



health
innovation
hub

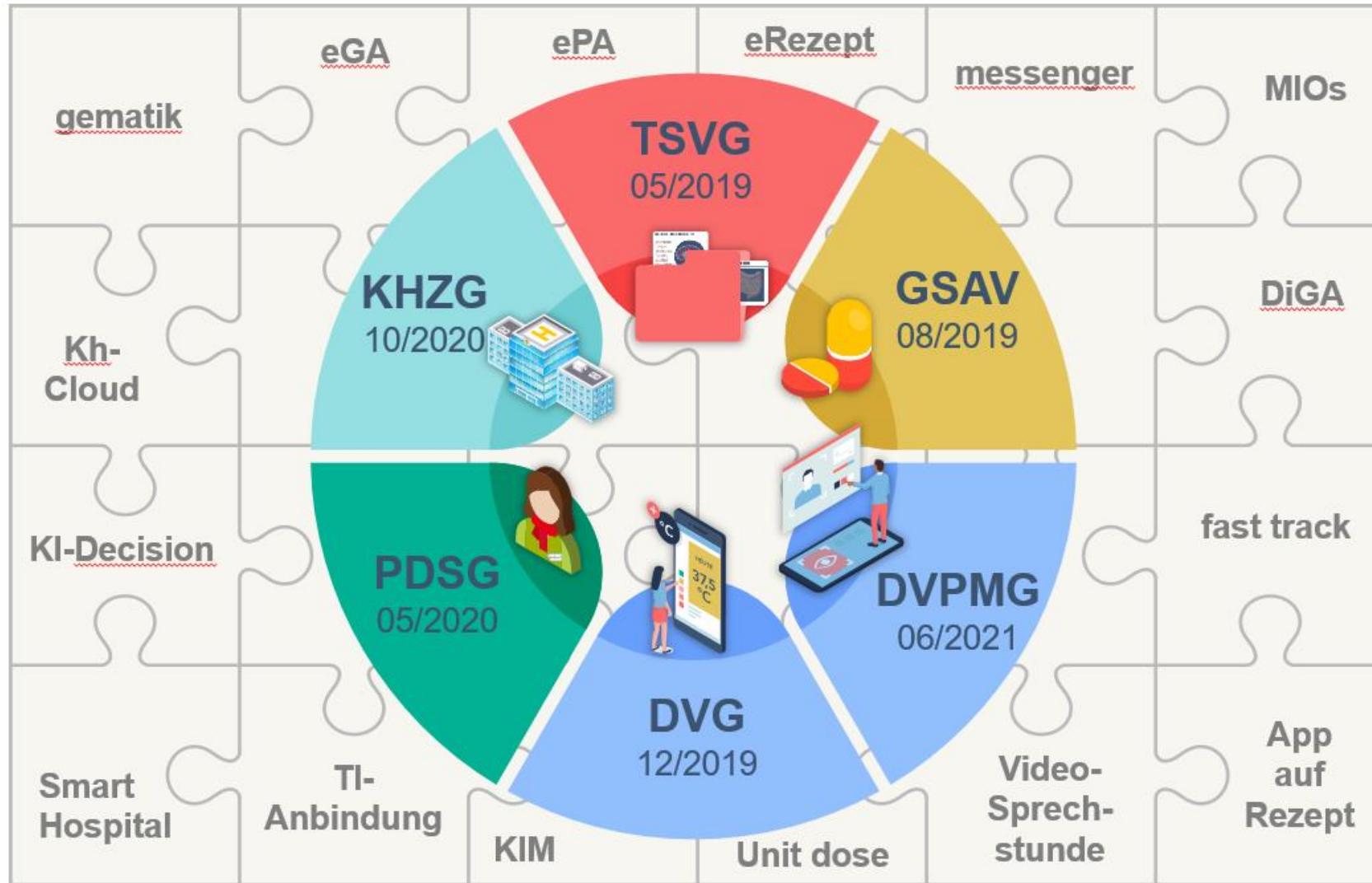
Datenschutzrechtliche Fragen der elektronischen Patientenakte (ePA)

Dr. Philipp Kircher

Director Data Protection & Medical Law, health innovation hub |
Rechtsanwalt, Berlin

17.09.2021 – 21. Herbsttagung AG Medizinrecht

Aktuelle Legislatur: Umfassende Digitalisierungsgesetzgebung



TSVG: Terminservice- und Versorgungsgesetz
GSAV: Gesetz für mehr Sicherheit in der Arzneimittelversorgung
DVG: Digitale-Versorgung-Gesetz

KBV: Kassenärztliche Bundesvereinigung
MIOs: Medizinische Informationsobjekte
ePA: elektronische Patientenakte

PDSG: Patientendaten-Schutz-Gesetz
DVPMG: Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz

46 Monate
↓
28 Gesetze
mit
digitalen
Inhalten
↓
6 Gesetze mit
Schwerpunkt
Digitalisierung

SGB V
46x geändert!

Der datenschutzrechtliche Rahmen

Konzeption und Zusammenspiel der Vorschriften



Art. 8 EMRK; Art. 7, 8 GRCh; Art. 16 AEUV; Art. 2 I i.V.m. Art. 1 I GG



Datenschutz-Grundverordnung – DS-GVO - VO (EU) 2016/679

Zwei-stufiges Vorgehen

1.

Zulässigkeit der Datenverarbeitung („Ob“)

- Gesetzliche Verarbeitungsbefugnis oder Einwilligung
- Zweckbindung
- Erforderlichkeit...

2.

Art und Weise der Datenverarbeitung („Wie“)

- Technische und organisatorische Maßnahmen
- Privacy by Design / Default
- Informationspflichten
- Betroffenenrechte
- Benennung eines Datenschutzbeauftragten
- ...

Doppeltes Verbot mit Zulässigkeitsvorbehalt

Personenbezogene Daten (Art. 6 DS-GVO)

- Verarbeitung grds. unzulässig, es sei denn
 - Einwilligung oder
 - Befugnisnormlegitimieren die Verarbeitung

Besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO)

- Verarbeitung ausdrücklich verboten, es sei denn
 - ausdrückliche Einwilligung oder
 - Befugnisnormlegitimieren die Verarbeitung

Zulässigkeit der Verarbeitung von Gesundheitsdaten

Art. 9 Abs. 2 DS-GVO (Befugnistatbestände)

Tatbestand	Detailierung
Lit. a)	• Ausdrückliche Einwilligung • bzgl. Daten nach Art. 9 Abs. 1 DS-GVO
Lit. c)	• Schutz lebenswichtiger Interessen • betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben
Lit. d)	• Organisation ohne Gewinnerzielungsabsicht • bzgl. Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte
Lit. e)	• Daten, die die betroffene Person offensichtlich öffentlich gemacht hat
Lit. f)	• Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte

Zulässigkeit der Verarbeitung von Gesundheitsdaten

Art. 9 Abs. 2 DS-GVO (Öffnungsklauseln)

Tatbestand	Detailierung
Lit. b)	Arbeitsrecht, Recht der sozialen Sicherheit und des Sozialschutzes
Lit. g)	erhebliches öffentliches Interesse
Lit. h)	- für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich - oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs - Verarbeitung durch Fachpersonal oder unter dessen Verantwortung, das Berufsgeheimnis/Geheimhaltungspflicht
Lit. i)	- Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit - Schutz vor schwerwiegenden grenzüberschreitende Gesundheitsgefahren - Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten
Lit. j)	im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Art. 89 Abs. 1

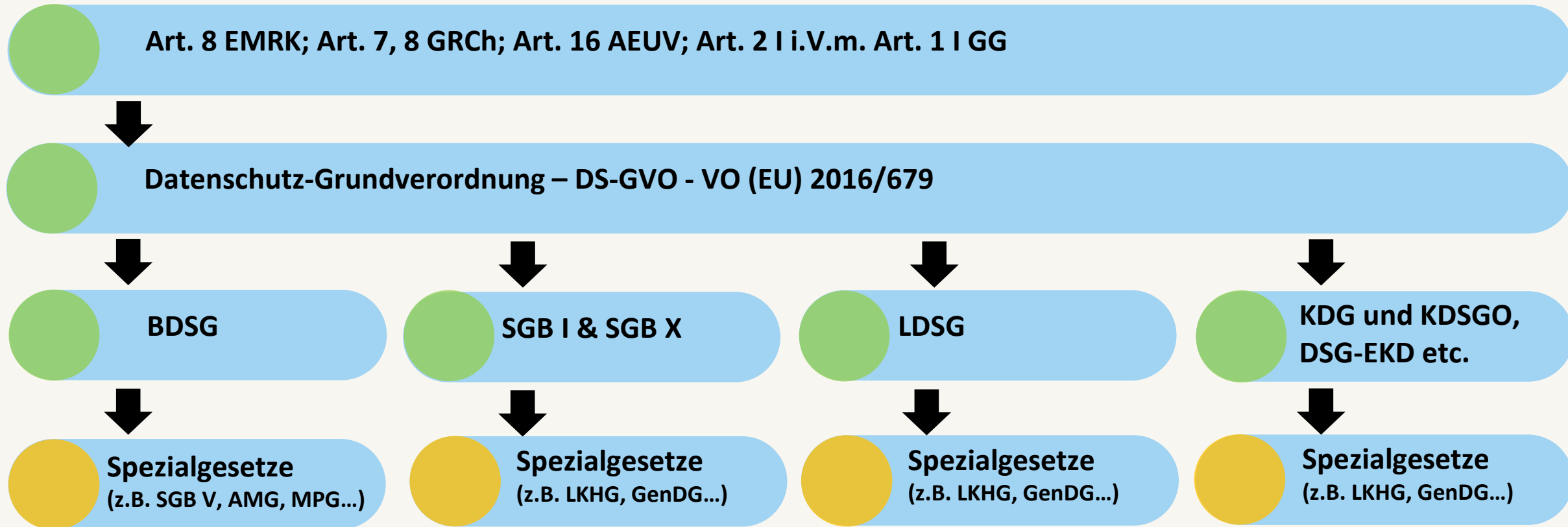
Wesentliche Öffnungsklauseln

Artikel	Bereich	Umfang
Art. 6 Abs. 1 UAbs. 1 lit. c) und e) DS-GVO i.V.m. Art. 6 Abs. 2, 3 DS-GVO	• Erfüllung einer rechtlichen Verpflichtung • Wahrnehmung einer Aufgabe im öffentlichen Interesse • Ausübung öffentlicher Gewalt	Umfangreiche Gestaltungsspielräume im öffentlichen Bereich
Art. 6 Abs. 4 DS-GVO	• Zweckänderung (allgemein)	Str!
Art. 9 Abs. 2 lit. a), b), g), h), i), j) DS-GVO	• Besondere Kategorien personenbezogener Daten • Einwilligung • Soziale Sicherheit und Sozialschutz • Erhebliches öffentliches Interesse • Gesundheits- und Sozialbereich • Öffentliche Gesundheit • Archiv- und Forschungszwecke	Umfangreiche Gestaltungsspielräume im öffentlichen und nicht-öffentlichen Bereich, insbesondere bei der "öffentlichen Gesundheit"
Art. 9 Abs. 4 DS-GVO	• Genetische Daten • Biometrische Daten • Gesundheitsdaten	Zusätzliche Bedingungen, einschließlich Beschränkungen
Art. 89 Abs. 2, 3 DS-GVO	• Forschungs-, Statistik- und Archivzwecke	Beschränkung von Betroffenenrechten

Wesentliche Öffnungsklauseln (Gesundheitsdaten)

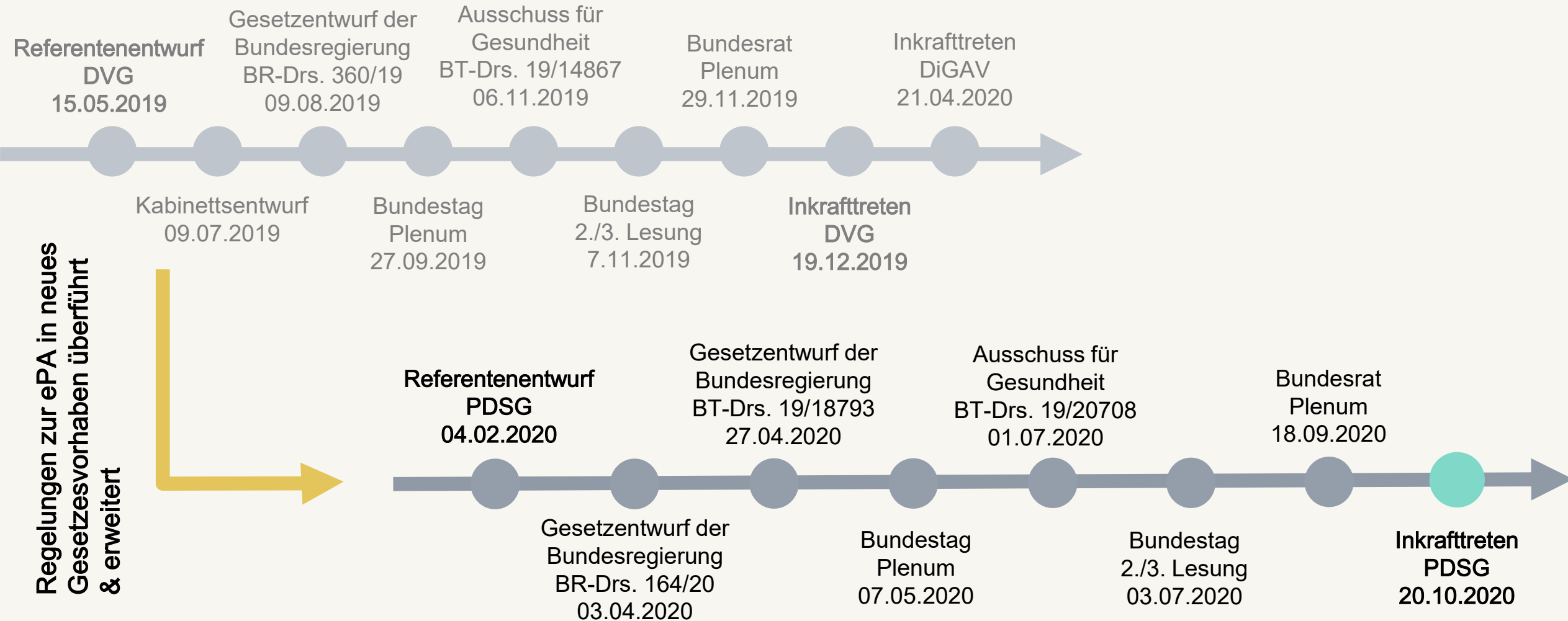
Artikel	Bereich	Umfang
Art. 6 Abs. 1 UAbs. 1 lit. c) und e) DS-GVO i.V.m. Art. 6 Abs. 2, 3 DS-GVO	• Erfüllung einer rechtlichen Verpflichtung • Wahrnehmung einer Aufgabe im öffentlichen Interesse • Ausübung öffentlicher Gewalt	Umfangreiche Gestaltungsspielräume im öffentlichen Bereich
Art. 6 Abs. 4 DS-GVO	• Zweckänderung (allgemein)	Str!
Art. 9 Abs. 2 lit. a), b), g), h), i), j) DS-GVO	• Besondere Kategorien personenbezogener Daten • Einwilligung • Soziale Sicherheit und Sozialschutz • Erhebliches öffentliches Interesse • Gesundheits- und Sozialbereich • Öffentliche Gesundheit • Archiv- und Forschungszwecke	Umfangreiche Gestaltungsspielräume im öffentlichen und nicht-öffentlichen Bereich, insbesondere bei der "öffentlichen Gesundheit"
Art. 9 Abs. 4 DS-GVO	• Genetische Daten • Biometrische Daten • Gesundheitsdaten	Zusätzliche Bedingungen, einschließlich Beschränkungen
Art. 89 Abs. 2, 3 DS-GVO	• Forschungs-, Statistik- und Archivzwecke	Beschränkung von Betroffenenrechten

Konzeption und Zusammenspiel der Vorschriften



Reform des SGB V nach PDMSG und DVPMG

Status Quo - ePA in DVG & PDSG



Status Quo - ePA im DVPMG



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

Erster Abschnitt - Anforderungen an die Telematikinfrastuktur
Zweiter Abschnitt - Gesellschaft für Telematik
Dritter Abschnitt - Betrieb der Telematikinfrastuktur
Vierter Abschnitt- Überwachung von Funktionsfähigkeit und Sicherheit
Fünfter Abschnitt - Anwendungen der Telematikinfrastuktur
Sechster Abschnitt -Telemedizinische Verfahren
Siebter Abschnitt - Anforderungen an Schnittstellen in informationstechnischen Systemen
Achter Abschnitt - Finanzierung und Kostenerstattung

Erster Titel - Aufgaben, Verfassung und Finanzierung der Gesellschaft für Telematik
Zweiter Titel - Beirat der Gesellschaft für Telematik
Dritter Titel - Schlichtungsstelle der Gesellschaft für Telematik
Erster Titel - Allgemeine Vorschriften
Zweiter Titel - Elektronische Patientenakte
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 Telematikinfrastuktur in der privaten Krankenversicherung
Achter Titel - Verfügbarkeit von Daten aus Anwendungen der Telematikinfrastuktur für Forschungszwecke

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

Zweiter Titel – Elektronische Patientenakte	Erster Untertitel - Angebot und Einrichtung der elektronischen Patientenakte	§ 341	Elektronische Patientenakte
		§ 342	Angebot und Nutzung der elektronischen Patientenakte
		§ 343	Informationspflichten der Krankenkassen
		§ 344	Einwilligung der Versicherten und Zulässigkeit der Datenverarbeitung durch die Krankenkassen und Anbieter der elektronischen Patientenakte
	Zweiter Untertitel - Nutzung der elektronischen Patientenakte durch den Versicherten	§ 345	Angebot und Nutzung zusätzlicher Inhalte und Anwendungen
		§ 346	Unterstützung bei der elektronischen Patientenakte
		§ 347	Anspruch der Versicherten auf Übertragung von Behandlungsdaten in die elektronischen Patientenakte durch Leistungserbringer
		§ 348	Anspruch der Versicherten auf Übertragung von Behandlungsdaten in die elektronische Patientenakte durch Krankenhäuser
		§ 349	Anspruch der Versicherten auf Übertragung von Daten aus Anwendungen der Telematikinfrastruktur nach § 334 und von elektronischen Arztbriefen in die elektronische Patientenakte
		§ 350	Anspruch der Versicherten auf Übertragung von bei der Krankenkasse gespeicherten Daten in die elektronische Patientenakte
	Dritter Untertitel - Zugriff von Leistungserbringern auf Daten in der elektronischen Patientenakte	§ 351	Übertragung von Daten aus der elektronischen Gesundheitsakte und aus Anwendungen nach § 33a in die elektronische Patientenakte
		§ 352	Verarbeitung von Daten in der elektronischen Patientenakte durch Leistungserbringer und andere zugriffsberechtigte Personen
		§ 353	Erteilung der Einwilligung
	Vierter Untertitel - Festlegungen für technische Voraussetzungen und semantische und syntaktische Interoperabilität von Daten	§ 354	Festlegungen der Gesellschaft für Telematik für die elektronische Patientenakte
		§ 355	Festlegungen für die semantische und syntaktische Interoperabilität von Daten in der elektronischen Patientenakte, des elektronischen Medikationsplans und der elektronischen Notfalldaten und der elektronischen Patientenkurzakte

Datenschutzrechtliche Verantwortlichkeit

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 i.V.m. § 341 Abs. 4 SGB V

*"Die mit dem PDSG neu gefassten und inhaltlich überarbeiteten Neuregelungen der §§ 291 ff SGB V enthalten ein **hinreichend normdichtes und klares Regelungsgefüge**, das durch eine Vielzahl aufeinander und insbesondere auch mit den Vorgaben der DSGVO abgestimmter materiell-rechtlicher, organisatorischer und prozeduraler Maßnahmen der Datensicherheit dient (...), der der Gesetzgeber beim Auf- und Ausbau der TI eine „herausragende Rolle“ beimisst (...). Dabei ist der Gesetzgeber auch seiner Beobachtungs- und Nachbesserungspflicht nachgekommen, indem er etwa auf die in der Praxis zu Tage getretenen datenschutzrechtlichen Defizite und Sicherheitslücken, auf die zum Teil auch die Klägerin hingewiesen hat, reagiert und entsprechende Gegenmaßnahmen ergriffen hat.*

*So hat er auf die zuvor bestehenden **Unklarheiten hinsichtlich der Abgrenzung der datenschutzrechtlichen Verantwortlichkeiten im Rahmen der TI durch die gesetzliche Normierung dieser Verantwortlichkeiten und die Einrichtung einer koordinierenden Stelle bei der gematik reagiert (§ 307 SGB V(...)).**"*

BSG, Urteil vom 20.01.2021 – B 1 KR 7/20 R, Rn. 104 f.

Sind ePA-Daten Sozialdaten?

Verarbeitung besonderer Kategorien personenbezogener Daten

“

§ 35 Abs. 1 S. 1 SGB I – Sozialgeheimnis

(1) Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Absatz 2 Zehntes Buch) von den Leistungsträgern nicht unbefugt verarbeitet werden (Sozialgeheimnis).

§ 67 Abs. 2 SGB X

(2) Sozialdaten sind personenbezogene Daten (Artikel 4 Nummer 1 der Verordnung (EU) 679/2016), die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden.

Sozialdatenschutz – Anwendbarkeit von SGB I und SGB X

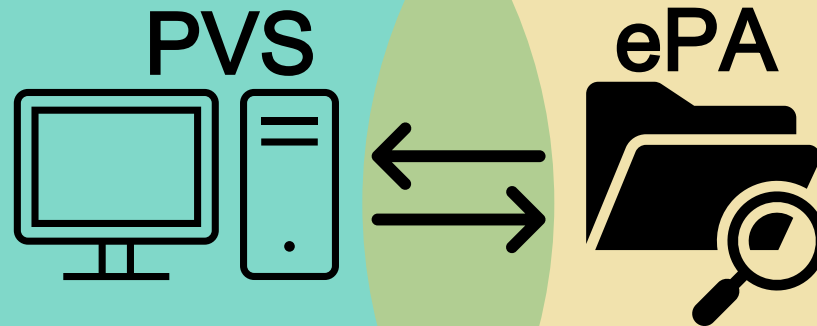
Stellen nach § 35 Abs. 1 SGB I

- **Leistungsträger** (Krankenkassen, Pflegekassen usw.) inkl. Verbände der Leistungsträger und Arbeitsgemeinschaften der Leistungsträger und ihrer Verbände
- Datenstelle der Rentenversicherung
- die im SGB genannten öffentlich-rechtlichen Vereinigungen
- Integrationsfachdienste
- die Künstlersozialkasse
- die Deutsche Post AG, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist
- die Behörden der Zollverwaltung, soweit sie Aufgaben nach § 2 des Schwarzarbeitsbekämpfungsgesetzes und § 66 des Zehnten Buches durchführen
- die Versicherungsämter und Gemeindebehörden sowie die anerkannten Adoptionsvermittlungsstellen (§ 2 Absatz 2 des Adoptionsvermittlungsgesetzes), soweit sie Aufgaben nach diesem Gesetzbuch wahrnehmen
- Stellen, die Aufgaben nach § 67c Absatz 3 des Zehnten Buches wahrnehmen.

 **Leistungserbringer (z.B. Vertragsärzte, zugelassene Krankenhäuser etc.) nicht umfasst!**

Verantwortlichkeitsgrenzen

- Die Praxisverwaltungssysteme sind keine Anwendungen der TI.
- Für die Datenverarbeitung 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).
- Für die Datenverarbeitung in Anwendungen der TI ist der Anbieter der Anwendung verantwortlich (§ 307 Abs. 3 SGB V).
- Verantwortliche für die ePA ist demnach die jeweilige **Krankenkasse** (§ 341 Abs. 4 SGB V).

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

Muss eine Datenschutz-Folgenabschätzung von Leistungserbringern erstellt werden, wenn Komponenten der TI zur Verarbeitung personenbezogener Daten verwendet werden?

Vorgaben der DS-GVO

Art. 35 Abs. 1 S. 1 DS-GVO

*„Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung **voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge**, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.“*

Art. 35 Abs. 3 lit. b) DS-GVO

„Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

(...)

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

(...)

Vorgaben der DS-GVO

EG 91 S. 4 DS-GVO

*„Die Verarbeitung personenbezogener Daten sollte **nicht als umfangreich** gelten, wenn die **Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt.***

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
16	Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO - auch wenn sie nicht als „umfangreich“ im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist - sofern eine nicht einmalige Datenerhebung mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden.	Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten	Ein Arzt nutzt ein Webportal oder setzt eine App an, um mit Patienten mittels Videotelefonie zu kommunizieren und Gesundheitsdaten durch Sensoren beim Patienten (z.B. Blutzucker, Sauerstoffmaske,...) detailliert und systematisch zu erheben und zu verarbeiten.

Im Gesetzgebungsverfahren durchgeführte DS-FA

§ 307 Abs. 1 S. 3 SGB V

„Für die Verarbeitung personenbezogener Daten mittels der Komponenten der dezentralen Infrastruktur nach § 306 Absatz 2 Nummer 1 durch Verantwortliche nach Satz 1 erfolgt in der Anlage zu diesem Gesetz eine Datenschutz-Folgenabschätzung nach Artikel 35 Absatz 10 der Verordnung (EU) 679/2016.“

1350

Bundesgesetzblatt Jahrgang 2021 Teil I Nr. 28, ausgegeben zu Bonn am 8. Juni 2021

Anhang zu Artikel 1 Nummer 84

Anlage

(zu § 307 Absatz 1 Satz 3 SGB V)

Datenschutz-Folgenabschätzung

**Beeinträchtigt das grobgranulare
Rechtemanagement die Wirksamkeit der
Einwilligung?**

Anforderungen an die Einwilligung

Art. 4 Nr. 11, Art. 9 Abs. 2 lit. a) DS-GVO

- *Freiwillig*
- *Für den bestimmten Fall*
- *In informierter Weise*
- *Unmissverständlich in Form einer Erklärung oder sonstigen eindeutigen bestätigenden Handlung / ausdrücklich*

Anforderungen an die Einwilligung

Ausdrückliche Erklärung nach § 339 Abs. 1, §§ 352, 353 SGB V

- Erteilung durch eindeutige bestätigende Handlung durch technische Zugriffsfreigabe
- über die Benutzeroberfläche eines geeigneten Endgeräts oder
- unter Nutzung der dezentralen Infrastruktur

Informiertheit

- § 291 Abs. 5, § 314 [insb. Nr.2, 3, 5, 6]
- § 336 Abs. 2 Nr. 1
- § 342 Abs. 2 Nr. 1 lit. g), h), Abs. 3
- § 343 [insb. Abs. 1 Nr. 12, 13]
- § 345 Abs. 2
- § 353 Abs. 2 Nr. 2
- § 358 Abs. 6, 7
- § 363 Abs. 5 SGB V

Anforderungen an die Einwilligung

Für den bestimmten Fall

- Zugriffszeitraum von Versicherten bestimmbar
- Zweckbestimmung gesetzlich vorschrieben (§ 352 SGB V)
- Umfang nach Art der Daten bekannt und über Erforderlichkeit beschränkt

Freiwillig

- Abwesenheit von Zwang (entkoppelt)
- Diskriminierungsverbot (§ 335 SGB V) sichert, dass notwendige Versorgungsleistungen auch ohne eine ePA-Einwilligung erbracht werden
- Vgl. BVerfG, Beschluss vom 4.1.2021 – 1 BvR 619/20
- Vgl. BSG, Urteil vom 20.1.2021 – B 1 KR 7/20 R

**Verstößt das Rechtemanagement gegen
Grundsätze der DS-GVO, insb. Privacy by Design
und Privacy by Default?**

Art. 25 DS-GVO - *Implementierung technischer und organisatorischer Maßnahmen „von Anfang an“*

Abs. 1 – Privacy by Design

- Berücksichtigung diverser Abwägungstopoi erforderlich (wie bei Art. 32 DS-GVO)
- Tatsächliche Freigabe kann über erforderliches Maß hinausgehen – Relevanz muss aber ärztlich entschieden werden!
- Kontext spricht im Zweifel für Datenverfügbarkeit

Abs. 2 – Privacy by Default

- ohne Eingreifen der betroffenen Person hat nur diese selbst Zugriff (Default)
- Zugriff von Leistungserbringern (inkl. Gehilfen) setzt Einwilligung durch Zugriffsfreigabe voraus
- Zugriffszeitraum standardmäßig 7 Tage ist kontextadäquat

**Stellen die unterschiedlichen Steuerungs- und
Einsichtsmöglichkeiten zwischen FdV und
dezentraler Infrastruktur eine ungerechtfertigte
Ungleichbehandlung dar?**

Ungleichbehandlung zwischen unterschiedlichen Nutzern?

Bereits nach PDSG

- *ePA steht allen Versicherten grundsätzlich unterschiedslos zur Verfügung*
- *Unterschiedliche Funktionalitäten technisch von existierender Infrastruktur bedingt*
- *DS-GVO und Art. 3 GG gewähren keinen Anspruch, dass unterschiedliche technische Nutzungszugänge zu einem freiwilligen, zusätzlichen Leistungsangebot funktional unterschiedslos ausgestaltet und jedermann zur Verfügung gestellt werden müssen (lediglich derivatives Teilhaberecht)*
- *Vertreterregelung, um Rechte durch Vertrauensperson wahrnehmen zu lassen (§ 342 Abs. 2 Nr. 2 SGB V)*

Seit DVPMG

- *Ab 01.01.2022 neben FdV auf mobilen Endgeräten auch Benutzeroberfläche eines geeigneten stationären Endgeräts (zB PC)*

Gilt die DS-GVO im Gesundheits- und Sozialbereich überhaupt?

Anwendbarkeit der DS-GVO im Sozialdatenschutz

§ 35 Abs. 2 SGB I – Verhältnis zu sonstigem Datenschutzrecht

“

Die Vorschriften des Zweiten Kapitels des Zehnten Buches und der übrigen Bücher des Sozialgesetzbuches regeln die Verarbeitung von Sozialdaten abschließend, **soweit nicht die Verordnung (EU) 2016/679** des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung **unmittelbar gilt**. Für die **Verarbeitungen von Sozialdaten im Rahmen von nicht in den Anwendungsbereich der Verordnung (EU) 2016/679 fallenden Tätigkeiten finden die Verordnung (EU) 2016/679 und dieses Gesetz entsprechende Anwendung**, soweit nicht in diesem oder einem anderen Gesetz Abweichendes geregelt ist.

BSG, Urteil vom 20.1.2021 – B 1 KR 7/20 R

- *DS-GVO findet keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt (vgl. Art. 2 Abs. 2 lit. a) DS-GVO und Art. 16 Abs. 2 AEUV)*
- *Umfang der Regelungskompetenz nach Art. 16 Abs. 2 AEUV umstritten*
- *Festlegung der Gesundheitspolitik sowie die Organisation des Gesundheitswesens und die medizinische Versorgung ist Sache der Mitgliedstaaten (vgl. Art. 168 Abs. 7 Satz 1 und 2 AEUV)*
- *Frage im Sozialdatenschutzrecht nicht entscheidungserheblich, wenn DS-GVO nicht Prüfmaßstab für nationales Recht ist oder jedenfalls nationales Recht mit der DS-GVO vereinbar ist.*



**In Ermangelung einer Vorlage zum EuGH bleibt diese Frage offen.
Sie ist nicht nur für das Sozialdatenschutzrecht sondern das gesamte Gesundheitswesen relevant!**

Beschlagnahmeschutz von ePA-Daten?

Nicht umgesetzter Änderungsvorschlag zu § 97 Abs. 2 S. 1 StPO

(1) Der Beschlagnahme unterliegen nicht

- 1. schriftliche Mitteilungen zwischen dem Beschuldigten und den Personen, die nach § 52 oder § 53 Abs. 1 Satz 1 Nr. 1 bis 3b das Zeugnis verweigern dürfen;*
- 2. Aufzeichnungen, welche die in § 53 Abs. 1 Satz 1 Nr. 1 bis 3b Genannten über die ihnen vom Beschuldigten anvertrauten Mitteilungen oder über andere Umstände gemacht haben, auf die sich das Zeugnisverweigerungsrecht erstreckt;*
- 3. andere Gegenstände einschließlich der ärztlichen Untersuchungsbefunde, auf die sich das Zeugnisverweigerungsrecht der in § 53 Abs. 1 Satz 1 Nr. 1 bis 3b Genannten erstreckt.*

*(2) Diese Beschränkungen gelten nur, wenn die Gegenstände im Gewahrsam der zur Verweigerung des Zeugnisses Berechtigten sind; hiervon ausgenommen sind die elektronische Gesundheitskarte nach § 291 des Fünften Buches Sozialgesetzbuch **sowie die elektronische Patientenakte nach § 341 des Fünften Buches Sozialgesetzbuch hinsichtlich der von einem zur Verweigerung des Zeugnisses Berechtigten eingestellten Daten.***

(...)

Vgl. Art. 4 Referentenentwurf des BMG zum PDSG vom 04.02.2020

Begründung der Bundesregierung

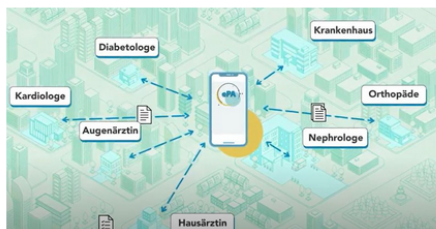
Für die sensiblen Gesundheitsdaten nach Absatz 2 gilt der Beschlagnahmeschutz nach der Strafprozessordnung (StPO). Hierfür bedarf es keiner gesonderten Regelung. Schriftliche Aufzeichnungen oder schriftliche Mitteilungen eines Zeugnisverweigerungsberechtigten unterfallen dem Beschlagnahmeverbot des § 97 Abs. 1 StPO, wenn sie im Gewahrsam des Zeugnisverweigerungsberechtigten sind. Nach § 11 Abs. 3 des Strafgesetzbuches (StGB) gilt dies auch für Daten, die von dem Zeugnisverweigerungsberechtigten in die elektronische Patientenakte eingestellt werden. Darüber hinaus greift das Beschlagnahmeverbot für die elektronische Patientenakte gemäß §§ 97 Abs. 3 StPO auch dann, wenn sich die elektronische Patientenakte bei der aktenführenden Krankenkasse befindet, da es sich bei letzterer im Rahmen der Führung der elektronischen Patientenakte um eine „mitwirkende Person“ nach § 53a Abs. 1 S. 1 StPO handelt.

BT-Drucks. 19/18793, S. 113

a.A.: *Dochow*, MedR 2021, 13 (20 ff.), *Kircher*, GuP 2021, 1 (11 dort Fn.82), *Solscheid*, MedR 2021, 795.

Weitere Informationen unter <https://hih-2025.de/magazin/>

Magazin



SMART PRAXIS, EPATIENT, GOOD NEWS

Die elektronische Patientenakte – Basis für eine bessere Medizin

Willkommen
Version
Sie ver
Dopp

REDEKER | SELLNER | DAHS

eken.



Vereinbarkeit der Regelungen zur elektronischen Patientenakte (ePA) nach dem Patienten-Datenschutz-Gesetz (PDSG) mit europäischem Datenschutzrecht

Rechtsgutachten im Auftrag des health innovation hub



GuP

1/2021

11. Jahrgang, Seiten 1–40

Rechtszeitschrift für das gesamte Gesundheitswesen

Herausgegeben von: Prof. Dr. Peter Axer | Prof. Dr. Markus Flinn | Prof. Dr. Ingo Heberlein | Prof. Dr. Thorsten Kingreen | Dr. Martin Krasney | Dr. Kyrill Makoski | Prof. Dr. Frank Ulrich Montgomery | Prof. Dr. Hermann Plagemann | Dr. Elke Roos | Marcus Schlam | Prof. Dr. Stefan Schick | Prof. Dr. Bernd Schütze | Prof. Dr. Astrid Waltrabenstein | Wolfgang Wellner | Prof. Dr. Felix Weitz | Dr. Ole Ziegler
Schriftleitung: Prof. Dr. Hermann Plagemann und Dr. Ole Ziegler
www.gup.nomos.de

AUFSÄTZE

Das Patientendaten-Schutz-Gesetz (PDSG) und die elektronische Patientenakte (ePA)

– Regulationsüberblick und Vereinbarkeit mit der DS-GVO

von Dr. Philipp Kircher*

Mit dem Patientendaten-Schutz-Gesetz (PDSG) wurden die Re- II. Vorbetr



Aktuelle Literatur und Rechtsprechung zum Thema

Literatur

- *Dochow*, Das Patienten-Datenschutz-Gesetz (Teil 1): Die elektronische Gesundheitskarte und Telematikinfrastruktur, MedR 2020, 979
- *Dochow*, Das Patienten-Datenschutz-Gesetz (Teil 2): Die elektronische Patientenakte und erweiterte Datenverarbeitungsbefugnisse der Krankenkassen, MedR 2021, 13
- *Dochow*, Das Patienten-Datenschutz-Gesetz (Teil 3): Die Datenspende, MedR 2020, 41
- *Kircher*, Das Patientendaten-Schutz-Gesetz (PDSEG) und die elektronische Patientenakte (ePA), GuP 2021, 1
- *Eichenhofer*, Die elektronische Patientenakte – aus sozial-, datenschutz- und verfassungsrechtlicher Sicht, NVwZ 2021, 1090
- *Solscheid*, Beschlagnahmeschutz und Beweisverwertung einer elektronischen Patientenakte („ePA“), MedR 2021, 795
- *Berry*, Vereinfachung der medizinischen Forschung durch Nutzung von Datenbeständen der elektronischen Patientenakte? – Das Potential des § 363 Abs. 8 SGB V im Gefüge des Datenschutzrechtes, GesR 2021, 553

Rechtsprechung

BVerfG, Beschluss vom 4.1.2021 – 1 BvR 619/20

BSG, Urteil vom 20.1.2021 – B 1 KR 7/20 R (m. Anm. *Kircher*, SGB 2021, i.E.)

Herzlichen Dank!

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