WEBINAR

DATENSCHUTZ IM BIOTECH-UNTERNEHMEN

Der Landesbeauftragte für
den **DATENSCHUTZ** und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

BIONTECH

SPEAKER

Michael Heusel-Weiss

LfDI Rheinland-Pfalz

Gesundheit, Soziales, Biotechnologie & Umwelt

- Bereichsleitung
- Bearbeitung von Beschwerden, Hinweisen und Beratungsanfragen
- Erlass aufsichtsrechtlicher Bescheide
- Einbindung in Gesetzgebungsverfahren
- Bundesweite Abstimmung datenschutzrechtlicher Fragen im AK Gesundheit und Soziales der DSK und weiterer Gremien
- diverse Aktivitäten zur besseren Umsetzung des Datenschutzrechts in der Praxis (z.B. Initiative „Mit Sicherheit gut behandelt“)

Michael Smolle

LfDI Rheinland-Pfalz

Kommunales, Forschung, Hochschulen, Kultur , OZG, Videoüberwachung

- Bereichsleitung
- Bearbeitung von Beschwerden, Hinweisen und Beratungsanfragen
- Erlass aufsichtsrechtlicher Bescheide
- Einbindung in Gesetzgebungsverfahren
- Bundesweite Abstimmung datenschutzrechtlicher Fragen im AK Wissenschaft und Forschung der DSK

Stefanie Kirchner

Senior Director Data Privacy

Data Privacy Officer

- Datenschutzbeauftragte
- Beratung des Unternehmens in allen datenschutzrechtlichen Belangen
- Durchführung von Datenschutzschulungen
- Überwachung der Einhaltung der datenschutzrechtlichen Vorgaben
- Verantwortlich Datenpannen zu untersuchen und an die Behörde zu melden
- Zusammenarbeit mit Aufsichtsbehörden

ÜBERBLICK WEBINAR-REIHE

Ablauf

- 4 Webinare in 2025
- Schwerpunkt liegt auf der Biotechnologie Branche, aber alle Datenschutzinteressierte sind herzlich eingeladen

Zielsetzung / Lessons Learned

- Rechtsrahmen Datenschutz in der Biotechnologie Branche
- LfDI – Beratung und Hilfestellung
- Umsetzung der gesetzlichen Vorschriften – wie ist das machbar?

AGENDA WEBINAR #2

Datenschutz und Forschungsvorhaben

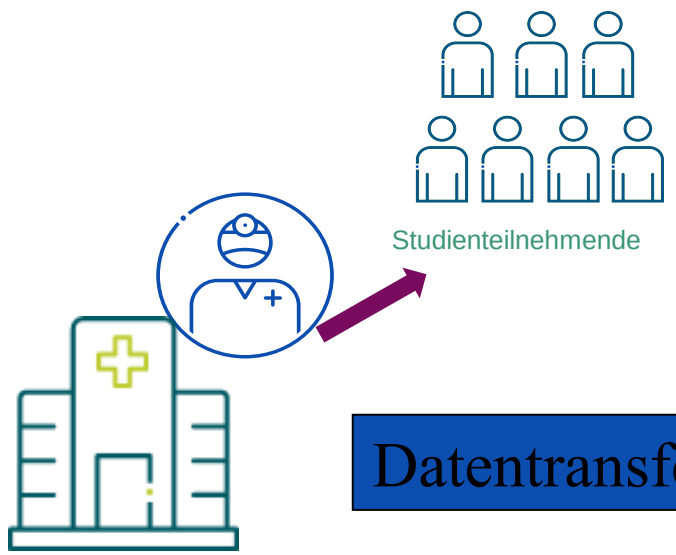
- Datenverarbeitung in der klinischen Studie

  Fortsetzung Fall aus Webinar #1 - Zuordnung der datenschutzrechtlichen Verantwortlichkeit für die Datenverarbeitung

- Pseudonymisierung und Anonymisierung

- European Health Data Space (EHDS)

FALLBEISPIEL

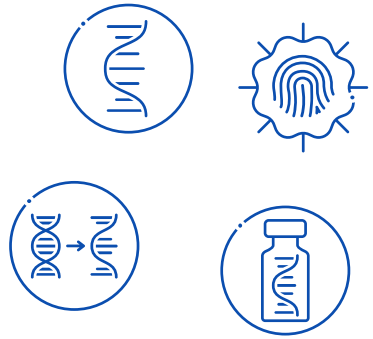


Studienteilnehmende

Studienzentren

Datentransfer

Unternehmen/ Sponsor



- Datenverarbeitung innerhalb der Studie
- Datenverarbeitung in der Forschung
- EHDS

DATENVERARBEITUNG IN DER KLINISCHEN STUDIE

Einschlägige Rechtsvorschriften:

- EU-VO Nr. 536/2014 über klinische Prüfungen mit Humanarzneimitteln

- EU-VO Nr. 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DS-GVO)

  In der DS-GVO wird ausdrücklich auf die einschlägigen Rechtsvorschriften für klinische Prüfungen Bezug genommen (Erwägungsgründe 158 + 161).

  Daraus ergibt sich, dass beide Rechtsvorschriften gleichzeitig anwendbar sind und die Verordnung über klinische Prüfungen einen sektorspezifischen Rechtsakt darstellt, der spezielle datenschutzrechtliche Vorschriften, aber keine allgemeinen Abweichungen von der DS-GVO enthält (Opinion 3/2019 des EDSA, Rn 4).

DATENVERARBEITUNG IN DER KLINISCHEN STUDIE

Einschlägige Rechtsvorschriften:

Gesetz über den Verkehr mit Arzneimitteln (AMG)

- Begriffsbestimmungen § 4 AMG
  ------- klinische Studie - Artikel 2 Absatz 2 Nummer 1 der Verordnung (EU) Nr. 536/2014
  Nr. 23 Klinische Prüfung - Artikel 2 Absatz 2 Nummer 2 der Verordnung (EU) Nr. 536/2014
  Nr. 24 Sponsor - Artikel 2 Absatz 2 Nummer 14 der Verordnung (EU) Nr. 536/2014
  Nr. 25 Prüfer - Artikels 2 Absatz 2 Nummer 16 der Verordnung (EU) Nr. 536/2014

- Verarbeitungserlaubnis § 40 b AMG

  § 40 b Abs. 1 AMG – Einwilligung (nach Aufklärung) in die Teilnahme (Art. 29 Nr. 536/2014)
  § 40 b Abs. 6 S. 1 AMG – Einwilligung in die Datenverarbeitung

- Format der verarbeiteten Daten

  § 40 b Abs. 6 S. 3 Nr. 1 lit. b AMG - Pseudonymisierung
  § 42 a AMG – Datenschutz und Pseudonymisierung

DATENVERARBEITUNG IN DER KLINISCHEN STUDIE

Einordnung des Verhältnisses von Sponsor – Prüfer / Prüfzentrum mit Studienteam zueinander aus datenschutz-rechtlicher Sicht (unabhängig von der Verantwortlichkeit im Sinne von EU-VO 536/2014)

Wer ist verantwortlich für die Erhebung / Pseudonymisierung / Übermittlung etc. der Teilnehmerdaten??

3 Optionen in der DS-GVO

Art. 4 Nr. 7	für die Datenverarbeitung Verantwortlicher
Art. 26	für die Datenverarbeitung gemeinsam Verantwortliche
Artt. 4 Nr. 8, 28	Auftragsverarbeiter

DATENVERARBEITUNG IN DER KLINISCHEN STUDIE

Einordnung des Verhältnisses von Sponsor – Prüfer / Prüfzentrum mit Studienteam zueinander aus datenschutz-rechtlicher Sicht

Gemeinsamer Nenner:

Die datenschutzrechtliche Verantwortlichkeit kann bei klinischen Studien nicht abstrakt festgelegt werden, sondern muss anhand der tatsächlichen Verhältnisse eines konkreten (Einzel-) Falles bestimmt werden. Dabei kommt es immer darauf an, was die beiden Parteien tatsächlich an Aufgaben erledigen.

Dabei wird in Publikationen regelmäßig betont, dass man sich angesichts der Komplexität der Datenverarbeitungsvorgänge in diesem Bereich der Schwierigkeiten bei der Anwendung der festgelegten Definitionen bewusst sei.

So z.B. im WP 169, S. 40 oder im Kurzpapier (KP) Nr. 16 der Datenschutzkonferenz (DSK).

DATENVERARBEITUNG IN DER KLINISCHEN STUDIE

Einordnung des Verhältnisses von Sponsor – Prüfer / Prüfzentrum mit Studienteam zueinander aus datenschutz-rechtlicher Sicht

WP 169 der Art. 29-Gruppe

Beispiel 25 „Klinische Arzneimittelstudien“ S. 36 – Sponsor und Prüfzentrum als gemeinsam für die Verarbeitung Verantwortliche (Art. 26 DS-GVO)

Leitlinien 07/2020 des EDSA, S. 26, Beispiel: Klinische Studien

Für den Fall, dass der Prüfer nicht an der Erstellung eines Prüfplans beteiligt ist (er akzeptiert lediglich den vom Sponsor bereits ausgearbeiteten Prüfplan), und der Prüfplan nur vom Sponsor entworfen wird, sind das Prüfzentrum als Auftragsverarbeiter und der Sponsor als Verantwortlicher für die klinischen Prüfungsdaten zu betrachten (Art. 28 DS-GVO).

Werden Prüfplan/Studienprotokoll gemeinsam erstellt, kann gemeinsame Verantwortlichkeit angenommen werden.

Der EDSA betont, dass die Erhebung personenbezogener Daten aus der Patientenakte zu Forschungszwecken von der Speicherung und Verwendung derselben Daten für die Zwecke der Patientenversorgung zu unterscheiden ist, für die der Gesundheitsdienstleister weiterhin der Verantwortliche bleibt.

DATENVERARBEITUNG IN DER KLINISCHEN STUDIE

Einordnung des Verhältnisses von Sponsor – Prüfer / Prüfzentrum mit Studienteam zueinander aus datenschutz-rechtlicher Sicht

Leitlinien 07/2020 des EDSA, Rn 68:

Allein die Nutzung eines gemeinsamen Datenverarbeitungssystems oder einer gemeinsamen Infrastruktur führt nicht zu einer gemeinsamen Verantwortung, wenn die durchgeführten Verarbeitungen trennbar und ohne Intervention des anderen Beteiligten durchgeführt werden.

Schiemann/Peters/Zumdick, A&R 4/2019, S. 147, 154
Die Einordnung datenschutzrechtlicher Verantwortlichkeiten am Beispiel der klinischen Prüfung

Präferenz für die Einordnung der datenschutzrechtlichen Verantwortlichkeit von Sponsor und Prüfzentrum bei einer klassischen kommerziellen Prüfung als gemeinsame Verantwortlichkeit.

DATENVERARBEITUNG IN DER KLINISCHEN STUDIE

Erläuternde / vertiefende Quellen zum Thema „datenschutzrechtliche Verantwortlichkeit“

- Stellungnahme 1/2010 (WP 169) der Art. 29-Gruppe zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“

- Stellungnahme 3/2019 des EDSA zu den Fragen und Antworten zum Zusammenspiel der VO über klinische Prüfungen und der DS-GVO

- Leitlinien 07/2020 des EDSA zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DS-GVO, Version 2.0

  https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteEDSA_Art29Gruppe/Guidelines/EDPB_20210701.pdf?__blob=publicationFile&v=3

- Mehrere sog. Kurzpapiere der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK)

  https://www.datenschutzkonferenz-online.de/kurzpapiere.html

- Kügel/Müller/Hofmann – Kommentar zum Arzneimittelgesetz (AMG), 3. Auflage von 2022

DATENVERARBEITUNG IN DER KLINISCHEN STUDIE

Kurze Vorstellung eines möglichen weiteren Akteurs bei einer klinischen Studie:

CRO - *Contract Research Organisation* oder *Clinical Research Organization* = Auftragsforschungsinstitut.

Eine CRO wird als Auftragsverarbeiter des Sponsor behandelt, da Letzerer den Zweck und die unverzichtbaren Mittel der klinischen Studie definiert.

Eine CRO erhält wie der Sponsor nur pseudonymisierte Daten.

EUCROF-Verhaltenskodex für Dienstleister in der klinischen Forschung
EUCROF-Kodex am 12. September 2024 endgültig verabschiedet, Beschluss 2024-64 der **CNIL**

https://cro.eucrof.eu/gdpr-form

Derzeit Vorbereitungen zur Einrichtung eines

EUCROF Code of Conduct Supervisory Committee (COSUP), das das Leitungsorgan des Kodex bildet. Der COSUP ist das einzige Gremium, das berechtigt ist, unparteiisch und unabhängig operative Entscheidungen über die Einhaltung des Kodex durch die CROs zu treffen.

DATENVERARBEITUNG IN DER KLINISCHEN STUDIE

Genetische (Art. 4 Nr. 13 DS-GVO) und biometrische (Art. 4 Nr. 14 DS-GVO) Daten

Positionspapier der DSK vom 15. Mai 2024

Anforderungen an die Sekundärnutzung von genetischen Daten zu Forschungszwecken

https://www.datenschutzkonferenz-online.de/media/dskb/2024-05-15_DSK-Beschluss_Genetische-Daten.pdf

In Vorbereitung ist eine Richtlinie des EDSA für die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken mit einem Abschnitt dazu.

PSEUDONYMISIERUNG UND ANONYMISIERUNG

Beides stellt eine Konkretisierung des Grundsatzes der Datenvermeidung und Datensparsamkeit (Art. 5 Abs. 1 lit. c DS-GVO) als einem vorrangigen Ziel des Datenschutzes dar, wonach keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten sind.

Auf das notwendige Maß ist die Datenverarbeitung dann beschränkt, wenn nur solche Daten verwendet werden, ohne die der Zweck der Verarbeitung nicht erreicht werden kann.

Wenn für einen bestimmten Zweck beispielsweise die Verarbeitung des Lebensalters ausreicht, darf nicht das vollständige Geburtsdatum verarbeitet werden.

Dieser Grundsatz erstreckt sich aber nicht nur auf die Menge der verarbeiteten Daten, sondern auch auf die Dauer der Zugänglichkeit.

PSEUDONYMISIERUNG UND ANONYMISIERUNG

Müssen zunächst personenbezogene Daten erhoben werden, kann dem oben genannten Grundsatz und dem Recht auf informationelle Selbstbestimmung aber zu einem späteren Zeitpunkt mit einer Anonymisierung bzw. einer Pseudonymisierung der erhobenen Daten Rechnung getragen werden.

Daraus ergibt sich die Pflicht, in jeder Phase eines Forschungsvorhabens zu prüfen, ob unter Berücksichtigung des Forschungszwecks eine Veränderung der Einzelangaben in der Weise möglich ist, dass diese einer bestimmten Person nicht mehr zugeordnet werden können. Dies kann der Fall sein nach dem Abschluss der Prüfung der Einzelangaben auf Plausibilität.

Art. 89 Abs. 1 DS-GVO

Zur Zeit wird von einer Arbeitsgruppe eine Leitlinie des Europäischen Datenschutzausschusses (EDSA) zur Anonymisierung personenbezogener Daten erarbeitet.

Die Leitlinie 01/2025 des EDSA vom 16.01.2025 zur Pseudonymisierung liegt vor.

PSEUDONYMISIERUNG UND ANONYMISIERUNG

Pseudonymisierung - Art.4 Nr. 5 DS-GVO = die Verarbeitung personenbezogener Daten in einer Weise, dass die personen-bezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Pseudonymisierung

- hat das Ziel, die unmittelbare Kenntnis der vollen Identität des Betroffenen während solcher Verarbeitungs-vorgänge, bei denen ein Personenbezug nicht erforderlich ist, auszuschließen.

- verringert die Verknüpfbarkeit eines Datenbestands mit der Identität einer Person und stellt somit eine sinnvolle Sicherheitsmaßnahme dar.

- kann das Ersetzen des Namens und anderer direkter Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck bedeuten, die Bestimmung einer Person auszuschließen oder wesentlich zu erschweren.

Erlaubnis

PSEUDONYMISIERUNG UND ANONYMISIERUNG

Zuordnungs- bzw. Referenzliste
Im Falle der Verwendung einer Referenzliste werden die eine Person unmittelbar identifizierenden Daten durch eine für das Einzelvorhaben zu bildende Zuordnungsvorschrift derart verändert, dass das so gebildete Pseudonym nur mit Kenntnis dieser Zuordnungsvorschrift wieder einer natürlichen Person zugeordnet werden kann. So wird beispielsweise in einer Tabelle dem Namen eine Forschungs-ID zugeordnet.

Idealerweise werden die Aufgaben auf verschiedene Verantwortliche verteilt. Von einem wird die Pseudonymisierung durchgeführt, ein anderer verwahrt die Zuordnungsregel und wiederum andere dürfen die pseudonymen Forschungsdaten verarbeiten. Erfolgt die Pseudonymisierung zudem von einem vertrauenswürdigen, unabhängigen Dritten (Datentreuhänder oder Vertrauensstelle), wird das Risiko einer Re-Identifizierung weiter gemindert.

Die Berechtigung für den Zugriff auf eine Zuordnungsregel ist festzulegen und technisch und organisatorisch zu gewährleisten. Vorstellbar wäre die Speicherung auf einem Rechner, zu dem nur der Datenschutzbeauftragte eines Unternehmens oder einer Forschungseinrichtung passwortgeschützt Zugriff nehmen kann.

Die Beschäftigten bzw. die Wissenschaftler arbeiten selbst nur mit einem Datensatz, der keine identifizierenden Daten enthält.

Eine vertragliche Verpflichtung zur Vermeidung der Re-Identifizierung von Einzelpersonen kann Pseudonymisierung als organisatorische Maßnahme ergänzen.

PSEUDONYMISIERUNG UND **ANONYMISIERUNG**

Anonym erhobene bzw. im Verlauf der weiteren Datenverarbeitung anonymisierte Daten unterliegen nicht dem Datenschutzrecht. Datenschutzrechtliche Nutzungsbeschränkungen bestehen dann nicht (vgl. Erwägungsgründe 26, 28 zur DS-GVO).

Anonymisierung - Der Prozess, in dessen Verlauf personenbezogene Daten in Daten umgewandelt werden, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder derart in Daten umgewandelt werden, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.

Diskutiert wird darüber, ob Anonymisierung als Phase der Verarbeitung im Sinne von Art. 4 Nr. 2 DS-GVO zu behandeln ist, die einer Erlaubnis bedarf. Für die Artikel-29-Datenschutzgruppe stellt Anonymisierung in ihrer Stellungnahme 05/2014 eine Weiterverarbeitung personenbezogener Daten dar und muss als solche der Anforderung der Vereinbarkeit unter Berücksichtigung der Rechtsgrundlagen und Bedingungen der Weiterverarbeitung entsprechen. Auch von Datenschutzaufsichtsbehörden wird vertreten, dass die Erzeugung anonymisierter Daten aus personenbezogenen Einzelangaben noch den Datenschutzvorschriften unterliegt.

PSEUDONYMISIERUNG UND **ANONYMISIERUNG**

Es gibt **3** unterschiedlich starke Formen der Anonymisierung:

Formal - Löschung von unmittelbar identifizierenden Daten, wie z.B. dem Namen, der Anschrift, Kontonummern oder dem Geburtsdatum

Faktisch - Die Zuordnung einer Einzelangabe zu einer betroffenen Person muss nicht schlechthin ausgeschlossen sein, sondern es genügt für eine erfolgreiche Anonymisierung, wenn eine Zuordnung nach der Lebenserfahrung nicht zu erwarten ist.

Der Begriff des Personenbezuges ist relativ, d.h. es ist auf das konkrete Wissen des Verantwortlichen abzustellen. Die Zuordenbarkeit ist von den individuellen Fähigkeiten dieser Stelle abhängig. Erst wenn die Zuordnung mit den dort zur Verfügung stehenden Hilfsmitteln erfolgen kann, soll ein Personenbezug bestehen.

Absolut - Es reicht jede theoretische, von den tatsächlichen Möglichkeiten des Verantwortlichen losgelöste Verknüpfung zwischen Person und Datum aus. Es wird nicht auf die tatsächlichen Möglichkeiten des Verantwortlichen abgestellt, sondern vielmehr objektiv auf die generell verfügbaren Verknüpfungstechniken oder das in Theorie verfügbare Zusatzwissen, um den Bezug herstellen zu können.

PSEUDONYMISIERUNG UND **ANONYMISIERUNG**

Faktische Anonymität ist letztlich eine Frage der Wahrscheinlichkeit

Zur Beantwortung der Frage, ob trotz erhobener personenbeziehbarer Daten von anonymen Daten auszugehen ist, muss eine Analyse des Risikos für eine Re-Identifizierung im Einzelfall erfolgen.

Das Re-Identifizierungsrisiko bezeichnet die Eintrittswahrscheinlichkeit einer möglichen De-Anonymisierung von faktisch anonymisierten Daten unter Berücksichtigung der aus einer De-Anonymisierung möglicherweise entstehenden Folgen für die betroffene Person.

Werden zu einem wissenschaftlichen Zweck Angaben zu Geschlecht, Alter und Fächerkombination von den Lehrkräften einer überschaubaren Zahl von Grundschulen erhoben, besteht für die Re-Identifizierung einer männlichen Lehrkraft mittleren Alters über die Schul-Homepage einfach zu erlangendes Zusatzwissen wohl ein hohes Risiko.

Für eine HIV-Studie sind möglicherweise komplexere Anonymisierungs-Techniken zu wählen als für eine Studie zum grippalen Infekt.

PSEUDONYMISIERUNG UND **ANONYMISIERUNG**

Kurzer Exkurs

Davon abzugrenzen sind aggregierte Daten.

Solche zusammengefassten Daten, wie z.B. die sich aus einer statistischen Erhebung ergebenden Summenangaben zu den einzelnen Erhebungsmerkmalen, enthalten keine Einzelangaben zu einer Person mehr.

Anonyme Daten enthalten dagegen mindestens eine Einzelangabe über eine Person, ohne dass die Person allerdings bekannt ist.

PSEUDONYMISIERUNG UND **ANONYMISIERUNG**

Grundlegende Verfahren zur Anonymisierung

Generalisierung - ersetzen eines genauen Datums durch einen weniger spezifischen Wert, z.B.

- Vollständiges Geburtsdatum durch Geburtsjahr
- Geburtsjahr durch Zeitraum Lebensalter 50 – 60 Jahre
- die Angabe einer Region statt einer Stadt oder eines Monats statt einer Woche
- …

Randomisierung – eine Reihe von Techniken, welche die Daten in einer Weise verfälschen, dass durch hinzugefügte Daten die direkte Verbindung zwischen Daten und Betroffenem entfernt wird.

Weiterführend beispielsweise Artikel-29-Datenschutzgruppe, WP 216

PSEUDONYMISIERUNG UND **ANONYMISIERUNG**

Risiken für eine robuste Anonymisierung:

- Herausgreifen *oder singling out*, d. h. die Möglichkeit, in einem Datenbestand einige oder alle Datensätze zu isolieren, welche die Identifizierung einer Person ermöglichen

- Verknüpfbarkeit, d. h. die Fähigkeit, mindestens zwei Datensätze, welche dieselbe Person oder Personengruppe betreffen, zu verknüpfen (in derselben Datenbank oder in zwei verschiedenen Datenbanken).

- Inferenz, d. h. die Möglichkeit, den Wert eines Merkmals mit einer signifikanten Wahrscheinlichkeit von den Werten einer Reihe anderer Merkmale abzuleiten.

EUROPEAN HEALTH DATA SPACE (EHDS) - ÜBERBLICK

- 26. März 2025 - Die EHDS-Verordnung ist mit dem Beginn des Übergangszeitraums in Kraft getreten.
- Die Verordnung gilt grundsätzlich ab dem 26. März 2027, wobei bestimmte Regelungen auch erst zu einem späteren Zeitpunkt – 2029 / 2031 / 2035 - gelten (Art. 105 EHDS-VO).
- Die Verordnung hat also keine sofortige Wirkung!

  Vielmehr wurde der Prozess ihrer praktischen Umsetzung durch die Veröffentlichung erst eingeleitet. Während einige Elemente von den Mitgliedstaaten auf freiwilliger Basis bereits jetzt umgesetzt werden können, werden die meisten Verpflichtungen erst vier Jahre nach Inkrafttreten der Verordnung gelten.
- Insbesondere muss in jedem Mitgliedstaat mindestens eine zentrale Zugangsstelle für Gesundheitsdaten (Art. 55 EHDS-VO) aufgebaut werden, die den Zugang zu Gesundheitsdaten verwalten und die Daten auffindbar und verfügbar machen.

EHDS - ÜBERBLICK

Art. 1 Abs. 1 EHDS-VO - Gegenstand

Mit dieser Verordnung wird der europäische Gesundheitsdatenraum („European Health Data Space — EHDS“) mit gemeinsamen Vorschriften, Standards und Infrastrukturen sowie einem Governance-Rahmen geschaffen, um den Zugang zu elektronischen Gesundheitsdaten für die Zwecke der Primärnutzung von Gesundheitsdaten sowie der Sekundärnutzung dieser Daten zu erleichtern.

3 zentrale Ziele des EHDS

- Erleichterter Austausch von Gesundheitsdaten zum Zwecke der Erbringung von Gesundheitsdienstleistungen in der gesamten EU
- Aufstellung einheitlicher Anforderungen für elektronische Systeme für Patientendaten
- Schaffung eines einheitlichen rechtlich-organisatorischen Rahmens für die Weiterverwendung von Gesundheitsdaten

Also - Schaffung von Interoperabilität (Art. 2 Abs. 2 lit. f EHDS-VO) zwischen den Gesundheitssystemen und –diensten in der gesamten EU.

EHDS - ÜBERBLICK

Grundsätzlich unmittelbare Geltung der EHDS-VO in den Mitgliedstaaten!

Aber – sog. Öffnungsklauseln im Text der Verordnung, die Anwendung von Gesetzen der Mitgliedstaaten zulassen.

z.B.

- Art. 3 Abs. 3 – Beschränkung der Zugangsrechte für Patient:innen auf ihre Gesundheitsdaten
- Art. 10 Abs. 1 – Widerspruchsrecht für Patient:innen – Opt-out-Prinzip
- Art. 50 Abs. 2 + Abs. 3 – Pflichten für Gesundheitsdateninhaber

EHDS - ÜBERBLICK

Primärnutzung (Art. 2 Abs. 2 lit. d EHDS-VO) von Gesundheitsdaten mit Electronic Health Record (EHR)-Systeme oder mit Wellness-Anwendungen insbesondere für die Gesundheitsversorgung.

Art. 2 Abs. 2 lit. j + lit. k EHDS-VO
Art. 2 Abs. 2 lit. z / ab EHDS-VO

Sekundärnutzung (Art. 2 Abs. 2 lit. e EHDS-VO) von Gesundheitsdaten auf der Grundlage von gesetzlichen Nutzungsrechten mit Opt out-Recht der Patient:innen (Art. 71 EHDS-VO) u.a. für Forschungszwecke.

Artt. 66, 68 EHDS-VO – grundsätzlich anonymisierte Daten, ausnahmsweise pseudonymisierte Daten

EHDS - ÜBERBLICK

Primärnutzung – Art. 2 Abs. 2 lit. d EHDS-VO

„Verarbeitung elektronischer Gesundheitsdaten für die Gesundheitsversorgung zur Beurteilung, Erhaltung oder Wiederherstellung des Gesundheitszustands der natürlichen Person, auf die sich diese Daten beziehen ….“

Opt-out-Möglichkeit gemäß Digital-Gesetz (DigiG – mit digitalen Lösungen den Versorgungsalltag verbessern)

Sekundärnutzung – Art. 2 Abs. 2 lit. e EHDS-VO

Verarbeitung von Daten, die einer Auswertung *über ihren originären, vorrangigen Verwendungszweck hinaus* zugeführt werden. Maßgeblich für die Einstufung als Sekundärdaten sind Unterschiede zwischen dem primären Erhebungsanlass und der nachfolgenden Nutzung.

Opt-out-Möglichkeit gemäß Gesundheitsdatennutzungsgesetz (GDNG – Forschungsmöglichkeiten verbessern) im Hinblick auf die Daten aus der ePA .

EHDS - ÜBERBLICK

Sekundärnutzung - Art. 53 Abs. 1 EHDS-VO benennt die Zwecke, für die elektronische Gesundheitsdaten zur Sekundärnutzung verarbeitet werden können.

„Die Zugangsstellen für Gesundheitsdaten (Art. 55) gewähren einem Gesundheitsdatennutzer (Art. 2 Abs. 2 lit. u EHDS-VO) nur dann Zugang zu den in Artikel 51 genannten elektronischen Gesundheitsdaten für die Sekundärnutzung, wenn die Verarbeitung der Daten durch diesen Gesundheitsdatennutzer für einen der folgenden Zwecke erforderlich ist: …“

Darüber hinaus dürfen Forschende, Unternehmen oder öffentliche Einrichtungen nur dann auf pseudonymisierte Daten zugreifen, wenn anonymisierte Daten für ihre Zwecke nicht ausreichen. Es ist untersagt, die Identität der betroffenen Personen zu rekonstruieren oder dies auch nur zu versuchen.

WEBANGEBOTE ZUM THEMA

- https://www.datenschutz.rlp.de/
- https://biotech.rlp.de/biotechnologie-rheinland-pfalz
- https://www.datenschutzkonferenz-online.de/

- https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf
- https://www.datenschutzkonferenz-online.de/media/dskb/2024-09-11_DSK_Positionspapier%20_Wissenschaftliche_Forschungszwecke.pdf
- https://datenschutzkonferenz-online.de/media/st/2023-03-27_DSK- Stellungnahme_EHDS.pdf
- https://health.ec.europa.eu/latest-updates/frequently-asked-questions-european-health-data-space-2025-03-05_en?prefLang=de&etrans=de
- https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en

- DIN Medizinische Informatik - Pseudonymisierung (ISO 25237:2017)
- Stiftung Datenschutz – Grundsatzregeln und Praxisleitfaden für die Anonymisierung
- Praxishilfe zur Anonymisierung/Pseudonymisierung - Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS) u.a., Version 2 Stand: 27. Januar 2024
- Health Insurance Portability and Accountability Act 66 (HIPAA)

WEBINAR #3

Einblick in den Internationalen Datentransfer:

- Übersicht über Kapitel V der DS-GVO und die verschiedenen Übermittlungsinstrumente
- Datentransfer in die USA, aktuelle Situation und Ausblick

⇨ Termin im 3. Quartal 2025 (wird rechtzeitig bekannt gegeben)

DANKE FÜR IHRE AUFMERKSAMKEIT!

Der Landesbeauftragte für
den **DATENSCHUTZ** und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

BIONTECH