Deutscher Anwaltverein

Arbeitsgemeinschaft Medizinrecht

# 20. Herbsttagung

**vom 11. bis 12. September 2020 in Berlin**

## Arbeitsgruppe Digital Health

# Aktuelle rechtliche Aspekte der Digitalisierung

Dr. Philipp Kircher

Berlin

health innovation hub

# Aktuelle rechtliche Aspekte der Digitalisierung

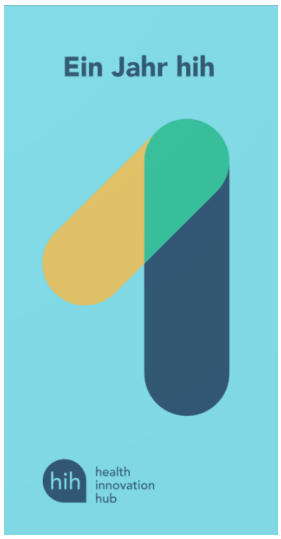
## ePa nach PDSG / Schrems II und DiGA

Dr. Philipp Kircher
Director Data Protection & Medical Law - health innovation hub
Rechtsanwalt, Berlin

**11.09.2020, 20. Herbsttagung Medizinrecht, DAV AG Medizinrecht**



# Der health innovation hub des BMG




## Brücke Staat ⇔ reale Welt

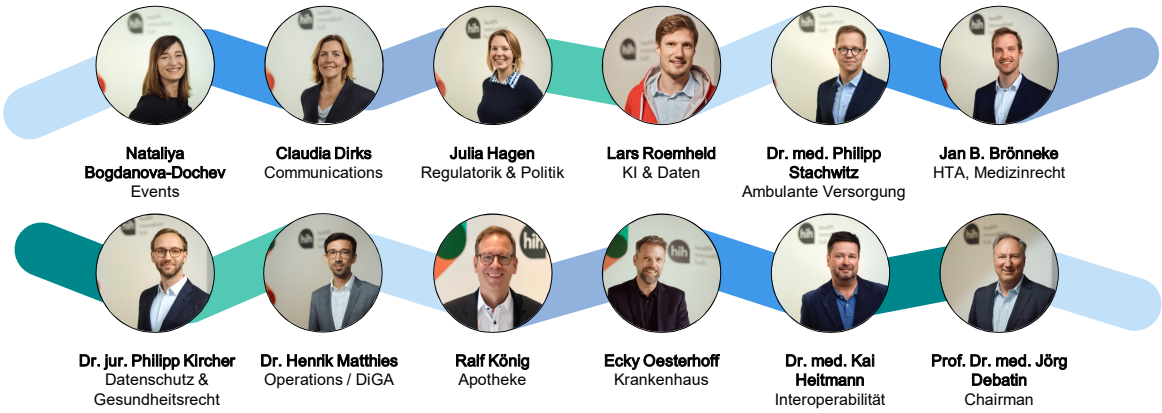
Unsere Aufgaben:

- Versorgungskonzepte des BMG bewerten und inhaltlich beraten
- digitale Innovationen frühzeitig zu erkennen,
- ihren Nutzen und Eignung zu bewerten,
- ihre Umsetzung in die Regelversorgung befördern,
- Brücken zwischen Digitalszene & Stakeholdern bauen.

Der Auftrag endet am 31.12.2021.

# Das hih-Team - Sparring Partner & Think Tank

INTERDISZIPLINÄRE DIGITALKOMPETENZ



**Nataliya Bogdanova-Dochev**
Events

**Claudia Dirks**
Communications

**Julia Hagen**
Regulatorik & Politik

**Lars Roemheld**
KI & Daten

**Dr. med. Philipp Stachwitz**
Ambulante Versorgung

**Jan B. Brönneke**
HTA, Medizinrecht



**Dr. jur. Philipp Kircher**
Datenschutz & Gesundheitsrecht

**Dr. Henrik Matthies**
Operations / DiGA

**Ralf König**
Apotheke

**Ecky Oesterhoff**
Krankenhaus

**Dr. med. Kai Heitmann**
Interoperabilität

**Prof. Dr. med. Jörg Debatin**
Chairman





hih health innovation hub

## AGENDA

1. DVG & PDSG – status quo

2. ePA – datenschutzrechtliche Verantwortlichkeit

3. ePA – neue Haftungsrisiken?

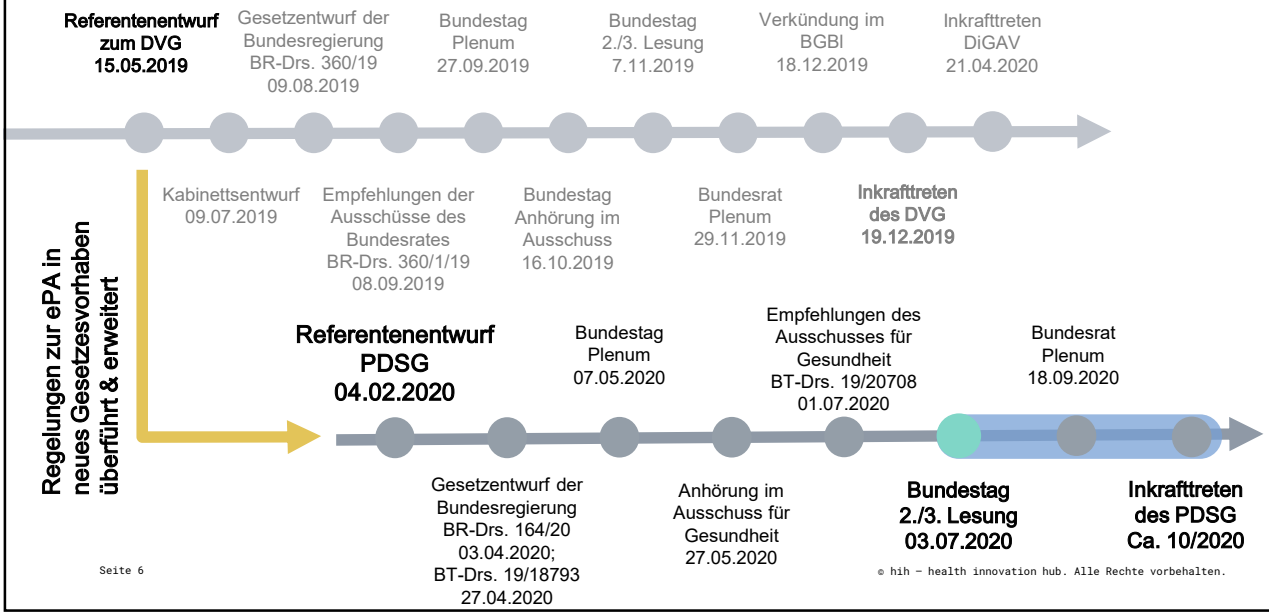
4. DiGA – Auswirkungen von Schrems II

health innovation hub

# DVG & PDSG – status quo



## Status Quo - ePA in DVG & PDSG




Seite 6

# Zwei neue Kapitel zur TI und zur IOP im SGB V

**Zehntes Kapitel**
Versicherungs- und Leistungsdaten, Datenschutz, Datentransparenz

**Elftes Kapitel**
Telematikinfrastruktur §§ 306 bis 383

**Zwölftes Kapitel**
Interoperabilitätsverzeichnis §§ 384 bis 393

**Elftes Kapitel**
Straf- und Bußgeldvorschriften → **Dreizehntes Kapitel**
Straf- und Bußgeldvorschriften §§ 394 bis 397

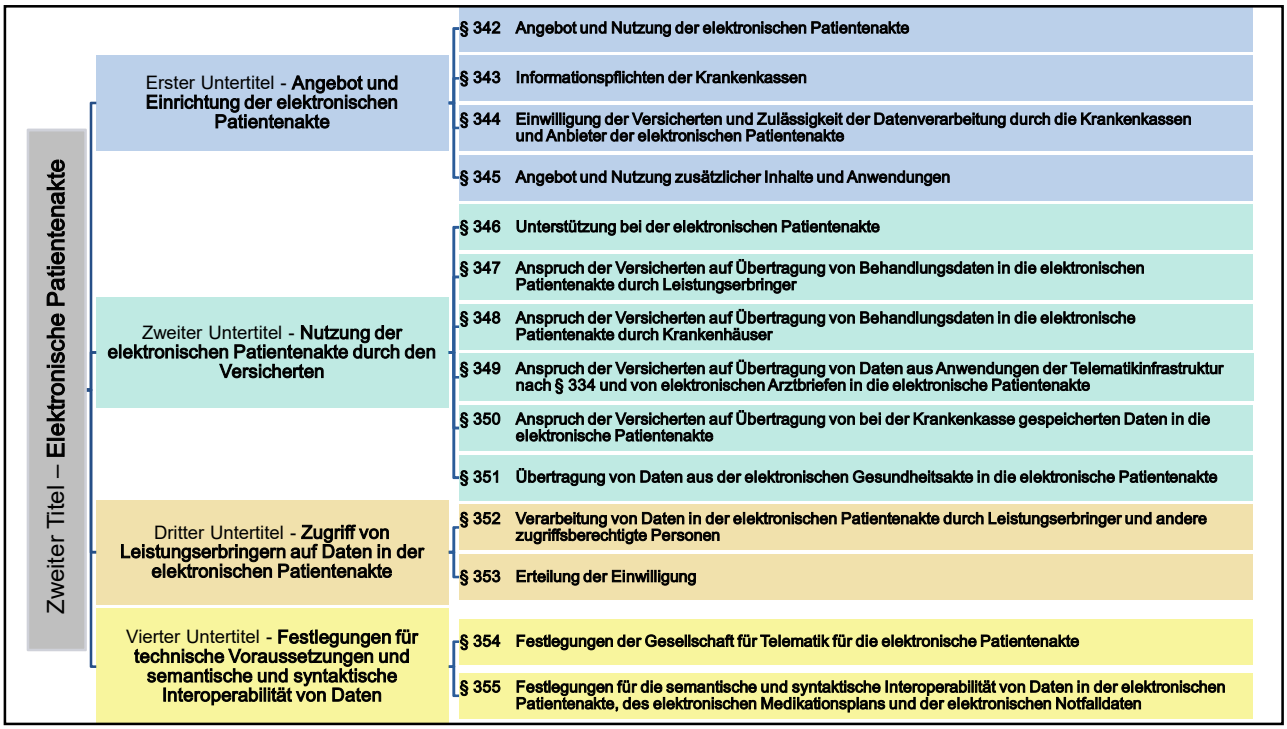
**Zwölftes Kapitel**
Überleitungsregelungen aus Anlaß der Herstellung der Einheit Deutschlands → **Vierzehntes Kapitel**
Überleitungsregelungen aus Anlaß der Herstellung der Einheit Deutschlands §§ 398 bis 400

**Dreizehntes Kapitel**
Weitere Übergangsvorschriften → **Fünfzehntes Kapitel**
Weitere Übergangsvorschriften §§ 401 bis 417




**Elftes Kapitel - Telematikinfrastruktur**

- Erster Abschnitt - **Anforderungen an die Telematikinfrastruktur**
- Zweiter Abschnitt - **Gesellschaft für Telematik**
  - Erster Titel - **Aufgaben, Verfassung und Finanzierung der Gesellschaft für Telematik**
  - Zweiter Titel - **Beirat der Gesellschaft für Telematik**
  - Dritter Titel - **Schlichtungsstelle der Gesellschaft für Telematik**
- Dritter Abschnitt - **Betrieb der Telematikinfrastruktur**
- Vierter Abschnitt- **Überwachung von Funktionsfähigkeit und Sicherheit**
  - Erster Titel - **Allgemeine Vorschriften**
  - Zweiter Titel - **Elektronische Patientenakte**
    - Erster Untertitel - **Angebot und Einrichtung der elektronischen Patientenakte**
    - Zweiter Untertitel - **Nutzung der elektronischen Patientenakte durch den Versicherten**
    - Dritter Untertitel - **Zugriff von Leistungserbringern auf Daten in der elektronischen Patientenakte**
    - Vierter Untertitel - **Festlegungen für technische Voraussetzungen und semantische und syntaktische Interoperabilität von Daten**
  - Dritter Titel - **Erklärungen des Versicherten zur Organ- und Gewebespende und Hinweise auf deren Vorhandensein und Aufbewahrungsort**
  - Vierter Titel - **Hinweis des Versicherten auf das Vorhandensein und den Aufbewahrungsort von Vorsorgevollmachten oder Patientenverfügungen**
  - Fünfter Titel - **Elektronischer Medikationsplan und elektronische Notfalldaten**
  - Sechster Titel - **Übermittlung ärztlicher Verordnungen**
  - Siebter Titel - **Nutzung der Anwendungen der Telematikinfrastruktur in der privaten Krankenversicherung**
  - Achter Titel - **Verfügbarkeit von Daten aus Anwendungen der Telematikinfrastruktur für Forschungszwecke**
- Fünfter Abschnitt - **Anwendungen der Telematikinfrastruktur**
- Sechster Abschnitt -**Telemedizinische Verfahren**
- Siebter Abschnitt - **Anforderungen an Schnittstellen in informationstechnischen Systemen**
- Achter Abschnitt - **Finanzierung und Kostenerstattung**




hih health innovation hub

# Wer ist datenschutzrechtlich verantwortlich?

# Verantwortlicher nach Art. 4 Nr. 7 DS-GVO

7. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

**Art. 4 Nr. 7 HS. 1 DS-GVO**

- Getrennte oder gemeinsame Verantwortlichkeit
- Maßgeblich ist die **Entscheidung** über
- **Zwecke** (ein erwartetes Ergebnis, das beabsichtigt ist oder die geplanten Aktionen leitet)
- **Mittel** (Art und Weise, wie ein Ergebnis oder Ziel erreicht wird)

vgl. Taeger/Gabel/Arning/Rothkegel, 3. Aufl. 2019, DS-GVO Art. 4 Rn. 169




**Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder - 12.09.2019**

**Datenschutzrechtliche Verantwortlichkeit innerhalb der Telematik-Infrastruktur**

Die Datenschutzkonferenz vertritt zur Frage der datenschutzrechtlichen Verantwortlichkeit innerhalb der Telematik-Infrastruktur nach § 291a Abs. 7 SGB V folgende Auffassung:

Die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) ist

a) datenschutzrechtlich alleinverantwortlich für die zentrale Zone der TI („TI-Plattform Zone zentral“) sowie

"b) im Sinne des Artikel 26 DSGVO datenschutzrechtlich mitverantwortlich für die dezentrale Zone der TI („TI-Plattform Zone dezentral“). Der Umfang der Verantwortung der gematik für die dezentrale Zone der Telematik-Infrastruktur bedarf einer gesetzlichen Regelung. Die gematik ist verantwortlich für die Verarbeitung, insbesondere soweit sie durch die von ihr vorgegebenen Spezifikationen und Konfigurationen für die Konnektoren, VPN-Zugangsdienste und Kartenterminals bestimmt ist."

# Verantwortlicher nach Art. 4 Nr. 7 DS-GVO

7. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

**Art. 4 Nr. 7 HS. 2 DS-GVO**

- Wenn **Zwecke und Mittel gesetzlich vorgegeben**
- kann durch Gesetz ein **Verantwortlicher bestimmt werden** oder es können bestimmte Kriterien seiner Benennung vorgesehen werden

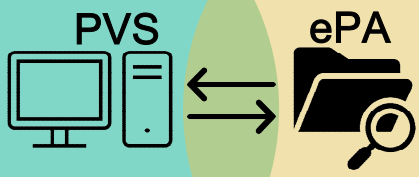
→ **§ 307 Abs. 4 SGB V (idF PDSG)**





# Verantwortlichkeitsgrenzen

- Die Praxisverwaltungs-systeme sind keine Anwendungen der TI.
- Für die Datenverarbeitung in in einem PVS (zB ärztliche Dokumentation vor Upload in ePA oder Downloads aus ePA) gilt weiterhin das BDSG (vgl. § 22 BDSG).
- Verantwortliche sind idR die **Leistungserbringer**.




- Die ePA ist eine Anwendung der TI (§ 334 Abs. 1 Nr. 1 SGB V idF PDSG).
- Für die Datenverarbeitung in Anwendungen der TI ist der Anbieter der Anwendung verantwortlich (§ 307 Abs. 3 SGB V idF PDSG).
- Verantwortliche für die ePA ist demnach die jeweilige **Krankenkasse** (§ 342 Abs. 1 SGB V idF PDSG).

health innovation hub

# Ergeben sich neue Risiken der Arzthaftung durch die ePA?



# Die ePA dient einer besseren Versorgung

**These:**

Die Verfügbarkeit von behandlungsrelevanten Informationen

- verbessert die Anamnese
- vermeidet Zweifelsfälle
- erhöht tendenziell die Behandlungsqualität
- hilft insbesondere Behandlungsfehler zu vermeiden
- ist daher **geeignet Haftungsfälle zu reduzieren**.

# Muss alles in der ePA sofort gelesen werden?

**Nein**,
- die ePA ist ein Aufbewahrungsort der PatientInnen, und **kein Posteingang** der Leistungserbringer! (Keine Anwendung von § 130 Abs. 1 BGB.)

**Im Gegenteil:**
ÄrztInnen **dürfen** Gesundheitsdaten aus der ePA **nur** abrufen und ggf. speichern (verarbeiten), wenn dies für die konkrete Behandlungssituation **erforderlich** ist! (Vgl. § 22 Abs. 1 Nr. 1 lit. b) BDSG)

Daran ändert auch die Einwilligung nach §§ 352, 353 SGB V (idF PDSG) nichts!




# Primärdokumentation vs. ePA

wenn erforderlich

## Primärdokumentation

- **Ärztlich** geführte Akte über Behandlung von PatientInnen
- **Im Primärsystem** / Leistungserbringerumgebung
- Dient der **ärztl. Dokumentation**
- **Gesetzliche Befugnis** zur Datenverarbeitung (§ 22 Abs. 1 Nr. 1 lit. b) BDSG)
- **Dokumentationspflicht** (§ 630f Abs. 2 BGB)
- **Aufbewahrungspflicht** (§ 630f Abs. 3 BGB)

## Elektronische Patientenakte

- **Versichertengeführte** Akte
- Von Krankenkassen angeboten
- **Extern** gespeicherte Daten
- Dient der Verfügbarkeit von Daten in der Hand der **Versicherten**
- **Einwilligung** und Zugriffsfreigabe für Leistungserbringer erforderlich (§ 353 SGB V)
- **Kein Ersatz** der ärztlichen Dokumentation!

wenn gewünscht

# ePA - Welche Haftungsregelungen gelten?

- Keine neuen zivilrechtlichen Haftungsregelungen durch das PDSG
- Keine neuen Pflichten in den §§ 630a ff. BGB
- Haftungsfragen folgen den bekannten Regelungen im BGB
- Die Kasuistik der Rechtsprechung zu haftungsrelevanten Behandlungsfehlern dürfte dabei übertragbar sein

Hier insbesondere: **Anamneseerhebungsfehler**




# Anamneseerhebungsfehler

- Behandlungsfehler kommen in Betracht, wenn die Behandlung nicht den **allgemein anerkannten fachlichen Standards** (§ 630a Abs. 2 BGB) entspricht.
- Hierzu gehört eine der Befunderhebung, Diagnostik und Therapie **vorangehende Anamnese**.
- ÄrztInnen können und müssen gezielt nach Vorbehandlungen und relevanten Dokumenten fragen. Sie steuern das Gespräch mit PatientInnen.
- Eine Pflicht zu genauerem Nachfragen oder zum Anfordern und Lesen fremder Behandlungsunterlagen ergibt sich, wenn es medizinisch-fachlich **sachgerecht** ist.
- Während man sich in der Regel auf die Richtigkeit fachfremder Informationen vertrauen darf, sind solche der eigenen Fachdisziplin kritisch zu würdigen.

health innovation hub

# Schrems II und DiGA



# Bisher kein spezifischer Weg in die Regelversorgung

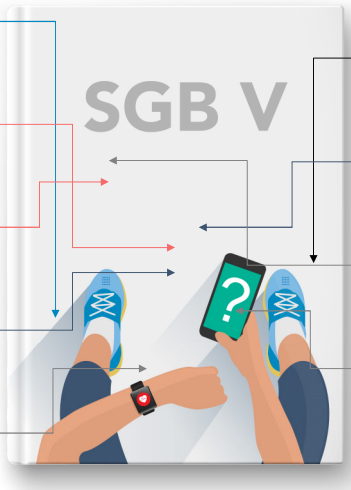
§§ 20 ff. Prävention

§ 32 Heilmittel

§ 33 Hilfsmittel

§§ 63 ff. Modellvorhaben

§§ ...




§ 137f – neu DMP

§ 140a Besondere Versorgung

§ 291g Videosprechstunde

§ 291a Anwendungen eGK/TI

Seite 22

Quelle: © Caption Health, © Butterfly

# Digitale Gesundheitsanwendung nach § 33a SGB V

**Medizinprodukt**

der Klasse I oder IIa nach MDR sowie Übergangsfristen (Klasse I und IIa MDD)

**Zweckbestimmung**

Unterstützung Versicherte oder in der (v.a. ambulanten) Versorgung durch Leistungserbringer*innen

SGB V

**DiGA nach § 33a SGB V**

**Hauptfunktion**

beruht wesentlich auf digitalen Technologien

**Funktionalitäten**

Erkennung, (Überwachung), Behandlung, Linderung, (Kompensierung) von Krankheiten, Verletzungen oder Behinderungen

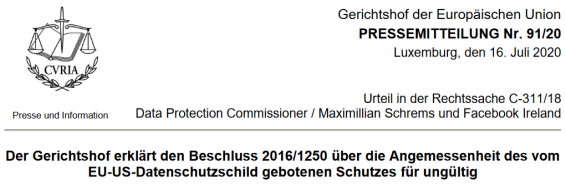




# EuGH Urteil vom 16.07.2020, Rs. C-311/17 – Privacy Shield

**Hintergrund:**

- EuGH hatte 2015 das „Safe Habor"-Abkommen bzgl. Datentransfers in die USA für ungültig erklärt. (Urt. v. 06.10.2015, Schrems I, C-362/14)
- Für das Nachfolgeabkommen „Privacy Shield" gab es einen Angemessenheitsbeschluss der EU-Kommission vom 12.07.2016.



Gerichtshof der Europäischen Union
**PRESSEMITTEILUNG Nr. 91/20**
Luxemburg, den 16. Juli 2020

Presse und Information

Urteil in der Rechtssache C-311/18
Data Protection Commissioner / Maximillian Schrems und Facebook Ireland

**Der Gerichtshof erklärt den Beschluss 2016/1250 über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für ungültig**

- Erneutes Vorlageverfahren des High Court (Irland) beim EuGH wg. einer Beschwerde von Maximilian Schrems bzgl. Drittstaatentransfer durch Facebook Ireland in USA.

**Wesentliche Inhalte des Urteils:**

- Komissionsbeschluss 2016/1250 zum **Privacy Shield (USA) ist ungültig**.
- Komissionsbeschluss 2010/87 für **Standardvertragsklauseln** für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern ist gültig – Setzt aber ein **adäquates Datenschutzniveau im Drittland voraus (!), das aber ist bei den USA eben nicht anzunehmen!**

# Bisherige Angemessenheitsentscheidungen der EU

**Adequacy decisions**

How the EU determines if a non-EU country has an adequate level of data protection.

The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection.

Quelle: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

- **Angemessenheitsbeschluss der EU-Kommission bezüglich der USA war auf das Privacy Shield begrenzt!**





# Digitale Gesundheitsanwendungen-Verordnung (DiGAV)

**Verordnung**
**über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung – DiGAV)**

**Vom 8. April 2020**

Auf Grund des § 134 Absatz 3 Satz 17 und des § 139e Absatz 7 bis 9 des Fünften Buches Sozialgesetzbuch, die durch Artikel 1 Nummer 23 des Gesetzes vom 9. Dezember 2019 (BGBl. I S. 2562) eingefügt worden sind, verordnet das Bundesministerium für

5. Zielsetzung, Wirkungsweise, Inhalt und Nutzung der digitalen Gesundheitsanwendung in einer allgemeinverständlichen Form,
6. den Funktionen der digitalen Gesundheitsanwen-

- In Kraft getreten am 21.04.2020
- Konkretisiert insb. Anforderungen für die Aufnahme in das DiGA-VZ
- → **Strenge Datenschutzanforderungen in § 4 DiGAV**

# Eingeschränkte Drittstaatentransfers nach § 4 Abs. 3 DiGAV

**§ 4 Absatz 3 DiGAV**

(3) Im Rahmen einer digitalen Gesundheitsanwendung darf die Verarbeitung von personenbezogenen Daten durch die digitale Gesundheitsanwendung selbst sowie bei einer Verarbeitung personenbezogener Daten im Auftrag nur im Inland, in einem Mitgliedstaat der Europäischen Union oder in einem diesem nach § 35 Absatz 7 des Ersten Buches Sozialgesetzbuch gleichgestellten Staat oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat erfolgen.

- DiGAV verlangt immer einen Angemessenheitsbeschluss!
- Weitere Instrumente nach Art. 46, 47 DS-GVO sind ausgeschlossen!

**Begründung Zu Absatz 3**

Die Regelung erstreckt die sozialdatenschutzrechtlichen Einschränkungen der Auftragsdatenverarbeitung unter Einsatz ausländischer Dienstleister nach § 80 Absatz 2 des Zehnten Buches Sozialgesetzbuch auf die Datenverarbeitung digitaler Gesundheitsanwendungen sowie eine beim Einsatz der digitalen Gesundheitsanwendung erfolgende Verarbeitung von Daten im Auftrag. Hierdurch wird gewährleistet, dass auch bei der Nutzung etwa von Cloud-Diensten durch den Hersteller die Datenhoheit der Versicherten gewahrt wird. 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. Im Rahmen der Risikoanalyse der Schutzbedarfsbestimmung ist auch die geographische Belegenheit der nach § 2 anzugebenden Serverstandorte zu berücksichtigen.






- Mit dem EuGH-Urteil vom 16.07.2020 zum Privacy Shield ist auch der DiGA-Leitfaden des BfArM mit Stand vom 10. Juni 2020 insoweit überholt.
- Leitfaden wurde mit Version 2.0 bereits am 31.07.2020 entsprechend aktualisiert.

**3.3.3 Datenverarbeitung außerhalb Deutschlands**

Die DSGVO erlaubt eine Datenverarbeitung innerhalb der EU. Eine Verarbeitung außerhalb der EU in einem sog. Drittstaat ist zulässig, sofern ein vergleichbares Schutzniveau im Drittstaat besteht (Angemessenheitsbeschluss nach Artikel 45 DSGVO). Die weitreichenden Ausnahmen nach Artikel 46 und 47 DSGVO sind für DiGA aufgrund des regelhaft anzunehmenden besonderen Schutzbedarfs der verarbeiteten Daten nicht anwendbar.

Die DiGAV beschränkt analog zu den für Krankenkassen geltenden Regeln (§ 80 SGB X) den Ort der Datenverarbeitung auf die Bundesrepublik Deutschland, die Mitgliedstaaten der Europäischen Union, die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und die Schweiz und Staaten, für die ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt. Eine Verarbeitung von personenbezogenen Daten außerhalb der EU auf Basis von Art. 46 DSGVO (Standardvertragsklauseln) oder Art. 47 (Corporate Binding Rules) ist für DiGA nicht zulässig.

In einer aktuellen Liste der Staaten, für die ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt, sind die USA aufgeführt. Hier gilt der Angemessenheitsbeschluss jedoch nur für Unternehmen, die unter den EU-US Privacy Shield fallen. Hierbei ist zu beachten, dass im EU-US Privacy Shield zwischen HR-Daten und Non-HR-Daten differenziert wird[1] und nicht alle gelisteten Unternehmen die für die Teilnahme am EU-US Privacy Shield erforderlichen Vorgaben für beide Arten von Daten erfüllen. Gesundheitsdaten fallen durchweg in den Bereich der Non-HR-Daten.

Eine Verarbeitung von Gesundheitsdaten in den USA ist für eine DiGA somit nur dann zulässig, wenn das die Daten (selbst oder im Auftrag) verarbeitende Unternehmen unter den EU-US Privacy Shield fällt und dort die Vorgaben für die Verarbeitung von Non-HR Daten erfüllt.

## Auswirkungen auf DiGA

- Ein **Transfer von personenbezogenen Daten in die USA** ist mit der Rechtsprechung des EuGH vom 16.07.2020 zum Privacy Shield für DiGA-Hersteller **nicht zulässig**.
- Das gilt auch für **Auftragsverarbeiter** der DiGA-Hersteller.
- Die Möglichkeit auf andere Instrumente der DS-GVO (z.B. **Standardvertragsklauseln**) zurückzugreifen ist bereits durch die **DiGAV ausgeschlossen.**
- **Es bedürfte daher erst einer neuen Angemessenheitsentscheidung der EU in Bezug auf das Datenschutzniveau der USA.**






## Links

**Alle hih Veranstaltungen:**
https://hih-2025.de/veranstaltungen/

**Aufzeichnungen:**

- DiGA-Sprechstunde (Verschreibung & Nutzung): https://hih-2025.de/diga-sprechstunde-verschreibung-und-nutzung/
- DiGA-Summit (deutsch): https://hih-2025.de/diga-summit-summary-video-docs-next-steps/
- KH-Summit: https://hih-2025.de/krankenhaus-digital-summit-die-zukunft-wird-jetzt-gemacht-2/

health innovation hub

# Herzlichen Dank!

Dr. Philipp Kircher
Director Data Protection & Medical Law
philipp.kircher@hih-2025.de