Bird & Bird & DiGA

Anforderungen an den Datenschutz und die Datensicherheit von DiGA

Fachwebinar am 20. Mai 2020, 16:00 Uhr

Unsere Referenten

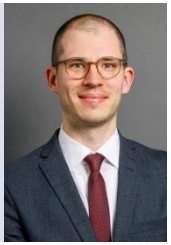
Bird & Bird LLP, Standort Düsseldorf
Schwerpunkt: Tech & Comms

Dr. Fabian Niemann
Partner
Tel:+4921120056254
fabian.niemann@twobirds.com

Lennart Schüßler
Partner
Tel: +4921120056377
lennart.schuessler@twobirds.com

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

Oliver Schmidt-Prietz, LL.M.
Associate
Tel: +4921120056377
oliver.schmidt-prietz@twobirds.com



Bird & Bird

Wir freuen uns auf Ihre Fragen!

Sie können Ihre Fragen entweder mündlich ("*Raise hand*") oder schriftlich im Chat stellen. Dabei können Sie entscheiden, ob Sie uns die Frage "privat" ("*send to host*") oder in die Runde ("*send to everyone*") stellen möchten.

Unterstützen Sie uns dabei, eine ruhige Geräuschkulisse zu ermöglichen!

Für eine optimale Akustikqualität achten Sie bitte darauf, dass Ihr Mikrofon auf "Mute" gestellt ist.

Bird & Bird

Willkommen zu unserem Webinar

Agenda

1. Privacy by Design: Was müssen die App-Hersteller beachten?
2. Datenschutzrechtliche Anforderungen für die Aufnahme in das DiGA-Verzeichnis
3. Verwendung personenbezogener Daten im Rahmen einer DiGA
4. IT-Sicherheitsanforderungen
5. Dos and Don'ts für DiGA-Hersteller, Distributoren sowie Nutzer

Bird & Bird

Privacy by Design: Was müssen die App-Hersteller beachten?

Bird & Bird

Privacy by Design

Was meint Privacy by Design?

- **Privacy by Design:** Datenschutz durch Technikgestaltung (*Art. 25 DSGVO*)
  - Verantwortliche **sollen frühzeitig organisatorische** und **technische Maßnahmen** treffen, die darauf ausgerichtet sind, **Datenschutzgrundsätze** (z.B. Datenminimierung) **bereits bei der Planung und technischen Gestaltung** unternehmensinterner Prozesse / Produkten / Dienstleistungen wirksam umzusetzen und den **Anforderungen der Datenschutzgrundverordnung (DSGVO)** genügen.

- **Allgemeiner Grundsatz - keine Konkretisierung, vielmehr:**

  "**Unter Berücksichtigung** des Stands der Technik, der **Implementierungskosten** und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie [...] Eintrittswahrscheinlichkeit und Schwere der [...] verbundenen Risiken für [...] natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen [...]." (*Art. 25 Abs. 1 DSGVO*)

- Auch DiGA müssen **schutzbedarfs- bzw. risikoorientiert** konzipiert und technisch umgesetzt werden.

Bird & Bird

Privacy by Design

Was heißt das für DiGA (Apps)?

- **Informationspflichten/Betroffenenrechte:**
  - Enthält Datenschutzerklärung alle wesentlichen Informationen (Katalog in *Art. 13/14 DSGVO*) für DiGA?
  - Sind Infos einfach in der App/über Website auffindbar (z.B. Menüpunkt „Datenschutz“)?
    ➔ Nutzer muss **vor Download/Nutzung** und **jederzeit Informationen/DS-Erklärung** einsehen können.
  - Können **Betroffenenrechte** (z.B. Auskunft, Löschung) organisatorisch und technisch wirksam umgesetzt werden?
    ➔ Gewährleistung der Rechte setzt **interne Organisation** (Richtlinien) und entsprechende technische Implementierung/Umsetzung voraus
    ➔ z.B. können Daten **effizient gelöscht** werden?

Bird & Bird

Privacy by Design

Was heißt das für DiGA (Apps)?

- **Zweckgebundene und nur erforderliche Datenverarbeitung sowie Datenübermittlung:**
  - Welche (Gesundheits-)Daten werden zu welchem **Zweck**, auf welcher **Rechtsgrundlage** und wie lange (abhängig vom Zweck) gespeichert?
    ➔ Nur für den jeweiligen Zweck erforderliche Daten dürfen zweckgebunden, auf Grund einer **vorher** festgelegten Rechtsgrundlage verarbeitet/gespeichert/ übermittelt werden.

  - **Bestimmungsgemäßer Gebrauch der DiGA**
    ➔ Analyse, welche **Daten hierfür zweckgebunden verarbeitet** werden dürfen
    ➔ Welche Daten dürfen für andere Zwecke, z.B. Produktverbesserung/Analyse verarbeitet werden (sind hier ggf. anonyme Daten ausreichend)?

Bird & Bird

Privacy by Design

Was heißt das für DiGA (Apps)?

- Kein standardmäßiges **Setzen von Cookies**, die für bestimmungsgemäßen Gebrauch nicht notwendig sind und keine standardmäßige Aktivierung der **Ortungsfunktion** in der App (erst nach Aktivierung/Zustimmung durch den Nutzer).

- Vor **ersten Start** der DiGA/App sollten **keine Daten verarbeitet**/übermittelt werden, soweit nicht für Download/Installation technisch erforderlich.

- Nutzer sollte einsehen können, welche **Einwilligungen bzw. erforderliche Zugriffsberechtigungen** erteilt wurden, Einwilligungen/Zugriffsberechtigungen sollten jederzeit innerhalb der App widerrufbar sein ("**Einwilligungsmanagement**").

Bird & Bird

Privacy by Design

Was heißt das für DiGA (Apps)?

- **Sicherheit der Verarbeitung:**
  - Implementierung - unter Berücksichtigung der Stand der Technik, Art und Umfang der Verarbeitung und den Risiken – von angemessenen technischen und organisatorischen Maßnahmen, die sichere Verarbeitung der Daten gewährleistet?
  - Sensible Gesundheitsdaten **grundsätzlich pseudonymisiert** und bei einer **Übermittlung an Dritte verschlüsselt**
  - IT-System der DiGA ist unter **ISO 2700** (oder vergleichbarer Standard) **zertifiziert**
  - Mitarbeiter sind **auf Vertraulichkeit** verpflichtet und geschult
  - Verfahren zu regelmäßigen **Überprüfung, Bewertung** und **Evaluierung** zur Wirksamkeit der Maßnahmen etabliert

Bird & Bird

Privacy by Design

Was heißt das für DiGA (Apps)?

- **Einholung Einwilligung <u>für DiGA</u>:**
  - Im Bereich der **DiGA ist Einwilligung die entscheidende Rechtsgrundlage**
  - Daher: Sicherstellung der dokumentierten Einholung **einer freiwilligen, spezifischen, ausdrücklichen** (insb. in Bezug auf Gesundheitsdaten) und **informierten** (klare, verständliche Sprache) **Einwilligung**
  - Design von **granularer/gebündelter Einwilligungsmechanismen** und technische Umsetzung notwendig

Bird & Bird

Privacy by Design

Was heißt das für DiGA (Apps)?

- **Einwilligung** muss **per aktiver und eindeutiger Handlung des Nutzers** eingeholt werden (keine "konkludente" Einwilligung).

- Nutzer muss über **jederzeitige Widerrufsmöglichkeit** informiert werden; nach Widerruf müssen personenbezogene Daten des DiGA-Nutzers **gelöscht werden (können)**
  ➔ sofern **keine gesetzlichen Aufbewahrungsfristen** bestehen.

Bird & Bird

Privacy by Design

Fazit

- **'Privacy by Design' Grundsatz** gibt vor, wie Anwendungen/Apps - und damit auch eine DiGA - datenschutzrechtlich **grundsätzlich konzipiert** sein muss.

- Eine unter Berücksichtigung des 'Privacy by Design'-Grundsatzes nach der DSGVO konzipierte/programmierte **DiGA erfüllt grundsätzlich** auch die **daten-schutzrechtlichen Vorgaben** für eine DiGA nach der ***DIGAV*** und die in *Anlage 1* zur DiGAV konkretisierten Anforderungen **(Checkliste/Self-Assessment**).

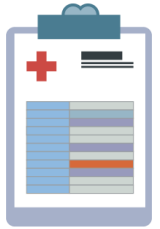
- **Achtung:** Hersteller sollten **datenschutzrechtliche Anforderungen** vor Design/Konzeptionierung der DiGA genau prüfen und bei Konzeptionierung implementieren ➔ **nachträgliche Anpassungen sind oft kostenintensiv** bzw. (technisch) nur schwer umzusetzen.

Bird & Bird

Datenschutzrechtliche Anforderungen für die Aufnahme in das DiGA-Verzeichnis

Bird & Bird

Aufnahme in das DiGA-Verzeichnis
Datenschutzrechtliche Anforderungen - DiGAV



- 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**.

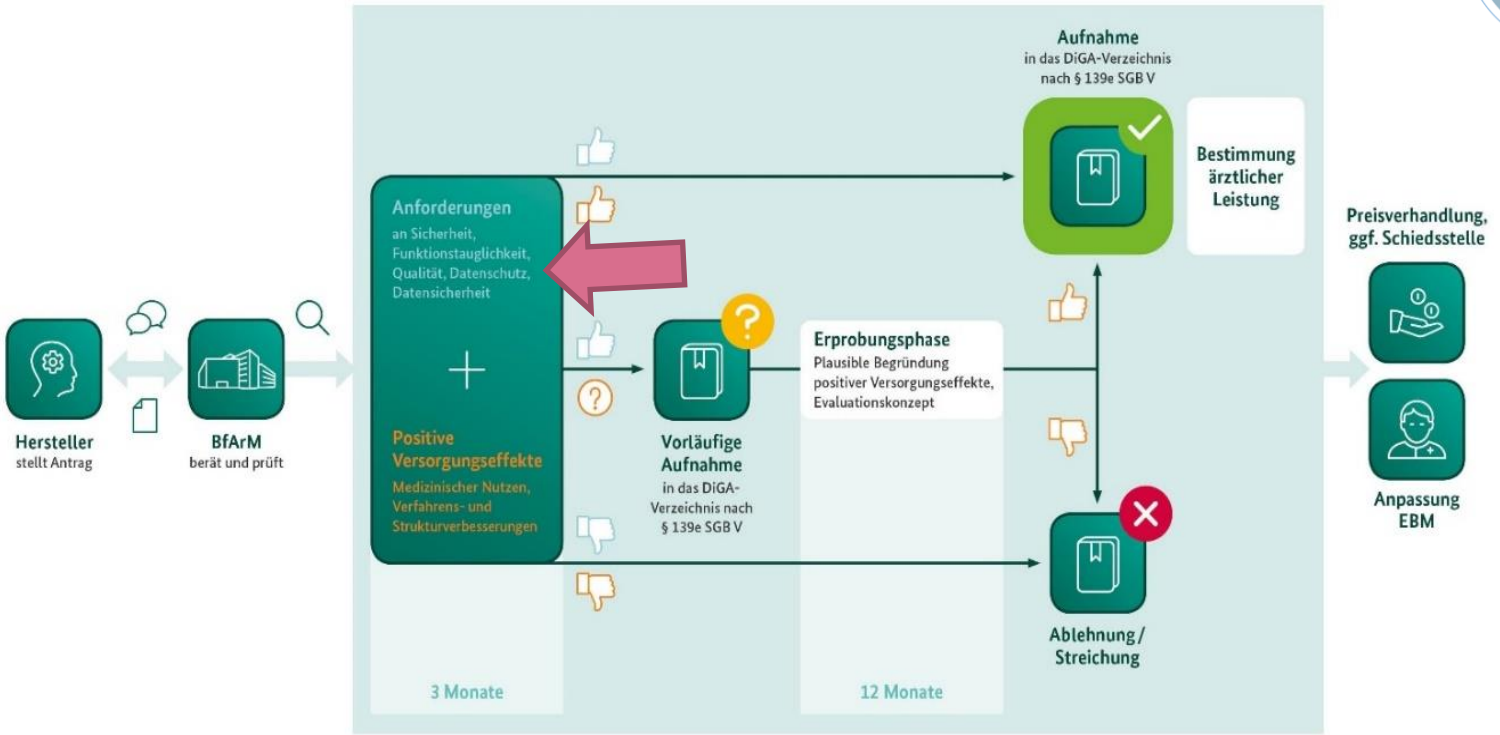
- Neben den allgemeinen datenschutzrechtlichen Vorgaben aus der DSGVO (und ggf. weiteren anwendbaren datenschutzrechtlichen Vorschriften) sind **für DiGA speziell die Vorgaben aus der Digitale Gesundheitsanwendungen-Verordnung** („*DiGAV*“) zu beachten.

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

Bird & Bird

Aufnahme in das DiGA-Verzeichnis

Übersicht Prüfverfahren



Bird & Bird

Aufnahme in das DiGA-Verzeichnis

Checkliste "Datenschutz"

- 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.

Bird & Bird

Aufnahme in das DiGA-Verzeichnis

Checkliste "Datenschutz"

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

Bird & Bird

Aufnahme in das DiGA-Verzeichnis
Checkliste "Datenschutz"

- 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**

Bird & Bird

Aufnahme in das DiGA-Verzeichnis
Checkliste "Datenschutz"

- Unter anderem Fragen zur
  - Gewährleistung der **Informationspflichten**

  - zur **technischen Umsetzung** der DiGA (z.B. implementierte technische und organisatorische Maßnahmen gemäß *Art. 32 DSGVO*) und **Organisation des Herstellers** hinsichtlich der Sicherstellung einer datenschutzkonformen Zusammenarbeit mit externen Dienstleistern bzw. Auftragsverarbeitern

  - Durchführung einer **Datenschutzfolgenabschätzung** (*Art. 35 DSGVO*)

  - Meldung von Verletzungen des Schutzes personenbezogener Daten („**Data Breach**“)

Bird & Bird

Checkliste "Datenschutz"

Exkurs: *Datenverarbeitung außerhalb Deutschlands*

- **Beschränkung des Orts der Datenverarbeitung** (gem. *§ 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** (EWG + 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 und (nur) Privacy Shield zertifizierte Unternehmen in den USA).

Bird & Bird

Checkliste "Datenschutz"

Exkurs: *Datenverarbeitung außerhalb Deutschlands*

- **Beschränkung des Orts der Datenverarbeitung** (gem. *§ 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**?

Bird & Bird

Aufnahme in das DiGA-Verzeichnis

Checkliste "Datenschutz"

- Bei Abfrage der Anforderungen/Kriterien werden als mögliche Antworten "**zutreffend**", "**nicht zutreffend**" und "**zulässige Begründung für nicht zutreffend**" vorgegeben.

- Erfüllung des geforderten Kriteriums ist gegeben, wenn alle zugehörigen Aussagen mit **„zutreffend“** angekreuzt wurden.

- Es werden auch **vorgefertigte** „Nicht zutreffend“-Antworten zur Auswahl gestellt, deren Ankreuzen **keine** negative Auswirkung auf die Erfüllung des übergeordneten Kriteriums hat.

Bird & Bird

Aufnahme in das DiGA-Verzeichnis

Checkliste "Datenschutz"

- **Achtung:** Eine nicht zur Auswahl vorgegebene „Nicht zutreffend“-Antwort **erfordert eine schriftliche Begründung**, warum übergeordnete Kriterium dennoch erfüllt wird.

- **Fehlt Begründung**, gilt der **Antrag als unvollständig**, und es ergeht Anweisung des BfArM zur Nachreichung der Begründung.

- Sofern innerhalb der gesetzten Frist **keine plausible Begründung** vorliegt, wird Antrag durch das BfArM **ohne weitere Prüfung abgewiesen**.

Bird & Bird

Verwendung personenbezogener Daten im Rahmen einer DiGA

Bird & Bird

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

Bird & Bird

Einwilligung

Zulässige Zwecke

- **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.

Bird & Bird

Einwilligung

Zulässige Zwecke

- **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.

Bird & Bird

Einwilligung

(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*.

Bird & Bird

Einwilligung

(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**
  - Raum für **Weiterentwicklung ohne Einwilligung** nach *Art. 9 Abs 2 (j), 89 DSGVO* i.V.m. *§ 27 BDSG* oder *§ 4 Abs. 2 S. 1 Nr. 4 DiGAV* lex specialis?

Bird & Bird

Einwilligung

(Un-)Zulässige Zwecke

- **Weitere Beispiele:**
  - 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.

Bird & Bird

Einwilligung
Zusammenfassung der Zwecke

- 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."

Bird & Bird

Einwilligung

Zusammenfassung der Zwecke

- **Zusammenfassung der Zwecke in *einer* Einwilligungserklärung** nur unter bestimmten Voraussetzungen:
  - nur für Zwecke gemäß Nr. 1 - 3 zulässig und
  - nur dann, wenn Daten zusätzlich zum Zweck des bestimmungsgemäßen Gebrauchs (Nr. 1) der DiGA durch die Nutzer zu Zwecken der Nummern 2 und 3 ebenfalls erforderlich sind, um eine Erprobung durchzuführen (Nr. 2) oder erfolgsabhängige Preisbestandteile ermitteln zu können (Nr. 3).

- **Stets gesondert** einzuholen: Einwilligung nach **Nr. 4.**
  ➔ Hier werden Daten zu eigenen Zwecken des DiGA-Herstellers verarbeitet.

Bird & Bird

Rechtliche Grundlagen

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
  - *Art. 9 Abs 2 (j), 89 DSGVO* i.V.m. *§ 27 BDSG* oder *§ 4 Abs. 2 S. 1 Nr. 4 DiGAV* (siehe oben)?

Bird & Bird

IT-Sicherheitsanforderungen

Bird & Bird

Aufnahme in das DiGA-Verzeichnis

Checkliste "Datensicherheit"

- **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**

Bird & Bird

Aufnahme in das DiGA-Verzeichnis

Checkliste "Datensicherheit"

- **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.

Bird & Bird

Checkliste "Datensicherheit"

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**

Bird & Bird

Checkliste "Datensicherheit"

Wann hat eine DiGA einen sehr hohen Schutzbedarf?

➔ Kriterien gemäß dem BSI-Standard 200-2 maßgeblich

Schutzbedarfskategorie „sehr hoch“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Innen- oder Außenwirkung	• Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden ist für die Institution existenzbedrohend.

Tabelle 4: Schutzbedarfskategorie „sehr hoch“

Bird & Bird

Checkliste "Datensicherheit"

Welche Zusatzanforderungen gelten bei sehr hohem Schutzbedarf?

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

Bird & Bird

IT-Sicherheitsanforderungen

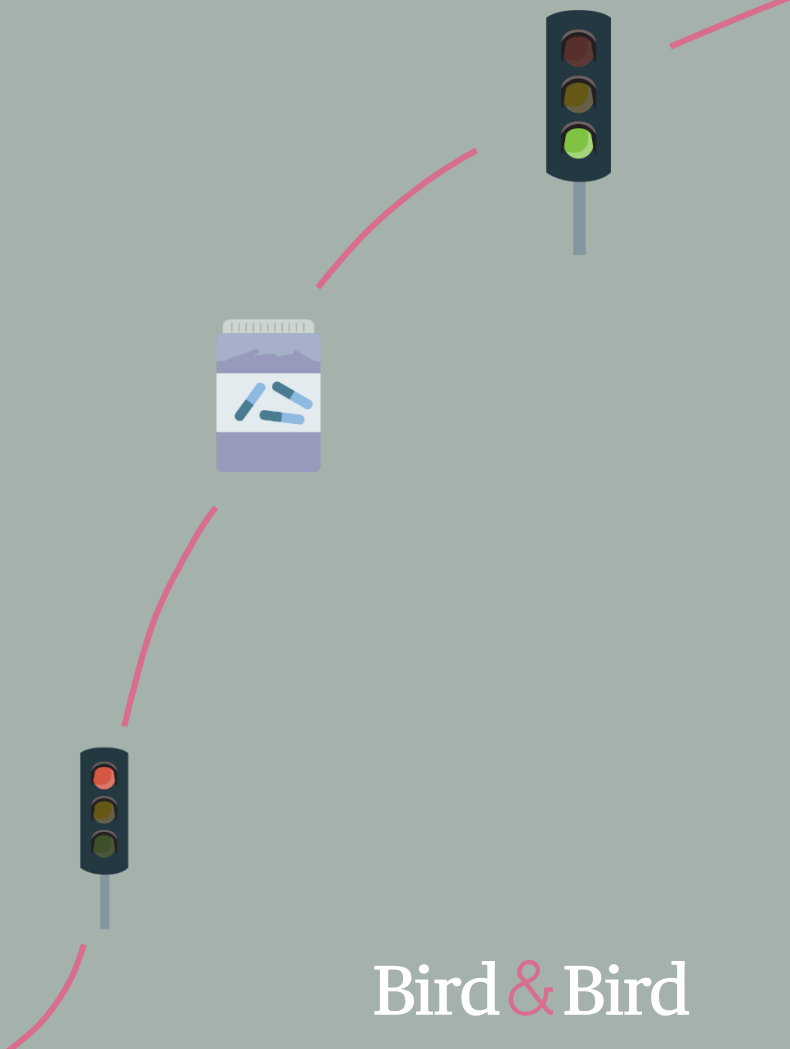
Technische Richtlinie BSI TR-03161

- Gegenstand und Zielsetzung der BSI TR **"Sicherheitsanforderungen an DiGA"**
  - wendet sich **an Hersteller** von DiGA für mobile Endgeräte
  - soll als **Leitfaden** dienen, um Entwickler von mobilen Anwendungen im Gesundheitswesen bei der Erstellung sicherer mobiler Applikationen zu unterstützen
  - beschreibt **mögliche Bedrohungen** und die minimalen Sicherheitseigenschaften von DiGA
- Bedeutung der BSI TR für Zertifizierung (in der Zukunft)

Bird & Bird

Dos and Don'ts für DiGA-

- Hersteller
- Distributoren
- Nutzer



Bird & Bird

Dos and Don’ts für Hersteller, Distributoren und Nutzer

Dos

- **Privacy by Design**-Gedanke: erst Vorgaben prüfen, dann implementieren
- 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
- Genau prüfen, auf welche **Rechtsgrundlagen** Verarbeitungstätigkeiten im Zusammenhang mit der DiGA jeweils gestützt werden können

Bird & Bird

Dos and Don’ts für Hersteller, Distributoren und Nutzer

Dos

- **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**

Bird & Bird

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 Standardvertragsklauseln oder Processor Binding Corporate Rules)

- **Nicht-zweckgebundene Verarbeitung** von personenbezogenen Daten; **keine Trennung von Daten**, die für verschiedene Zwecke (bestimmungsgemäßer Gebrauch/ Leistungsabrechnung) verarbeitet werden

Bird & Bird

Dos and Don’ts für Hersteller, Distributoren und Nutzer

Don’ts

- Verarbeitung von Daten **„auf Vorrat“** ohne Anwendung eines (nachvollziehbaren) Löschkonzepts

- **Unverschlüsselte** bzw. **nicht dem Stand der Technik** entsprechende Übermittlung von Gesundheitsdaten

Bird & Bird

Vielen Dank für Ihre Aufmerksamkeit

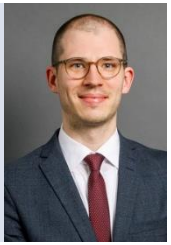
Sie haben Rückfragen? Benötigen weitere Informationen? Sprechen Sie uns gerne an!

Dr. Fabian Niemann
Partner
Tel:+4921120056254
fabian.niemann@twobirds.com

Lennart Schüßler
Partner
Tel: +4921120056377
lennart.schuessler@twobirds.com

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

Oliver Schmidt-Prietz, LL.M.
Associate
Tel: +4921120056377
oliver.schmidt-prietz@twobirds.com



Bird & Bird

Unsere Webinar-Reihe geht weiter

27. Mai 2020, 16:00 Uhr: Werberechtliche & vertriebliche Aspekte der DiGA

- Bewerbung und besondere Restriktionen für Medizinprodukte
- Risiken bei Non-Compliance mit werberechtlichen und regulatorischen Vorgaben
- Medical Apps in der Regelversorgung der gesetzlichen Krankenversicherung
- Kostenerstattung im DiGA-Verfahren

Dr. Alexander Csaki
Partner
Tel: +498935816199
alexander.csaki@twobirds.com

Christian Lindenthal, LL.M.
Counsel
Tel: +498935816152
christian.lindenthal@twobirds.com

Wolfgang Ernst
Associate
Tel: +498935816152
wolfgang.ernst@twobirds.com

Clarissa Junge-Gierse
Associate
Tel: +498935816199
clarissa.junge-gierse@twobirds.com

Bird & Bird

Vielen Dank & Bird & Bird

twobirds.com