Deutsche Stiftung für Recht und Informatik

GESUNDHEITSAPPS AUF REZEPT

Anforderungen an den Datenschutz und die Datensicherheit

Dr. Natallia Karniyevich
Bird & Bird LLP

Herbstakademie 2021

Agenda

1. Was ist eine App auf Rezept/eine DiGA?
2. Datenschutzrechtliche Anforderungen für die Aufnahme in das DiGA-Verzeichnis
3. IT-Sicherheitsanforderungen
4. Verwendung personenbezogener Daten im Rahmen einer DiGA
5. Dos and Don'ts für DiGA-Hersteller, Distributoren sowie Nutzer

Was ist eine App auf Rezept/eine DiGA?

DiGA sind nach der Legaldefinition des § 33a Abs. 1 S. 1 SGB V

„Medizinprodukte niedriger Risikoklasse, deren Hauptfunktion wesentlich auf digitalen Technologien beruht und die dazu bestimmt sind, bei den Versicherten oder in der Versorgung durch Leistungserbringer die Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder die Erkennung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen zu unterstützen.“

Datenschutzrechtliche Anforderungen für die Aufnahme in das DiGA-Verzeichnis

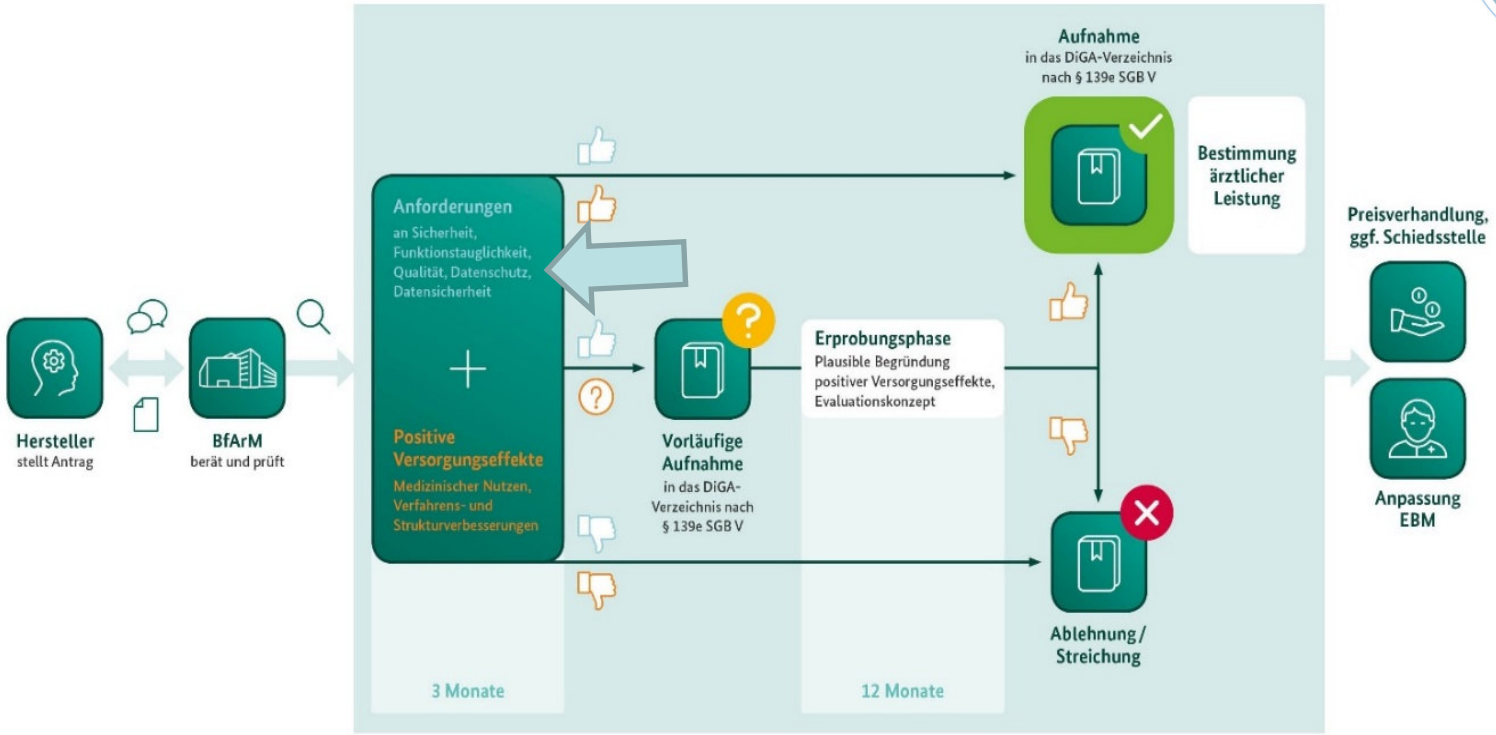
Datenschutzrechtliche Anforderungen für die Aufnahme in das DiGA-Verzeichnis

- Jede DiGA muss ein **Prüfverfahren** beim **Bundesinstitut für Arzneimittel und Medizinprodukte** (BfArM) erfolgreich durchlaufen, um in dem Verzeichnis erstattungsfähiger DiGA (DiGA-Verzeichnis) gelistet zu werden – **geprüft werden** hierbei auch **datenschutzrechtliche Vorgaben**.

- Neben den allgemeinen datenschutzrechtlichen Vorgaben aus der DSGVO (und ggf. weiteren anwendbaren datenschutzrechtlichen Vorschriften) sind **für DiGA speziell die Vorgaben aus der Digitale Gesundheitsanwendungen-Verordnung** („*DiGAV*“) zu beachten.

- **BfArM-Leitfaden**: Die DiGAV **"konkretisiert und ergänzt"** die in der DSGVO festgelegten Anforderungen.

Datenschutzrechtliche Anforderungen für die Aufnahme in das DiGA-Verzeichnis – Übersicht Prüfverfahren



Quelle: Bundesinstitut für Arzneimittel und Medizinprodukte

Datenschutzrechtliche Anforderungen für die Aufnahme in das DiGA-Verzeichnis

- Datenschutzrechtliche Anforderungen der DiGA müssen im Rahmen der Prüfung **dem BfArM gegenüber dargelegt** werden.
- **Grundlage** hierfür ist eine vom Anbieter der DiGA **auszufüllende Checkliste** (*Anlage 1 der DiGAV*) – Checkliste stellt zugleich eine Art **Self-Assessment Katalog** für Anbieter der DiGA dar.
- Ausgefüllte Checkliste ist **bei Antragsstellung mit einzureichen** und wird als Grundlage der Prüfung der Anforderungen zum Datenschutz herangezogen.

Datenschutzrechtliche Anforderungen für die Aufnahme in das DiGA-Verzeichnis

Nr.	Themenfeld	Anforderung	zutreffend	nicht zutreffend	zulässige Begründung für „nicht zutreffend"
Datenschutz					
1.	Datenschutz-Grundverordnung als anzuwendendes Recht	Die Verarbeitung personenbezogener Daten durch die digitale Gesundheitsanwendung und deren Hersteller unterfällt der Verordnung (EU) 2016/679 sowie ggf. weiteren Datenschutzregelungen.			
2.	Einwilligung	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?			Es wird keine Einwilligung eingeholt, da der Zweck der Verarbeitung aus einer rechtlichen Verpflichtung des Herstellers der digitalen Gesundheitsanwendung resultiert.
3.	Einwilligung	Erfolgt die Abgabe von Einwilligungen und Erklärungen der betroffenen Person durchgängig ausdrücklich, d. h. durch eine aktive, eindeutige Handlung der betroffenen Person?			Es wird keine Einwilligung eingeholt, da der Zweck der Verarbeitung aus einer rechtlichen Verpflichtung des Herstellers der digitalen Gesundheitsanwendung resultiert.
4.	Einwilligung	Kann die betroffene Person erteilte Einwilligungen einfach, barrierefrei, jederzeit und auf einem einfach verständlichen Weg mit Wirkung für die Zukunft widerrufen?			Es wird keine Einwilligung eingeholt, da der Zweck der Verarbeitung aus einer rechtlichen

Datenschutzrechtliche Anforderungen für die Aufnahme in das DiGA-Verzeichnis

- Der Hersteller muss in Checkliste **40 Aussagen zu der Erfüllung der Anforderungen** zum **Datenschutz** nach *§ 4 DiGAV* und den allgemeinen Anforderungen nach der DSGVO treffen.
- Unter anderem Fragen zur
  - Einholung der **Einwilligung**
  - Datenverarbeitung **außerhalb Deutschlands**
  - Einhaltung der **Datenminimierung**
  - Gewährleistung der **Informationspflichten**
  - Durchführung einer **Datenschutzfolgenabschätzung**
  - Meldung von Verletzungen des Schutzes personenbezogener Daten („**Data Breach**“)

Exkurs: Datenverarbeitung außerhalb Deutschlands

Beschränkung des Orts der Datenverarbeitung (*§ 4 Abs. 3 DiGAV*) auf die Verarbeitung:

- im **Inland** (Deutschland)
- in einem **Mitgliedsstaat der EU** oder in einem diesem nach *§ 35 Abs. 7 SGB I* **gleichgestellten Staat** (EWR + Schweiz) oder
- in einem Staat, für welchen ein **Angemessenheitsbeschluss** gem. *Art. 45 DSGVO* vorliegt (nur wenige Länder: z.B. Argentinien, Israel, Japan, Kanada (teilweise), Neuseeland, Schweiz).

Exkurs: Datenverarbeitung außerhalb Deutschlands

Beschränkung des Orts der Datenverarbeitung (*§ 4 Abs. 3 DiGAV*) auf die Verarbeitung:

- **Nicht zulässig:** Verarbeitung von personenbezogenen Daten außerhalb der EU auf Basis von *Art. 46 DSGVO* (z.B. EU Standardvertragsklauseln) oder *Art. 47 DSGVO* (Binding Corporate Rules)

- **Vereinbarkeit** dieser einschränkenden Regelung mit dem **Unionsrecht**?

IT-Sicherheitsanforderungen

IT-Sicherheitsanforderungen

- **Konkrete Anforderungen** an die **Datensicherheit** als Voraussetzung für eine Aufnahme ins DiGA-Verzeichnis (*Anlage 1 - Checkliste „Datensicherheit“*)
- **Ziel**: Schutz der **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** sämtlicher über eine DiGA verarbeiteten Daten
- **Sicherheit** als ein sich in der ständigen Entwicklung befindender **Prozess**

IT-Sicherheitsanforderungen

- **Kriterien zur Datensicherheit**, die von den DiGA-Herstellern beachtet werden müssen:
  - Basisanforderungen, die für alle DiGA gelten
  - Zusatzanforderungen bei DiGA mit sehr hohem **Schutzbedarf**: müssen zusätzlich zu den Basisanforderungen nur von DiGA erfüllt werden, für die im Rahmen der geforderten **Schutzbedarfsanalyse ein sehr hoher Schutzbedarf** festgestellt wurde.

IT-Sicherheitsanforderungen – Basisanforderungen, die für alle DiGA gelten

- Müssen von den DiGA **ausnahmslos erfüllt** werden oder aufgrund einer Nicht-Anwendbarkeit für bestimmte Arten von DiGA **„nicht zutreffend“** sein
- **Ziel**: **Sicherheit als Prozess** beim Hersteller zu verankern
- Betrifft u.a. folgende **Themenfelder**:
  - **Informationssicherheits-** und **Service-Management** ➔ Schutzbedarfsanalyse; Release-, Change- und Configuration-Management
  - Nutzung von **Fremdsoftware**

IT-Sicherheitsanforderungen – Zusatzanforderungen bei DiGA mit sehr hohem Schutzbedarf

- **Sieben zusätzliche Anforderungen im Bereich**
  - **Verschlüsselung** gespeicherter Daten,
  - **Authentisierung**,
  - Ergreifen der Maßnahmen gegen **DoS** und **DDoS** sowie
  - Vorkehrungen im Zusammenhang mit **eingebetteten Webservern**

Verwendung personenbezogener Daten im Rahmen einer DiGA

Verwendung personenbezogener Daten im Rahmen einer DiGA – Rechtliche Grundlagen: Einwilligung

- Anforderungen an eine **Einwilligung als Grundlage** für die Verarbeitung personenbezogener Daten im Rahmen einer DiGA, *§ 4 Abs. 2 S. 1 DiGAV*:
  - ausdrücklich
  - ausschließlich **zu begrenzten**, in *§* 4 Abs. 2 S. 1 DiGAV abschließend aufgeführten **Zwecken**
- allgemeine Anforderungen
  - **freiwillig, informiert**, für den **bestimmten** Fall, **widerruflich**
  - muss **vor** der Erfassung von personenbezogenen Daten eingeholt werden

Verwendung personenbezogener Daten im Rahmen einer DiGA – Rechtliche Grundlagen: Einwilligung

- **Begrenzung der Einholung einer Einwilligung auf bestimmte Zwecke:**
  - **Nr. 1: bestimmungsgemäßer Gebrauch** der DiGA durch die Nutzer: Datenerhebung und -Verarbeitung, die erforderlich ist, um die DiGA entsprechend ihrem Verwendungszweck im Rahmen der Krankenbehandlung einzusetzen.
  - **Nr. 2: Nachweis positiver Versorgungseffekte** im Rahmen einer Erprobung nach *§ 139e Abs. 4 SGB V*: Zum Nachweis der proklamierten positiven Versorgungseffekte bei einer vorläufigen Aufnahme in das DiGA-Verzeichnis.

Verwendung personenbezogener Daten im Rahmen einer DiGA – Rechtliche Grundlagen: Einwilligung

- **Begrenzung der Einholung einer Einwilligung auf bestimmte Zwecke:**
  - **Nr. 3: Nachweisführung bei Vereinbarungen** *nach § 134 Abs.1 Satz 3 SGB V:* Diese Regelung fordert für die Preisvereinbarungen zwischen Krankenkassen und DiGA-Herstellern **erfolgsabhängige Preisbestandteile** ein.

    ➔ Die hierfür **notwendigen Daten** dürfen (Kennzahlen des Nutzungserfolgs wie z.B. niedrige Abbrecherquote) auf Grundlage der Einwilligung verarbeitet werden, damit diese in die **Kostenerstattung** einberechnet werden können.

  - **Nr. 4: Dauerhafte Gewährleistung** der technischen Funktionsfähigkeit, der Nutzerfreundlichkeit und der Weiterentwicklung der DiGA.

Verwendung personenbezogener Daten im Rahmen einer DiGA – (Un-)Zulässige Zwecke

- Eine von der betroffenen Person eingeholte **ausdrückliche Einwilligung**, über die eine **Verarbeitung von Gesundheitsdaten** zu **anderen als** den oben genannten Zwecken legitimiert werden soll, ist **nicht zulässig**! (vgl. *§ 4 Abs. 4 S. 1 DiGAV)*

- Beispiele für Zwecke:
  - **Werbung**: ausdrücklich **ausgeschlossen**, *§ 4 Abs. 4 S. 1 DiGAV*.
  - **Weiterentwicklung**: ausdrücklich **zulässig**, *§ 4 Abs. 2 S. 1 Nr. 4 DiGAV*.
  - **Analyse**: **zulässig, soweit** die Analyse wiederum zulässigen Zweck verfolgt, namentlich der dauerhaften Gewährleistung der technischen **Funktionsfähigkeit,** der **Nutzerfreundlichkeit** und der **Weiterentwicklung**, *§ 4 Abs. 2 S. 1 Nr. 4 DiGAV*.

Verwendung personenbezogener Daten im Rahmen einer DiGA – (Un-)Zulässige Zwecke

- **Folgen für AI/Machine Learning/Data Analytics:**
  - **Zulässig (mit Einwilligung)**, wenn es zulässigem Zweck, insbesondere **Weiterentwicklung** gilt ("R&D")
  - Reine **Sales Optimierung problematisch**
  - Das **Anzeigen von Nutzerfragebögen über die DiGA** zur Erhebung und anschließenden Verarbeitung von Rückmeldungen zur Nutzererfahrung oder zu möglichen technischen Problemen: zulässig, *§ 4 Abs. 2 S. 1 Nr. 4 DiGAV*.
  - **Umfassendes Tracking** der Nutzeraktivitäten: **nicht** zulässig.
  - **„Bezahlung" von Angeboten** innerhalb einer DiGA durch die **Bereitstellung von Daten**: wohl nicht zulässig.

Verwendung personenbezogener Daten im Rahmen einer DiGA – Zusammenfassung der Zwecke in einer Einwilligung

- Gemäß dem *EG 32* und *EG 43 DSGVO* sowie den Leitlinien des *EDSA*: Bei einem Bündel an Verarbeitungszwecken soll für jeden Zweck eine *separate Einwilligung* eingeholt werden.
- Sonderregelung für DiGA in *§ 4 Abs. 2 S. 2 DiGAV*:

"Die Einwilligung zu der **Datenverarbeitung nach Satz 1 Nummer 4** [Dauerhafte Gewährleistung der technischen Funktionsfähigkeit, der Nutzerfreundlichkeit und der Weiterentwicklung der DiGA] **ist getrennt von einer Einwilligung** in die Datenverarbeitung für **Zwecke nach *Satz 1 Nummer 1 bis 3***

- ➔ Nr. 1: **bestimmungsgemäßer Gebrauch** der DiGA durch die Nutzer;
- ➔ Nr. 2: Nachweis **positiver Versorgungseffekte** im Rahmen einer Erprobung nach *§ 139e Abs. 4 SGB V;*
- ➔ *Nr. 3*: **Nachweisführung bei Vereinbarungen** nach *§ 134 Abs. 1 Satz 3 SGB V*]

einzuholen."

Verwendung personenbezogener Daten im Rahmen einer DiGA – Gesetzliche Erlaubnistatbestände

- Datenverarbeitung kann **weiterhin auf gesetzliche Erlaubnistatbestände** gestützt werden, die sich aus anderen Vorschriften außerhalb der DiGAV ergeben.
- Solche **Erlaubnistatbestände sind jedoch im Bereich von Gesundheitsdaten** für kommerzielle Anbieter **beschränkt**, sodass oft nur die Einwilligung zu den oben genannten begrenzten Zwecken bleibt.
- Zum Beispiel:
  - *§ 302 SGB V*: **Abrechnung des DiGA-Herstellers** gegenüber der **Krankenkasse**
  - *Art. 9 Abs. 2 h) DSGVO / § 22 Abs. 1 Nr. 1 b) BDSG*: Verarbeitung zu Zwecken der Gesundheitsvorsorge
  - *§ 27 Abs. 1 BDSG*: Verarbeitung zu Zwecken der wissenschaftlichen Forschung

Dos and Don’ts für Hersteller, Distributoren und Nutzer

Dos and Don’ts für Hersteller, Distributoren und Nutzer

- **Dos:**
  - **Privacy by Design**-Gedanke: erst Vorgaben prüfen, dann implementieren;
  - Genau prüfen, auf welche **Rechtsgrundlagen** Verarbeitungstätigkeiten im Zusammenhang mit der DiGA jeweils gestützt werden können;
  - Bei der Entwicklung einen entsprechenden **Einwilligungsmechanismus** im Hinblick auf die Vorgaben der DiGAV vorsehen und implementieren;
  - Allgemeine **Anforderungen** an eine **Einwilligung** nach der DSGVO beachten;
  - **Datenschutz-Folgenabschätzung** durchführen;
  - Alle für den Hersteller der DiGA tätige Personen auf **Verschwiegenheit** verpflichten;
  - **Rechte der DiGA-Nutzer gewährleisten;**
  - Anforderungen an die **Verarbeitung außerhalb Deutschlands** (auch bei Einschaltung von Auftragsverarbeitern) beachten;
  - Bei Einbindung externer Dienstleister: **Auftragsverarbeitungsverträge.**

Dos and Don’ts für Hersteller, Distributoren und Nutzer

- Don'ts
  - In-App Verarbeitung der DiGA-Daten zu **Werbezwecken**;
  - **Verarbeitung** von personenbezogenen Daten **außerhalb des EWR** auf Basis *von Art. 46, 47 DSGVO* (z.B. EU Standard-vertragsklauseln oder Binding Corporate Rules);
  - **Nicht-zweckgebundene Verarbeitung** von personenbezogenen Daten; **keine Trennung von Daten**, die für verschiedene Zwecke (bestimmungsgemäßer Gebrauch/ Leistungsabrechnung) verarbeitet werden;
  - Verarbeitung von Daten **„auf Vorrat“** ohne Anwendung eines (nachvollziehbaren) Löschkonzepts;
  - **Unverschlüsselte** bzw. **nicht dem Stand der Technik** entsprechende Übermittlung von Gesundheitsdaten.

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Natallia Karniyevich
Associate
Tel: +4921120056254
natallia.karniyevich@twobirds.com