für Arzneimittel
und Medizinprodukte

Prüfung der Checklisten durch das BfArM

DiGAV

Anlage 1: Fragebogen gemäß § 4 Absatz 6 DiGAV

Teil 1: Plausibilitätsprüfung

- Wurden die Checklisten vollständig und korrekt ausgefüllt?
- Sind die angegebenen Begründungen der „nicht-zutreffend“-Antworten schlüssig?

Teil 2: Inhaltliche Prüfung

- **Überprüfung der gemachten Angaben** mit Hilfe des zur Verfügung gestellten Zugangs zur App bzw. zur Webanwendung
- Beispiele: Prüfung der Datenschutzerklärung, Testen der Authentisierungsmethoden, Analyse der Datenverbindungen usw. (siehe später)

Ausblick: Zertifikate

DiGAV

§ 4 Absatz 7 und 8 DiGAV

- Sowohl das Datensicherheitszertifikat (§ 4 Absatz 7 DiGAV) als auch das Datenschutzzertifikat (§ 4 Absatz 8 DiGAV) befinden sich aktuell noch in der Abstimmung, sodass hier keine konkreten Informationen zu Inhalten oder Zeitplänen getroffen werden können.

- Sobald es hier mehr Informationen gibt, werden diese zusammen mit entsprechenden Erläuterungen und Hinweisen veröffentlicht.

Wichtige Hinweise

Unabhängig von der Prüfentscheidung des BfArM ist der **Hersteller einer DiGA jederzeit verantwortlich für die Gewährleistung aller datenschutz- und informationssicherheitsbezogenen sowie sonstigen rechtlichen Anforderungen an sein Medizinprodukt**. Deren **Einhaltung bei der Nutzung der DiGA gemäß dem aktuellen Stand der gesetzlichen und technischen Anforderungen sowie die wahrheitsgemäße Bestätigung** der entsprechenden Einhaltung gegenüber dem BfArM im Rahmen des Antragsverfahrens liegen ebenfalls **in seiner Verantwortung**.

- Nachfolgend aufgeführte Punkte zum Thema Datenschutz und Datensicherheit stellen keine abschließende Liste für das Antragsverfahren dar!

Bundesinstitut
für Arzneimittel
und Medizinprodukte

1. Themenblock: Datenschutz

Einwilligung

Einwilligung – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 2 Datenschutz

Wird vor der Verarbeitung von personenbezogenen und -beziehbaren Daten eine freiwillige, spezifische und informierte Einwilligung der betroffenen Person zu den in § 4 Absatz 2 benannten Zwecken der Verarbeitung dieser Daten eingeholt?

DiGAV, Anlage 1, Anforderung 3 Datenschutz

Erfolgt die Abgabe von Einwilligungen und Erklärungen der betroffenen Person durchgängig ausdrücklich, d. h. durch eine aktive, eindeutige Handlung der betroffenen Person?

Einwilligung – Lessons Learned

Beispiel zu DiGAV, Anlage 1, Anforderungen 2+3 Datenschutz

Registrierung

- [X] Ich akzeptiere die AGB *
- [X] Ich akzeptiere die Datenschutzerklärung *

* Erforderliche Einwilligung

Registrierung

- [ ] Ich akzeptiere die **AGB** *
- [ ] Ich akzeptiere die **Datenschutzerklärung** *

* Erforderliche Einwilligung

Bundesinstitut für Arzneimittel und Medizinprodukte

Einwilligung – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 5 Datenschutz

Wird die betroffene Person vor Abgabe der Einwilligung auf das Recht und die Möglichkeiten zum Widerruf der Einwilligung hingewiesen?

DiGAV, Anlage 1, Anforderung 6 Datenschutz

Wurde die betroffene Person vor Abgabe einer Einwilligung in klarer, verständlicher, nutzerfreundlicher und der Zielgruppe angemessener Form darüber informiert, welche Kategorien von Daten zu welchen Zwecken durch die digitale Gesundheitsanwendung bzw. den Hersteller der digitalen Gesundheitsanwendung verarbeitet werden?

Einwilligung – Lessons Learned

Beispiel zu DiGAV, Anlage 1, Anforderungen 5+6 Datenschutz

Registrierung

☐ Ich akzeptiere die AGB *

☐ Ich akzeptiere die Datenschutzerklärung *

* Erforderliche Einwilligung

Registrierung

☐ Ich akzeptiere die **AGB** *

☐ Ich akzeptiere die **Datenschutzerklärung** *

* Erforderliche Einwilligung

Die Einwilligung kann jederzeit in den Einstellungen widerrufen werden.

Welche Kategorien von Daten werden zu welchen Zwecken erhoben?

Bundesinstitut für Arzneimittel und Medizinprodukte

Einwilligung – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 4 Datenschutz

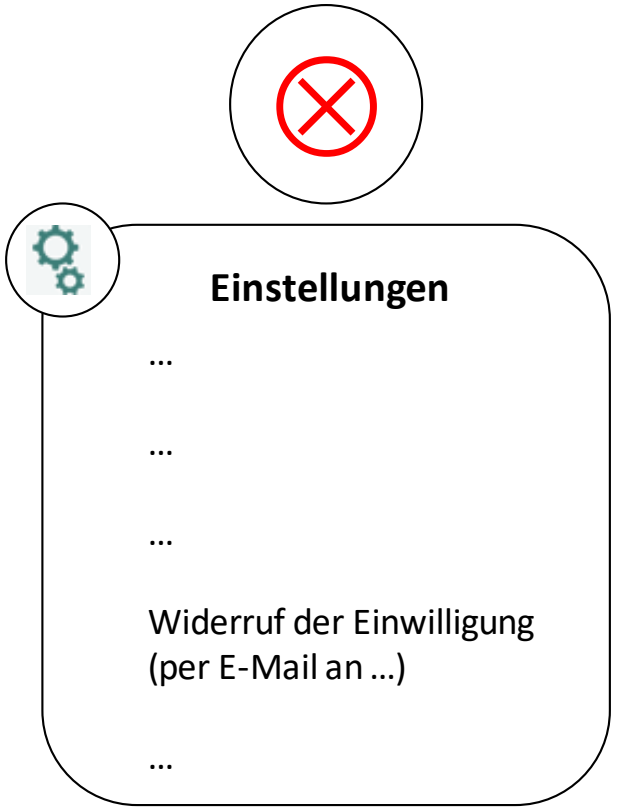
Kann die betroffene Person erteilte Einwilligungen einfach, barrierefrei, jederzeit und auf einem einfach verständlichen Weg mit Wirkung für die Zukunft widerrufen?

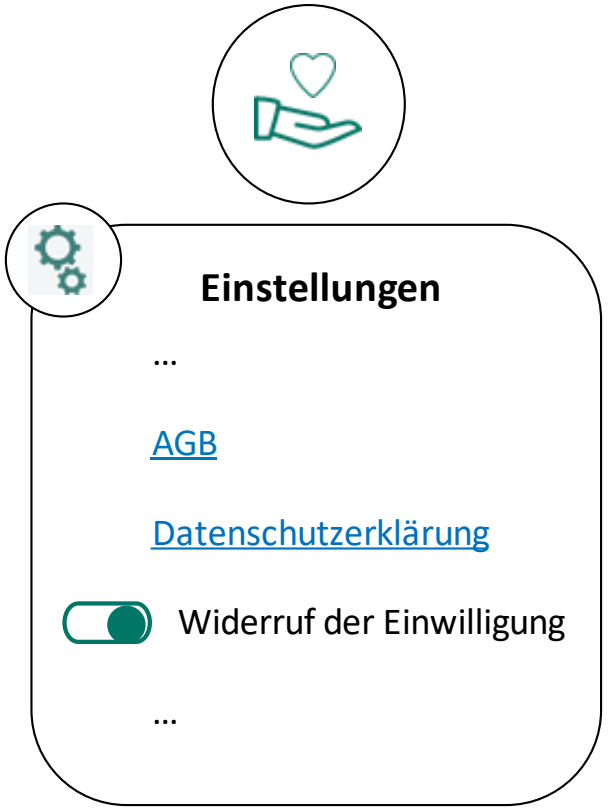
DiGAV, Anlage 1, Anforderung 7 Datenschutz

Kann die betroffene Person die Texte der abgegebenen Einwilligungen und Erklärungen jederzeit aus der digitalen Gesundheitsanwendung oder über eine aus der digitalen Gesundheitsanwendung referenzierten Quelle abrufen?

Einwilligungen – Lessons Learned

Beispiel zu DiGAV, Anlage 1, Anforderungen 4+7 Datenschutz





Bundesinstitut
für Arzneimittel
und Medizinprodukte

1. Themenblock: Datenschutz

Zweckbindung

Zweckbindung – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 8 Datenschutz

Erfolgt die Verarbeitung von personenbezogenen Daten durch die digitale Gesundheitsanwendung ausschließlich zu in § 4 Absatz 2 Satz 1 genannten Zwecken oder auf Grundlage sonstiger gesetzlicher Datenverarbeitungsbefugnisse nach § 4 Absatz 2 Satz 3?

Zwecke nach § 4 Absatz 2 Satz 1 DiGAV:

1. Bestimmungsgemäßer Gebrauch der DiGA durch die Nutzer
2. Nachweis positiver Versorgungseffekte im Rahmen einer Erprobung nach § 139e Absatz 4 SGB V
3. Nachweisführung bei Vereinbarungen nach § 134 Absatz 1 Satz 3 SGB V

} Können in einer Einwilligung zusammengefasst werden

4. Dauerhafte Gewährleistung der technischen Funktionsfähigkeit, der Nutzerfreundlichkeit und der Weiterentwicklung der DiGA

} Gemäß § 4 Absatz 2 Satz 2 DiGAV zusätzliche Einwilligung erforderlich

Bundesinstitut für Arzneimittel und Medizinprodukte

Zweckbindung – Lessons Learned

Beispiel zu DiGAV, Anlage 1, Anforderung 8 Datenschutz

Zwecke nach § 4 Absatz 2 Satz 1 Nr. 1-4 DiGAV in einer Einwilligung zusammengefasst

Registrierung

☐ Ich akzeptiere die **AGB** *

☐ Ich akzeptiere die **Datenschutzerklärung** *

* Erforderliche Einwilligung

Die Einwilligung kann jederzeit in den Einstellungen widerrufen werden.

Registrierung

☐ Ich akzeptiere die **AGB** *

☐ Ich akzeptiere die **Datenschutzerklärung** *

☐ Ich akzeptiere, dass meine Daten zum Zwecke der dauerhaften Gewährleistung der technischen Funktionsfähigkeit, der Nutzerfreundlichkeit und der Weiterentwicklung der DiGA verarbeitet werden.

* Erforderliche Einwilligung

Die Einwilligung kann jederzeit in den Einstellungen widerrufen werden.

Bundesinstitut für Arzneimittel und Medizinprodukte

1. Themenblock: Datenschutz

Datenminimierung und Angemessenheit

Datenminimierung und Angemessenheit – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 9 Datenschutz

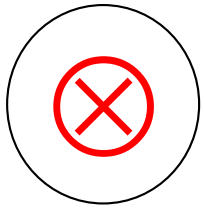
Sind die über die digitale Gesundheitsanwendung verarbeiteten personenbezogenen Daten dem Zweck angemessen sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt?

DiGAV, Anlage 1, Anforderung 10 Datenschutz

Hat der Hersteller der digitalen Gesundheitsanwendung sichergestellt, dass die Zwecke der Verarbeitung personenbezogener Daten durch die digitale Gesundheitsanwendung nicht in zumutbarer Weise durch andere, datensparsamere Mittel in gleichem Maße erreicht werden können?

Datenminimierung und Angemessenheit – Lessons Learned

Beispiel zu DiGAV, Anlage 1, Anforderungen 9+10 Datenschutz



3. Bei der Nutzung der App erhobene Daten
Bei der Verwendung unserer App erheben und verarbeiten wir personenbezogene Daten bzw. Gesundheitsdaten.
(1) Wir erheben und verarbeiten unter anderen folgende Daten von Ihnen für die jeweils benannten Zwecke:

- Vorname, Nachname, Adresse
- Handynummer, E-Mailadresse, Spitzname
- Lieblingsrestaurant, Hobbys
- Religion
- Diverse Gesundheitsdaten

3. Bei der Nutzung der App erhobene Daten
Bei der Verwendung unserer App erheben und verarbeiten wir personenbezogene Daten bzw. Gesundheitsdaten.
(1) Wir erheben und verarbeiten folgende Daten von Ihnen für die jeweils benannten Zwecke:

- Benutzername
- Vitalparameter
- Persönlicher Medikationsplan

-> abschließende Liste der Kategorien angeben!

Datenminimierung und Angemessenheit – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 11 Datenschutz

Werden gesundheitsbezogene Daten getrennt von ausschließlich für die Leistungsabrechnung erforderlichen Daten gespeichert?

DiGAV, Anlage 1, Anforderung 12 Datenschutz

Stellt der Hersteller der digitalen Gesundheitsanwendung sicher, dass mit nicht-produktbezogenen Aufgaben betraute Mitarbeiterinnen und Mitarbeiter keinen Zugriff auf gesundheitsbezogene Daten haben?

Datenminimierung und Angemessenheit – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 13 Datenschutz

Sofern die Nutzung der digitalen Gesundheitsanwendung nicht auf ein privates IT-System der nutzenden Person beschränkt ist:

- *wurden entsprechende Einsatzszenarien in der Datenschutzfolgenabschätzung explizit berücksichtigt?*
- *wird der Versicherte ausdrücklich darauf hingewiesen, dass die Nutzung der digitalen Gesundheitsanwendung in einer potenziell unsicheren Umgebung mit Sicherheitsrisiken einhergeht, die durch den Hersteller der digitalen Gesundheitsanwendung nicht vollständig adressiert werden können?*
- *wird bei Nutzung der digitalen Gesundheitsanwendung auf einem nicht nur von dem Versicherten verwendeten IT-System vollständig die – auch temporäre – Speicherung von gesundheitsbezogenen Daten auf diesem IT-System unterbunden?*

Datenminimierung und Angemessenheit – Lessons Learned

Beispiel zu DiGAV, Anlage 1, Anforderungen 13 Datenschutz

- Auf Risiko eines möglichen Datenzugriffs durch Unbefugte hinweisen
- Beispiele geben, wann dies der Fall sein kann: Nutzung der Anwendung auf einem öffentlichen Gerät bzw. Gemeinschaftsgerät
- Schutzmaßnahmen vorschlagen:
  - Verwendung eines privaten Surfmodus, wenn dieser von dem Webbrowser unterstützt wird
  - Nach Beendigung der Anwendung aus diese ausloggen

Datenminimierung und Angemessenheit – Oft gestellte Fragen aus Beratungsgesprächen

Die Datenschutzerklärung erwähnt diesbezüglich eindeutig: „Keine Übertragung, Methode oder elektronische Speicherung ist zu 100% sicher und während wir anstreben, jede kommerziell akzeptable Maßnahme zu verwenden, können wir nicht die absolute Sicherheit der personenbezogenen Daten garantieren.“ Ist dies so akzeptabel?

Nein. Es sollte für Nutzende genau spezifiziert werden, in welchen Situationen größere Sicherheitsrisiken bestehen, wie z. B. bei der Nutzung von Fremdgeräten oder unsicheren WLAN-Hotspots. Diese Warnung sollte für Nutzende möglichst prominent, also beispielsweise als Pop-Up bei der initialen Anmeldung in der DiGA erfolgen.

Des Weiteren deutet „*kommerziell akzeptable Maßnahmen*“ darauf hin, dass aus Kostengründen Datenschutz eingespart werden soll. Dies ist fragwürdig.

1. Themenblock: Datenschutz

Integrität und Vertraulichkeit

Integrität und Vertraulichkeit – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 14 Datenschutz

Sieht die digitale Gesundheitsanwendung angemessene technische und organisatorische Maßnahmen vor, um personenbezogene Daten gegen unbeabsichtigte oder unzulässige Zerstörung, Löschung, Verfälschung, Offenbarung oder nicht legitimierte Verarbeitungsformen zu schützen?

DiGAV, Anlage 1, Anforderung 15 Datenschutz

Ist der durch die digitale Gesundheitsanwendung gesteuerte Austausch von Daten zwischen dem Endgerät der betroffenen Person und externen Systemen durchgängig gemäß dem Stand der Technik verschlüsselt?

Integrität und Vertraulichkeit – Oft gestellte Fragen aus Beratungsgesprächen

Anforderung 15 lautet „*durchgängig gemäß dem Stand der Technik verschlüsselt*“. Gilt die Export-Funktion, die ja manuell ausgeführt wird, als "*durch die DiGA gesteuerter Austausch*"?

Ja, der Abruf der Daten von einem Server für den Datenexport muss verschlüsselt sein.

Integrität und Vertraulichkeit – Oft gestellte Fragen aus Beratungsgesprächen

DiGAV und DiGA-Leitfaden verweisen auf den Stand der Technik. Welche technischen Richtlinien muss ich kennen, um die in der Checkliste in Anlage 1 der DiGAV formulierten Anforderungen gemäß dem Stand der Technik umzusetzen?

Hier sind insbesondere – aber nicht abschließend! – die folgenden Richtlinien zu nennen:

- BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen
- BSI TR-02102-2 Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)
- BSI TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1
- BSI TR-03161 Sicherheitsanforderungen an digitale Gesundheitsanwendungen

1. Themenblock: Datenschutz

Richtigkeit

Richtigkeit – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 16 Datenschutz

Sieht die digitale Gesundheitsanwendung technische und organisatorische Maßnahmen vor, die sicherstellen, dass die über die digitale Gesundheitsanwendung verarbeiteten personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind?

DiGAV, Anlage 1, Anforderung 17 Datenschutz

Trifft der Hersteller alle angemessenen Maßnahmen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden?

Richtigkeit
– Oft gestellte Fragen aus Beratungsgesprächen

Die Fragen in den Anlagen 1 und 2 der DiGAV scheinen unter der Annahme entwickelt worden zu sein, dass der Hersteller der DiGA auch der für die Verarbeitung Verantwortliche ist. Bei unserem Produkt ist der Leistungserbringer verantwortlich für die Datenverarbeitung und wir als Hersteller des Produkts dienen lediglich als Datenverarbeiter im Auftrag des Leistungserbringers. Dafür holt der Leistungserbringer die Einwilligung des Patienten vor Verschreibung ein.

Das Vorgehen ist nicht zulässig. Der Hersteller der DiGA legt fest, wie Daten verarbeitet werden und ist damit Verantwortlicher gemäß Artikel 4 der DSGVO und ist daher unter anderem gemäß der Anforderung der DiGAV verantwortlich für die Richtigkeit der personenbezogenen Daten.
https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

1. Themenblock: Datenschutz

Erforderlichkeit

Erforderlichkeit – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 18 Datenschutz

Werden über die digitale Gesundheitsanwendung erhobene personenbezogene Daten nur so lange gespeichert, wie sie für die Erbringung der zugesagten Funktionalitäten der digitalen Gesundheitsanwendung oder zu anderen, unmittelbar aus rechtlichen Verpflichtungen resultierenden Zwecken zwingend erforderlich sind?

DiGAV, Anlage 1, Anforderung 19 Datenschutz

Werden personenbezogene Daten nach Erfüllung der Zwecke nach § 4 Absatz 2 Satz 1 Nummer 1 bis 4 nicht weiter gespeichert?

Erforderlichkeit – Lessons Learned

Beispiel zu DiGAV, Anlage 1, Anforderung 19 Datenschutz

Datenschutzerklärung

Speicherdauer:

Die personenbezogenen Daten werden ein Jahr lang gespeichert.

Datenschutzerklärung

Speicherdauer:

Die personenbezogenen Daten werden so lange gespeichert, wie sie zur Erfüllung des Zwecks/ der Zwecke, für den/die sie im Rahmen der Verordnung erhoben wurden, benötigt werden.

Erforderlichkeit
– Oft gestellte Fragen aus Beratungsgesprächen

Wir speichern die personenbezogenen Daten für 10 Jahre nach Beendigung der Nutzung der DiGA. Dies ergibt sich aus der Aufbewahrungspflicht, die wir analog zu § 630f BGB (PatRG) sowie dem Bundesmantelvertrag für Ärzte (§ 57) sowie der Berufsordnung für Ärzte ableiten. Wie steht das BfArM dazu?

Eine Ableitung von Aufbewahrungspflichten für Ärzte ist nicht zulässig. Für DiGA gilt die eindeutige Regelung einer Löschung der Daten nach Erfüllung der Zwecke nach § 4 Absatz 2 Satz 1 Nummer 1 bis 4.

1. Themenblock: Datenschutz

Datenportabilität

Datenportabilität – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 20 Datenschutz

Stellt der Hersteller der digitalen Gesundheitsanwendung Mechanismen bereit, über die die betroffene Person aus der digitalen Gesundheitsanwendung heraus das Recht auf Datenportabilität wahrnehmen und die von ihr, der betroffenen Person, der digitalen Gesundheitsanwendung bereitgestellten, sie betreffenden personenbezogenen Daten in einem geeigneten Format abrufen bzw. in eine andere digitale Gesundheitsanwendung überführen kann?

Datenportabilität – Lessons Learned

Informationen zu DiGAV, Anlage 1, Anforderungen 20 Datenschutz

Siehe auch Art. 20 DSGVO: Recht auf Datenübertragbarkeit
„die sie betreffenden personenbezogenen Daten (…) in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten“

Darüber hinaus: Zusätzliche Anforderungen an die Interoperabilität (Export in einem menschenlesbaren und maschinenlesbaren Format), der deutlich genauer spezifiziert ist.

→ Webinar „Interoperabilität bei DiGA“ am 23.09.2022, 9.30 – 12.30 Uhr

1. Themenblock: Datenschutz

Weitere Fragen zu den bisherigen Themen

1. Themenblock: Datenschutz

Informationspflichten

Informationspflichten – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 21 Datenschutz

Ist die Datenschutzerklärung der digitalen Gesundheitsanwendung über die Anwendungswebseite einfach auffindbar, barrierefrei zugänglich und frei einsehbar?

DiGAV, Anlage 1, Anforderung 23 Datenschutz

Ist die Datenschutzerklärung der digitalen Gesundheitsanwendung auch nach der Installation der digitalen Gesundheitsanwendung aus der digitalen Gesundheitsanwendung heraus bzw. in der digitalen Gesundheitsanwendung einfach auffindbar?

Informationspflichten – Lessons Learned

Beispiel zu DiGAV, Anlage 1, Anforderungen 21 und 23 Datenschutz

- ✓ Auf der Anwendungswebseite der DiGA lässt sich die Datenschutzerklärung direkt auffinden, ist barrierefrei zugänglich und frei einsehbar.
  - ➢ Es handelt sich um die Datenschutzerklärung der DiGA und nicht um die Datenschutzerklärung der Webseite
  - ➢ Barrierefreiheit gemäß Kapitel 3.6.3. im DiGA-Leitfaden

- ✓ Die Datenschutzerklärung der DiGA kann in der DiGA schnell aufgefunden und eingesehen werden.

Bundesinstitut für Arzneimittel und Medizinprodukte

Informationspflichten – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 22 Datenschutz

Enthält die Datenschutzerklärung der digitalen Gesundheitsanwendung alle relevanten Informationen zum Hersteller und dessen Datenschutzbeauftragtem, zu dem Zweck der digitalen Gesundheitsanwendung, zu den dazu verarbeiteten Datenkategorien, zum Umgang des Herstellers mit diesen Daten, zum Recht auf Widerruf gegebener Einwilligungen und zu den Möglichkeiten zur Wahrnehmung der Betroffenenrechte und setzt der Hersteller der digitalen Gesundheitsanwendung darüber hinausgehende Informationspflichten nach den Artikeln 13 und 14 der Verordnung (EU) 2016/679 angemessen um?

Informationspflichten – Lessons Learned

Beispiel zu DiGAV, Anlage 1, Anforderung 22 Datenschutz

Die Datenschutzerklärung enthält:

- ✓ Name und Adresse des Herstellers, Kontaktdaten des Datenschutzbeauftragten
- ✓ Zweck der DiGA
- ✓ die für den Zweck verarbeiteten Datenkategorien
- ✓ Umgang des Herstellers mit den verarbeiteten Daten
- ✓ Recht auf Widerruf gegebener Einwilligungen
- ✓ Möglichkeiten der Wahrnehmung der Betroffenenrechte
- ✓ Weitere Informationspflichten des Herstellers nach den Artikeln 13 und 14 der Verordnung (EU) 2016/679

Informationspflichten – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 24 Datenschutz

Kann die betroffene Person vom Hersteller der digitalen Gesundheitsanwendung Auskunft zu den über sie gespeicherten personenbezogenen Daten in dem in Artikel 15 der Verordnung (EU) 2016/679 festgelegten Umfang erhalten?

DiGAV, Anlage 1, Anforderung 26 Datenschutz

Kann die betroffene Person vom Hersteller der digitalen Gesundheitsanwendung die Berichtigung von sie betreffenden unrichtigen personenbezogenen Daten und die Vervollständigung von sie betreffenden unvollständigen personenbezogenen Daten verlangen?

Informationspflichten – Lessons Learned

Beispiel zu DiGAV, Anlage 1, Anforderung 24 Datenschutz

- ✓ Die betroffene Person kann vom Hersteller Auskunft zu den über sie gespeicherten personenbezogenen Daten erhalten. Der Umfang bemisst sich nach Artikel 15 der Verordnung (EU) 2016/679:
  - ➢ Auskunft über die personenbezogenen Daten und Informationen zu den Verarbeitungswecken, den Kategorien der personenbezogenen Daten, zu den Empfängern der Daten etc.
  - ➢ Form: Kopie oder bei elektronischem Antrag ein elektronisches Formular

Informationspflichten – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 25 Datenschutz

Ist in der Datenschutzerklärung der digitalen Gesundheitsanwendung ein nachvollziehbares Löschkonzept enthalten, das das Vorgehen bei Widerruf der Einwilligung und Deinstallation der digitalen Gesundheitsanwendung sowie den Umgang mit Ansprüchen auf Löschung von Daten sowie auf Einschränkung ihrer Verarbeitung regelt und den Anforderungen nach den Artikeln 17 bis 19 der Verordnung (EU) 2016/679 entspricht?

DiGAV, Anlage 1, Anforderung 27 Datenschutz

Wird die betroffene Person vor der Löschung des Benutzerkontos auf damit möglicherweise verlorengehende Daten und auf das Recht auf Datenübertragung gemäß Artikel 20 der Verordnung (EU) 2016/679 hingewiesen?

Informationspflichten – Lessons Learned

Beispiel zu DiGAV, Anlage 1, Anforderungen 25 und 27 Datenschutz

- ✓ Datenschutzerklärung enthält nachvollziehbares Löschkonzept
  - ➢ Beschreibung des Widerrufs der Einwilligung und der Deinstallation
    - ▪ Erfüllung der Anforderungen nach den Artikeln 17 bis 19 der Verordnung (EU) 2016/679, z. B. Löschung der personenbezogenen Daten, sobald die Zweckbestimmung nicht mehr gegeben ist
- ✓ Löschen des eigenen Kontos und der eigenen Daten aus der DiGA heraus
  - ➢ Vor der Löschung erscheint eine Warnmeldung mit dem Hinweis auf Löschung der Daten und das Recht auf Datenübertragung gemäß Artikel 20 der Verordnung (EU) 2016/679

Informationspflichten – Eingereichte Fragen

Wie viel Zeit in Wochen nach Ablauf der Verschreibung ist eine vom BfArM akzeptierte Löschfrist? Konkret: Eine nicht mit Datenexporten vertraute Patientin im Alter von 72 Jahren erzielt durch die Nutzung einer DiGA einen Therapiefortschritt (z.B. höheres Übungslevel). Sie erhält ihre Folgeverschreibung leider mit einer Verzögerung von 2 Monaten und ihr Profil samt Übungsfortschritt wurden gelöscht.

Es gibt keine akzeptierte Übergangszeit für eine Löschfrist. Es sollte frühzeitig daran erinnert werden, eine Folgeverschreibung vorzunehmen. Um Datenverlust vorzubeugen, sollte es neben dem Datenexport auch eine Datenimport-Funktion geben.

Gibt es eine Möglichkeit für Patient:innen der Löschung der Daten zu widersprechen? Wenn ja, wie lange ist dann die abermalige Löschfrist?

Dies ist nicht vorgesehen, stattdessen sollte ein Export angeboten werden, sodass die Daten lokal auf dem eigenen Gerät gespeichert werden können.

Informationspflichten – Eingereichte Fragen

Sofern eine DiGA Zugriffsmöglichkeiten für den Nutzer (Patienten) und den behandelnden Arzt (Arztportal) vorsieht: Welchen Umfang muss das Löschkonzept vor dem Hintergrund haben, dass sichergestellt werden kann/muss, dass nach Ende der Nutzung der DiGA durch den Patienten auch der Arzt seinen Zugang und die Nutzung der DiGA-Daten beendet?

Es sollte eine Löschung der Daten erfolgen. Damit verliert auch die Ärztin oder der Arzt den Zugang zu den Daten. Sollte diese oder dieser keine aktiven Patientinnen oder Patienten mehr besitzen, müssen auch die Daten der Ärztin bzw. des Arztes gelöscht werden.

1. Themenblock: Datenschutz

Datenschutz-Management

Datenschutz-Management – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 28 Datenschutz

Hat der Hersteller der digitalen Gesundheitsanwendung ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung umgesetzt, mit dem alle im Zusammenhang mit der digitalen Gesundheitsanwendung eingesetzten Systeme und Prozesse erfasst sind?

DiGAV, Anlage 1, Anforderung 29 Datenschutz

Hat der Hersteller der digitalen Gesundheitsanwendung alle Personen, die aus ihrer Tätigkeit heraus Zugang zu personenbezogenen Daten haben, auf die Verschwiegenheit verpflichtet?

Datenschutz-Management – Lessons Learned

Informationen zu DiGAV, Anlage 1, Anforderungen 28 Datenschutz

- Datenschutz-Management muss dokumentiert sein. Nachweise können bei Bedarf vom BfArM eingefordert werden.
- Bietet Sicherheit im Rechtsfall, wenn Datenschutzverletzungen angezeigt werden (welche gemäß DSGVO mit Geldbußen und Freiheitsstrafen geahndet werden können).

1. Themenblock: Datenschutz

Verarbeitung im Auftrag

Verarbeitung im Auftrag – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 36 Datenschutz

Werden über die digitale Gesundheitsanwendung oder den Hersteller der digitalen Gesundheitsanwendung personenbezogene Daten gar nicht an Auftragsverarbeiter oder ausschließlich an Auftragsverarbeiter weitergegeben, die über eine ausreichende Vertrauenswürdigkeit und Haftbarkeit verfügen, angemessene Mechanismen zum Schutz übernommener Daten realisieren und mit dem Hersteller in einem verpflichtenden vertraglichen Verhältnis stehen, das eine Abschwächung der dem Versicherten gegenüber gemachten Zusagen ausschließt?

Verarbeitung im Auftrag – Lessons Learned

Informationen zu DiGAV, Anlage 1, Anforderungen 36 Datenschutz

- Im Antrag müssen die *„Standorte der Datenverarbeitung“* sowie alle *„zur Datenverarbeitung beauftragten Dienstleister“ angegeben werden.*
- Anforderungen an den Datenschutz dürfen durch die Beauftragung nicht beeinflusst/gemindert werden.

1. Themenblock: Datenschutz

Datenweitergabe an Dritte

Datenweitergabe an Dritte – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 37 Datenschutz

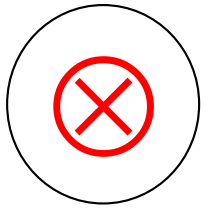
Werden über die digitale Gesundheitsanwendung oder den Hersteller der digitalen Gesundheitsanwendung keine personenbezogenen Daten an Dritte weitergegeben, sofern dies nicht unmittelbar für die Erfüllung von Zwecken nach § 4 Absatz 2 Satz 1 Nummer 1 oder die Erfüllung gesetzlicher Vorschriften erforderlich und auf diese Zwecke beschränkt ist?

Erinnerung: Zwecke nach § 4 Absatz 2 Satz 1 Nummer 1 DiGAV

zu dem bestimmungsgemäßen Gebrauch der digitalen Gesundheitsanwendung durch die Nutzer

Datenweitergabe an Dritte – Lessons Learned

Beispiel zu DiGAV, Anlage 1, Anforderungen 37 Datenschutz



Nicht erlaubt ist die Verwendung von personenbezogenen Daten für Marketingzwecke oder Werbung.

1. Themenblock: Datenschutz

Verarbeitung im Ausland

Verarbeitung im Ausland – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 38 Datenschutz

Erfolgt die Verarbeitung von Gesundheitsdaten sowie personenidentifizierbaren Bestands- und Verkehrsdaten ausschließlich im Inland, in einem anderen Mitgliedstaat der Europäischen Union, in einem diesem nach § 35 Absatz 7 des Ersten Buches Sozialgesetzbuch gleichgestellten Staat, oder auf Grundlage eines Angemessenheitsbeschlusses gemäß Artikel 45 der Verordnung (EU) 2016/679?

Zusätzlich: § 4 Absatz 3 DiGAV

Ergänzung im Referentenentwurf der DiGAV:
Die weitreichenden Ausnahmen nach Artikel 46 und 47 der Verordnung (EU) 2016/679 sind für digitale Gesundheitsanwendungen aufgrund des regelhaft anzunehmenden besonderen Schutzbedarfs der verarbeiteten Daten nicht anwendbar.

Verarbeitung im Ausland – Lessons Learned

Hinweise zu DiGAV, Anlage 1, Anforderung 38 Datenschutz

Handreichung zur „*Datenverarbeitung außerhalb Deutschlands*“ beachten!

BfArM-Webseite, DiGA:
https://www.bfarm.de/SharedDocs/Downloads/DE/Medizinprodukte/Datenverarbeitung_ausserhalb_Deutschlands_FAQ.pdf;jsessionid=D1973CA733753372069531E581EE0E8A.intranet241?__blob=publicationFile

- Verarbeitung personenbezogener Daten außerhalb der vorgenannten Länder nicht erlaubt
- Besondere Reglungen gelten, wenn Daten in der EU verarbeitet werden, der Mutterkonzern den Hauptsitz aber in einem Land hat, welches die zuvor genannten Kriterien nicht erfüllt
  - im Fall eines Herausgabeverlangens muss der Rechtsweg beschritten und ausgeschöpft werden
  - Schlüssel-Speicherung: Datenverarbeiter dürfen keinen Zugriff auf die Schlüssel haben (gilt auch für Schlüsselkopien)

Verarbeitung im Ausland – Lessons Learned

Beispiele zu DiGAV, Anlage 1, Anforderung 38 Datenschutz

Im Rahmen der inhaltlichen Prüfung werden die IP-Adressen überprüft, zu denen die App bzw. Anwendung eine Verbindung aufbaut.

Folgende Erfahrungen zu ungewollten Datenabfluss wurden hierbei schon gesammelt:

Unternehmen	Ursache
Google LLC	Google Schriftarten
Amazon.com, Inc.	Dienst „*Branch.io*“
Microsoft Corporation	Dienstleister Selligent GmbH Dienst „*CodePush*“

Bundesinstitut für Arzneimittel und Medizinprodukte

Verarbeitung im Ausland – Eingereichte Fragen

Können im DiGA-Antragsprozess Bedenken bei der Nutzung von AWS (Standort Frankfurt) als generellem Cloud-Anbieter bestehen, wenn jegliche personenbezogenen Daten sowieso getrennt und ausschließlich bei einem spezialisiertem und zertifiziertem europäischen Cloud-Anbieter gehosted werden?

Hier stellt sich die Frage, welche Daten noch bei AWS gespeichert werden. IP-Adressen sind ebenfalls als personenbezogene Daten zu werten, und gesundheitsbezogene Daten sind in diesem Zusammenhang ebenfalls kritisch zu sehen. Dies müsste dann im konkreten Einzelfall betrachtet werden (Darstellung des Herstellers, von wo welche Daten hinfließen). Es muss der Datenfluss dargestellt werden, aus dem auch hervorgeht, wie die Datentrennung erfolgt.

Verarbeitung im Ausland – Oft gestellte Fragen aus Beratungsgesprächen

Für die Bereitstellung der Inhalte nutzen wir bisher private YouTube-Videos. Dabei werden von der App keine Daten des Nutzers an YouTube übermittelt, jedoch übermittelt der Nutzer dabei natürlich seine IP-Adresse an YouTube. Ist dies ein Problem?

Ja, aufgrund der übermittelten IP-Adresse.

Ein Versicherter hält sich bei Nutzung der App physisch in den USA auf. Durch seine Internetverbindung können ggf. personenbezogene Daten über US-amerikanische Server laufen. Welche Vorgaben gelten dann?

In diesem Fall gilt US-amerikanisches Recht. Das gilt auch für die Verarbeitung von personenbezogenen Daten. Dass dann Daten in die USA fließen, liegt nicht mehr im Verantwortungsbereich des Herstellers der DiGA.

Verarbeitung im Ausland – Oft gestellte Fragen aus Beratungsgesprächen

Ist die Nutzung von App Stores wie Apple Store oder Google Play Store vor dem Hintergrund der Vorgaben zulässig?

Vor dem Hintergrund der Zurverfügungstellung von Apps ist dies akzeptabel.

Ist eine Nutzung von Dienstleistern wie Google Analytics for Firebase oder Facebook Pixel mit US-amerikanischem Mutterkonzern über einen Opt-in-Mechanismus möglich?

In § 4 Absatz 3 der DiGAV ist nicht vorgesehen, dass die Verarbeitung in Drittstaaten nicht mehr verboten ist, wenn der Anwender hierzu seine Zustimmung gibt. Daher ist eine Patienteneinwilligung im Zusammenhang mit einer Datenverarbeitung in Ländern ohne Angemessenheitsbeschluss nicht zulässig.

1. Themenblock: Datenschutz

Weitere Gewährleistungsziele

Weitere Gewährleistungsziele – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 39 Datenschutz

Ist die Verkettung von personenbezogenen Daten über zwei oder mehr digitale Gesundheitsanwendungen hinweg technisch ausgeschlossen oder muss die betroffene Person für eine Verkettung von Daten über zwei oder mehr digitale Gesundheitsanwendungen hinweg eine explizite, gesondert eingeholte, informierte Einwilligung abgeben?

DiGAV, Anlage 1, Anforderung 40 Datenschutz

Ist sichergestellt, dass eine Offenbarung von Informationen der betroffenen Person oder über die betroffene Person für die Öffentlichkeit oder eine für die betroffene Person nicht eingrenzbare Personengruppe gar nicht oder immer nur infolge einer expliziten, aktiven Handlung der betroffenen Person erfolgt, der eine zielgruppengerechte Information über die Art der offenbarten Informationen und den möglichen Kreis der Empfänger zugrunde liegt?

Weitere Gewährleistungsziele – Lessons Learned

Hinweise zu DiGAV, Anlage 1, Anforderung 40 Datenschutz

Was hier beispielsweise gemeint ist:

- Chat-Funktion
- Forum

Der oder die Nutzenden muss vor der Verwendung informiert/gewarnt werden, dass eingegebene Informationen für andere einsehbar sein.

Anmerkung: Chat und Forum dürfen keine therapeutischen Aufgaben erfüllen!

1. Themenblock: Datenschutz

Sonstige eingereichte Fragen

Cookies
– Eingereichte Fragen

Gibt es genauere Vorgaben zur Verwendung von Cookies von Seiten des BfArM für DiGA (Einwilligung, Einstufung technisch notwendig, funktional...) bzw. wie werden diese im DiGA-Antragsverfahren geprüft?

Genaue Vorgaben gibt es hierzu nicht. Es gelten jedoch die Anforderungen der DSGVO und der DiGAV. Dies bedeutet u. a.

- die erlaubten Zwecke der Datenverarbeitung gemäß § 4 Absatz 2 DiGAV müssen beachtet werden
- Vorgaben gemäß den Orten der Datenverarbeitung müssen beachtet werden
- Vorgaben gemäß der Weitergabe von Daten an Dritte müssen beachtet werden

Speicherung von IP-Adressen – Eingereichte Fragen

Auf welcher Rechtsgrundlage ist die kurzzeitige Speicherung von IP-Adressen (z.B. 7 Tage) zum Zwecke der Nachverfolgbarkeit von Angriffen bzw. Ausübung, Geltendmachung oder Verteidigung von Rechtsansprüchen bei DiGA umsetzbar?

Der Hersteller kann versuchen, dies mit einem Verweis auf § 4 Absatz 2 Satz 1 Nummer 1 zu begründen. Dies müsste dann im Einzelfall geprüft werden.

1. Themenblock: Datenschutz

Weitere Fragen zu den bisherigen Themen

2. Themenblock: Datensicherheit

Informationssicherheits- und Servicemanagement

Informationssicherheits- und Servicemanagement – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 1 Datensicherheit

Hat der Hersteller der digitalen Gesundheitsanwendung ein Informationssicherheitsmanagementsystem (ISMS) gemäß ISO 27001 oder gemäß ISO 27001 auf der Basis von IT-Grundschutz (BSI-Standard 200-2: IT-Grundschutz-Methodik) umgesetzt und kann ab dem 1. April 2022 auf Verlangen des Bundesinstituts für Arzneimittel und Medizinprodukte ein entsprechendes anerkanntes Zertifikat vorlegen?

Informationssicherheits- und Servicemanagement – Lessons Learned

Hinweise DiGAV, Anlage 1, Anforderung 1 Datensicherheit

Anforderung gilt für den Hersteller der DiGA! Ein ISMS-Zertifikat des Dienstleisters oder der Sensorherstellers, dessen Sensor im Rahmen der DiGA verwendet wird ist nicht ausreichend.

DiGA im DiGA-Verzeichnis

Bei der Einreichung des ISMS-Zertifikats muss eine Anzeige einer wesentlichen Veränderung gestellt werden, da neben der Änderung im Verzeichnis das Zertifikat geprüft werden muss. Bei weiteren DiGA desselben Herstellers reicht nachfolgend dann die (formlose) Meldung einer redaktionellen Änderung.

DiGA im Antragsverfahren

Seit dem 01.04.2022 muss ein entsprechendes Zertifikat vorgewiesen werden können. Damit ist es Teil der formalen Prüfung und wird auch im Rahmen dieser Prüfung abgefragt. Ein Antrag ohne ISMS-Zertifikat gilt nicht als formal vollständig.

Informationssicherheits- und Servicemanagement – Oft gestellte Fragen aus Beratungsgesprächen

Muss ausschließlich der Hosting Anbieter der DiGA ein ISMS bzw. eine ISO 27001 Zertifizierung vorweisen oder ebenfalls der Hersteller und Inverkehrbringer im Sinne der MDR der DiGA ?

Der Hersteller der DiGA muss ein entsprechendes ISMS zertifizieren und das Zertifikat auf Verlangen des BfArM vorlegen können. Eine entsprechende Zertifizierung des Hosters ist nicht ausreichend.

Kann der Antrag zur vorläufigen Aufnahme ins DiGA-Verzeichnis gestellt werden, sobald das ISMS Audit erfolgreich war oder muss das finale Zertifikat vorliegen?
Das finale Zertifikat muss vorliegen, andernfalls ist ein Antrag nicht formal vollständig.

Bundesinstitut für Arzneimittel und Medizinprodukte

Informationssicherheits- und Servicemanagement – Oft gestellte Fragen aus Beratungsgesprächen

Wir haben ein zertifiziertes Informationssicherheitsmanagementsystem (ISMS) gemäß HITRUST. Gilt dies als vergleichbares System zur ISO 27000er-Reihe oder wird eine zusätzliche Zertifizierung benötigt?

Ein gemäß HITRUST zertifiziertes ISMS wird nicht entsprechend § 7 DiGAV von einer akkreditierten Stelle ausgestellt. Laut DiGAV Anlage 1 gibt es nur die Optionen eines Zertifikats gemäß ISO 27001 oder gemäß ISO 27001 auf der Basis von IT-Grundschutz (BSI-Standard 200-2: IT-Grundschutz-Methodik).

2. Themenblock: Datensicherheit

Verhinderung von Datenabfluss

Verhinderung von Datenabfluss – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 4 Datensicherheit

Hat der Hersteller der digitalen Gesundheitsanwendung sichergestellt, dass die Kommunikation der digitalen Gesundheitsanwendung mit anderen Diensten technisch soweit eingeschränkt ist, dass aus der digitalen Gesundheitsanwendung heraus keine ungewollte Datenkommunikation erfolgen kann, über die personenbezogene Daten versendet werden?

Bundesinstitut für Arzneimittel und Medizinprodukte

Verhinderung von Datenabfluss – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 5 Datensicherheit

Wird bei jeder über offene Netze stattfindenden Datenkommunikation zwischen verschiedenen Systembestandteilen der digitalen Gesundheitsanwendung zumindest eine Transportverschlüsselung gemäß des Mindeststandards des BSI zur Verwendung von Transport Layer Security (TLS) nach § 8 Absatz 1 Satz 1 des BSI-Gesetzes eingesetzt?

DiGAV, Anlage 1, Anforderung 6 Datensicherheit

Prüft die digitale Gesundheitsanwendung bei jedem Zugriff auf über das Internet aufrufbare Funktionalitäten der digitalen Gesundheitsanwendung die Authentizität der aufgerufenen Dienste, bevor personenbezogene Daten mit diesen Diensten ausgetauscht werden?

Verhinderung von Datenabfluss – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 7 Datensicherheit

Hat der Hersteller der digitalen Gesundheitsanwendung sichergestellt, dass die digitale Gesundheitsanwendung keine ungewollten Log- oder Hilfsdateien schreibt?

DiGAV, Anlage 1, Anforderung 8 Datensicherheit

Hat der Hersteller der digitalen Gesundheitsanwendung sichergestellt, dass die digitale Gesundheitsanwendung keine Fehlermeldungen ausgibt, die möglicherweise vertrauliche Informationen offenbaren?

Verhinderung von Datenabfluss – Oft gestellte Fragen aus Beratungsgesprächen

Anforderung Nr. 4: Was bedeutet hier *„keine ungewollte Datenkommunikation“* bzw. reicht eine Meldung bzw. ein deutlicher Hinweis dazu vor Nutzung der Export Funktion, um die Anforderung zu erfüllen?

Die Nutzung der Exportfunktion ist keine ungewollte Datenkommunikation. Eine ungewollte Datenkommunikation wäre es zum Beispiel, wenn sich ein durch die Kamera aufgenommenes Bild in der Bildergalerie wiederfinden würde.

2. Themenblock: Datensicherheit

Authentisierung

Authentisierung – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 10 Datensicherheit

Ist durch geeignete technische Maßnahmen sichergestellt, dass zur Authentisierung einer die digitale Gesundheitsanwendung nutzenden Person verwendete Daten niemals über ungesicherte Transportverbindungen ausgetauscht werden?

DiGAV, Anlage 1, Anforderung 11 Datensicherheit

Verwendet bzw. beinhaltet die digitale Gesundheitsanwendung eine zentrale Authentisierungskomponente, die mit etablierten Standardkomponenten umgesetzt wurde, die alleinig für die initiale Authentisierung zulässig ist und deren Vertrauenswürdigkeit durch Dienste der digitalen Gesundheitsanwendung verifizierbar ist?

DiGAV, Anlage 1, Anforderung 12 Datensicherheit

Erzwingt die digitale Gesundheitsanwendung, dass eine die digitale Gesundheitsanwendung nutzende Person die für ihre Authentisierung genutzten Daten nur ändern kann, wenn hierbei für die Prüfung der Authentizität dieser Person ausreichende Informationen beigegeben werden?

Bundesinstitut für Arzneimittel und Medizinprodukte

Authentisierung – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 9 Datensicherheit

Müssen sich alle die digitale Gesundheitsanwendung nutzenden Personen über eine dem Schutzbedarf der durch die digitale Gesundheitsanwendung verarbeiteten Daten angemessene Methode authentisieren, bevor Zugriffe auf über die digitale Gesundheitsanwendung zugängliche Daten erfolgen können?

DiGAV, Anlage 1, Anforderung 13 Datensicherheit

Sofern die Authentisierung unter Nutzung eines Passworts erfolgt:

- *Zwingt die digitale Gesundheitsanwendung alle die digitale Gesundheitsanwendung nutzenden Personen, sichere Passwörter gemäß einer Passwort-Richtlinie zu benutzen, die u. a. eine Mindestlänge für Passwörter vorgibt und Grenzwerte für fehlgeschlagene Anmeldeversuche definiert?*
- *Ist sichergestellt, dass Passwörter niemals im Klartext übertragen oder gespeichert werden?*
- *Wird das Ändern oder Zurücksetzen von Passwörtern protokolliert und wird die betroffene Person – sofern geeignete Kontaktdaten vorliegen – sofort über das Zurücksetzen oder Ändern des Passworts informiert?*

Authentisierung – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 14 Datensicherheit

Sofern die digitale Gesundheitsanwendung Authentisierungsdaten auf einem Endgerät oder in einer darauf befindlichen Softwarekomponente speichert: Wird die explizite Zustimmung der die digitale Gesundheitsanwendung nutzenden Person abgefragt („Opt-In“) und wird diese auf die Risiken der Funktion hingewiesen?

DiGAV, Anlage 1, Anforderung 15 Datensicherheit

Sofern Informationen zur Identität oder Authentizität der die digitale Gesundheitsanwendung nutzenden Person oder zur Authentizität von Komponenten der digitalen Gesundheitsanwendung über dedizierte Sitzungen („Sessions“) zwischen Komponenten der digitalen Gesundheitsanwendung geteilt werden:

Unter anderem:

- *Besitzen Sitzungen eine maximale Gültigkeitsdauer und werden inaktive oder unterbrochene Sitzungen automatisch nach einer bestimmten Zeit invalidiert?*

Bundesinstitut
für Arzneimittel
und Medizinprodukte

Authentisierung – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 15a Datensicherheit

Kann die digitale Gesundheitsanwendung bis spätestens zum 1. Januar 2023 eine Authentisierung von GKV-Versicherten als die die digitale Gesundheitsanwendung nutzenden Personen über die sichere digitale Identität nach § 291 Absatz 8 des Fünften Buches Sozialgesetzbuch unterstützen?

Authentisierung – Lessons Learned

Beispiel zu DiGAV, Anlage 1, Anforderungen 9, 13, 14 und 15 Datensicherheit

- ✓ Authentisierung der betroffenen Person beim Starten der DiGA durch ein Passwort gemäß einer Passwort-Richtlinie (z. B. OWASP Passwort-Richtlinie)
  - ➢ Ungeeignete Passwörter werden nicht akzeptiert
- ✓ Ändern und Zurücksetzen des Passworts innerhalb der DiGA möglich
  - ➢ Sofortige Information der betroffenen Person, falls Kontaktdaten vorhanden sind
- ✓ Speicherung der Authentisierungsdaten nur nach expliziter Einwilligung der betroffenen Person, z. B. im Einstellungs-Menü der DiGA
- ✓ Die DiGA verriegelt sich nach einer angemessenen Zeit
  - ➢ Risikobasiert bspw. für Apps: 30 Minuten / Webanwendungen: 20 Minuten

Authentisierung – Eingereichte Fragen

Passwortrichtlinie: NIST Guideline der Entropie?

Die Vorgabe lautet „*sichere Passwörter gemäß einer Passwort-Richtlinie*“. Hier kann sich an den „Digital Identity Guidelines“ des NIST, an Vorgaben des BSI oder auch an OWASP orientiert werden.

Wann ist mit ersten Informationen oder Spezifikationen von der gematik zum Thema digitale Identitäten zu rechnen, deren Implementierung ab 01.01.23 für DiGA verpflichtend ist?

Die Gespräche hierzu laufen noch, es kann hier noch keine Aussage getroffen werden. Sollte sich hier noch etwas kurzfristig ändern, wird dies in den FAQ nachgereicht.

Authentisierung – Eingereichte Fragen

2FA:

- **Wann z. B. bei jedem Login vs. bei Wechsel der IP-Adresse oder Lokation?**

Eine 2FA ist nach heutigem Stand nur bei DiGA mit sehr hohem Schutzbedarf notwendig. Hier muss eine neue Authentisierung bei jedem Neustart der Anwendung sowie nach Ablauf einer angemessenen Zeit der Nicht-Nutzung erfolgen. Bei einem Wechsel der IP-Adresse sollte ebenfalls eine neue Authentisierung erfolgen, sofern eine Risikobetrachtung dies als notwendig erachtet.

2FA:

- **Medien für 2FA: SMS vs E-Mail vs Device PPK**

Wird aktuell nur für DiGA mit sehr hohem Schutzbedarf gefordert. Beide Faktoren müssen verschieden sein.

Authentisierung – Eingereichte Fragen

Schutz des Zugriffs auf Android/iOS Apps und Session-Logout: Welche Anforderungen bestehen diesbezüglich für DiGAs mit „hohem Schutzbedarf“? Ist beispielsweise folgendes Setup konform?

- **Erstmalige Anmeldung mit E-Mail-Adresse (inkl. Verifikation) und sicherem Passwort**
- **Schutz vor unerlaubter Nutzung durch Auswahl von 4-stelliger PIN (alternativ: biometrisches Verfahren, das durch Smartphone zur Verfügung gestellt wird)**
- **PIN-Eingabe bei jedem Start der App und nach x Minuten Inaktivität**
- **Opt-out der PIN-Überprüfung mit expliziter Warnung der Sicherheitsrisiken möglich.**

Aktuell wäre dies so möglich.

Authentisierung – Eingereichte Fragen

Ist eine Invalidierung der Session nach einer gewissen Zeit bei einer iOS/Android App notwendig (token-based authentication) oder reicht hier der zuvor beschriebene Zugriffsschutz aus?

Auch die Backend-Session muss nach einer gewissen Zeit einen Timeout haben.

2. Themenblock: Datensicherheit

Weitere Fragen zu den bisherigen Themen

2. Themenblock: Datensicherheit

Einbinden von Daten und Funktionen

Einbinden von Daten und Funktionen – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 21 Datensicherheit

Kann sich der Versicherte ausschließlich innerhalb der Vertrauensdomäne der digitalen Gesundheitsanwendung bewegen bzw. können aus der digitalen Gesundheitsanwendung heraus nur vertrauenswürdige, durch den Hersteller der digitalen Gesundheitsanwendung geprüfte externe Inhalte genutzt werden und wird der Versicherte in diesem Fall informiert, wenn die Vertrauensdomäne der digitalen Gesundheitsanwendung verlassen wird?

DiGAV, Anlage 1, Anforderung 22 Datensicherheit

Sofern die digitale Gesundheitsanwendung der nutzenden Person den Upload von Dateien erlaubt: Ist diese Funktion so weit wie möglich eingeschränkt (z. B. Ausschließen aktiver Inhalte), findet eine Sicherheitsprüfung der Inhalte statt und ist sichergestellt, dass Dateien nur im vorgegebenen Pfad gespeichert werden können?

Einbinden von Daten und Funktionen – Lessons Learned

Beispiel zu DiGAV, Anlage 1, Anforderung 21 Datensicherheit

- ✓ Gibt es innerhalb der DiGA externe Links, die aus der DiGA herausführen?
  - ➢ Falls ja: Information der Versicherten erforderlich

www.beispiel.de
[externer Link]

2. Themenblock: Datensicherheit

Regelmäßige und sichere Aktualisierung

Regelmäßige und sichere Aktualisierung – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 26 Datensicherheit

Informiert der Hersteller die betroffene Person (z. B. über Push-Mechanismen oder vor dem Start der digitalen Gesundheitsanwendung), wenn ein sicherheitsrelevantes Update der digitalen Gesundheitsanwendung zur Installation bereitgestellt oder durchgeführt wurde?

Bundesinstitut für Arzneimittel und Medizinprodukte

Regelmäßige und sichere Aktualisierung – Lessons Learned

Beispiel zu DiGAV, Anlage 1, Anforderung 26 Datensicherheit

- ✓ Liegt ein sicherheitsrelevantes Update der DiGA zur Installation vor oder wurde durchgeführt?
  - ➢ Falls ja: Versicherte sind vor dem Start der DiGA zu informieren

2. Themenblock: Datensicherheit

Sichere Deinstallation

Sichere Deinstallation – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 27 Datensicherheit

Werden bei Deinstallation der digitalen Gesundheitsanwendung alle auf IT-Systemen in der Verfügung der betroffenen Person gespeicherten, durch die digitale Gesundheitsanwendung angelegten Daten und Dateien – einschließlich Caches und temporärer Dateien – gelöscht?

Sichere Deinstallation – Lessons Learned

Hinweis zu DiGAV, Anlage 1, Anforderung 27 Datensicherheit

- Anforderung gilt für digitale Gesundheitsanwendungen in Form einer App und nicht für rein webbasierte Anwendungen

2. Themenblock: Datensicherheit

Penetrationstests

Penetrationstests – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 32a Datensicherheit

Hat der Hersteller der digitalen Gesundheitsanwendung für die im Verzeichnis nach § 139e Absatz 1 des Fünften Buches Sozialgesetzbuch aufzunehmende Version der digitalen Gesundheitsanwendung – einschließlich aller Backend-Komponenten – einen Penetrationstest durchgeführt, der dem vom Bundesamt für Sicherheit in der Informationstechnik empfohlenen Durchführungskonzept für Penetrationstests folgt, und – soweit die Anwendbarkeit gegeben ist – auch die jeweils aktuellen OWASP Top-10 Sicherheitsrisiken berücksichtigt, und kann er auf Nachfrage entsprechende Nachweise für die Durchführung der Penetrationstests und die Behebung der dabei gefundenen Schwachstellen vorlegen?

Penetrationstests – Lessons Learned

Information zu DiGAV, Anlage 1, Anforderung 32a Datensicherheit

Penetrationstests = ermöglichen die Nachbildung möglicher Angriffsmuster und können so dazu beitragen, Sicherheitslücken aufzudecken

- Anforderung wurde mit dem DVPMG für alle DiGA in die DiGAV aufgenommen
- Nachweis über die Durchführung eines Penetrationstests muss in der formalen Prüfung vorliegen, sonst wird dieser nachgefordert
  - muss sich auf die Version der antragsgegenständlichen Anwendung beziehen und alle Komponenten berücksichtigen
  - Basis: Durchführungskonzept für Penetrationstests des BSI und aktueller *OWASP mobile security testing Guide*
- Penetrationstest ist anforderungsbezogen zu wiederholen

Bundesinstitut für Arzneimittel und Medizinprodukte

2. Themenblock: Datensicherheit

Nutzung von Sensoren und externen Geräten

Nutzung von Sensoren und externen Geräten – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 33 Datensicherheit

Sofern die digitale Gesundheitsanwendung direkt auf Sensoren eines mobilen Endgeräts und/oder externe Hardware (z. B. körpernahe Sensorik) zugreift:

- *Hat der Hersteller der digitalen Gesundheitsanwendung festgelegt, unter welchen Rahmenbedingungen Sensoren oder angebundene Geräte installiert, aktiviert, konfiguriert und verwendet werden können und wird das Bestehen dieser Rahmenbedingungen vor der Ausführung entsprechender Funktionalitäten soweit als möglich sichergestellt?*
- *Stellt die digitale Gesundheitsanwendung sicher, dass Sensoren und angebundene Geräte bei der Installation bzw. erstmaligen Aktivierung für die digitale Gesundheitsanwendung in eine Grundeinstellung versetzt werden, die einer dokumentierten Sicherheitsrichtlinie entspricht?*
- *Kann der Versicherte von der digitalen Gesundheitsanwendung direkt angesteuerte Sensoren und Geräte in eine Grundeinstellung zurücksetzen, die einer dokumentierten Sicherheitsrichtlinie entspricht?*

Ist ein Datenaustausch zwischen der digitalen Gesundheitsanwendung und direkt angesteuerten Sensoren oder Geräten erst dann möglich, wenn die Installation und Konfiguration der Sensoren bzw. Geräte vollständig abgeschlossen ist?

Nutzung von Sensoren und externen Geräten – Rechtliche Vorgaben

DiGAV, Anlage 1, Anforderung 34 Datensicherheit

Sofern die digitale Gesundheitsanwendung Daten mit externer Hardware (z. B. körpernahe Sensorik) austauscht:

- *Sind die Abläufe zur Installation, Konfiguration, Aktivierung und Deaktivierung dieser Hardware zielgruppengerecht beschrieben und soweit als möglich gegen Fehlbedienungen gesichert?*
- *Erfolgt eine wechselseitige Authentisierung zwischen der digitalen Gesundheitsanwendung und externer Hardware?*
- *Werden Daten zwischen der digitalen Gesundheitsanwendung und externer Hardware nach einem initialen Handshake nur noch verschlüsselt ausgetauscht?*
- *Ist sichergestellt, dass bei einer Deinstallation der digitalen Gesundheitsanwendung oder bei einer Beendigung von deren Nutzung alle auf externer Hardware gespeicherten Daten gelöscht werden?*
- *Hat der Hersteller der digitalen Gesundheitsanwendung dokumentiert, wie eine angebundene Hardware sicher deaktiviert werden kann, so dass keine Daten verloren gehen und keine sensiblen Daten auf dem Gerät verbleiben?*

Nutzung von Sensoren und externen Geräten – Lessons Learned

Information zu DiGAV, Anlage 1, Anforderung 33 Datensicherheit

- ✓ Sensoren lassen sich in eine Grundeinstellung zurücksetzen
- ✓ erst nach der Installation und Konfiguration der Sensoren bzw. Geräte ist ein Datenaustausch zwischen DiGA und Sensoren bzw. Geräten möglich

Information zu DiGAV, Anlage 1, Anforderung 34 Datensicherheit

- ✓ Beschreibung der Installation, Konfiguration, Aktivierung und Deaktivierung der externen Hardware & leichte Durchführbarkeit dieser Schritte
- ✓ Löschung aller auf der externen Hardware gespeicherten Daten sobald die DiGA deinstalliert oder die Nutzung beendet wird
- ✓ Wechselseitige Authentisierung DiGA ↔ externe Hardware

Bundesinstitut für Arzneimittel und Medizinprodukte

Nutzung von Sensoren und externen Geräten – Eingereichte Fragen

Unter welchen Voraussetzungen ist die Nutzung der Google Fit SDK möglich? (z.B. rein lesender, nicht schreibender Zugriff)

Es muss sichergestellt werden, dass keine personenbezogenen Daten (auch keine IP-Adresse) an Google abfließen kann. Dies müsste dann im konkreten Einzelfall betrachtet werden (Darstellung des Herstellers, von wo welche Daten hinfließen). Es muss der Datenfluss dargestellt werden, aus dem auch hervorgeht, wie die Datentrennung erfolgt.

Nutzung von Sensoren und externen Geräten – Oft gestellte Fragen aus Beratungsgesprächen

Eine sinnvolle Ergänzung der App wäre die automatische Datenübertragung von Messgeräten in der App. Was würde dies in Bezug auf die Anforderungen der Datensicherheit bedeuten?

Die Datensicherheit für die in der App gespeicherten Daten sollte unabhängig von der Art und Weise sein, wie die Daten in die App gelangt sind. Der Datentransfer zwischen Smartphone und Messgerät muss Anforderungen 33 und 34 zur Datensicherheit in Anlage 1 der DiGAV erfüllen.

Nutzung von Sensoren und externen Geräten – Oft gestellte Fragen aus Beratungsgesprächen

Eine Anforderung der Frage 34 lautet: „Werden Daten zwischen der digitalen Gesundheitsanwendung und externer Hardware nach einem initialen Handshake nur noch verschlüsselt ausgetauscht?“. Ist Bluetooth verschlüsselbar bzw. gilt normale Bluetooth Kommunikation als verschlüsselt?

Bluetooth kann verschlüsselt betrieben werden. Für Bluetooth Low Energy ist Verschlüsselung über den Modus und das Level auswählbar. Weitere Informationen: https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/

2. Themenblock: Datensicherheit

Sonstige eingereichte Fragen

Schutzbedarf – Eingereichte Fragen

Welche Erfahrungen gibt es zum Schutzbedarf von DiGAs? Gibt es hier genauere BfArM-Vorgaben insbesondere zur Feststellung "hoch"/"sehr hoch", außer, dass eine Schutzbedarfsanalyse gemacht werden muss und dann entsprechend Anhang I und II beachtet werden müssen?

Die Einordnung ist durch den Hersteller selbst durchzuführen. Für die Einordnung des Schutzbedarfs gelten die Vorgaben aus dem *BSI-Standard 200-2*. In Kapitel 8.2 dieses Standards ist das Vorgehen beschrieben, wie man den Schutzbedarf einer DiGA feststellen kann. Tabelle 4 auf Seite 107 listet Kriterien für einen sehr hohen Schutzbedarf auf:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html
Die Schutzbedarfsanalyse sollte zudem eine Datenschutzfolgenabschätzung beinhalten.

Technisch-organisatorische Maßnahmen – Eingereichte Fragen

Erfolgt bzw. wie erfolgt die Prüfung der technisch-organisatorischen Maßnahmen (TOM) im Zuge des DiGA-Fast-Track Verfahrens von Seiten des BfArMs?

Im Einzelfall kann das BfArM Unterlagen einfordern, wenn Zweifel in der Einhaltung der Vorgaben bestehen.

2. Themenblock: Datensicherheit

Weitere Fragen zu den bisherigen Themen

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Bundesinstitut für Arzneimittel und Medizinprodukte
Kurt-Georg-Kiesinger-Allee 3
53175 Bonn

Ansprechpartner:
Fachgebiet DiGA-Fast-Track
diga@bfarm.de
Tel. +49 (0) 228 99 307 5989

www.bfarm.de
www.bfarm.de/innovation
www.bfarm.de/diga
www.bfarm.de/digitalfuture

Zertifikat seit 2010
audit berufundfamilie

Bundesinstitut
für Arzneimittel
und Medizinprodukte