Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. März 2023

Nutzung von Gesundheitsdaten braucht Vertrauen – Der Europäische Gesundheitsdatenraum darf das Datenschutzniveau der Datenschutz-Grundverordnung nicht aushöhlen

Die betroffenen Personen müssen darauf vertrauen dürfen, dass bei der Verarbeitung ihrer personenbezogenen Daten die Regelungen der europäischen Datenschutz-Grundverordnung (DS-GVO) und ihre Grundrechte nach Artikel 7, 8 der Charta der Grundrechte der Europäischen Union (GRCh) gewahrt bleiben, wie von der EU-Kommission in der Datenstrategie aus dem Jahr 2020[1] ausdrücklich zugesagt.

Auf Grundlage dieser Datenstrategie hat die EU-Kommission bisher mehrere Datengesetze initiiert, um zum gesamtgesellschaftlichen Vorteil einen Binnenmarkt für Daten zu schaffen. Zu einem ersten sektorenspezifischen Datenraum hat sie im Mai 2022 einen Verordnungsentwurf (EHDS-VO-E[2]) zur Schaffung und Regulierung eines Europäischen Gesundheitsdatenraums (European Health Data Space – EHDS) vorgestellt.

Der Entwurf der EHDS-Verordnung enthält Regelungen zur europaweiten Primärnutzung der elektronischen Gesundheitsdaten, um bei Gesundheitsversorgung auch auf Informationen aus den Systemen der anderen Mitgliedsstaaten zugreifen zu können. Von wesentlicher Bedeutung ist darüber hinaus die Regulierung der Sekundärnutzung von elektronischen Gesundheitsdaten, vor allem für Zwecke der Forschung, die u. a. eine zentrale Zugangsstelle vorsieht, die den Zugang zu den elektronischen Gesundheitsdaten vermittelt.

---

[1] Europäische Kommission, Mitteilung COM(2020) 66: „Eine europäische Datenstrategie“ vom 19. Februar 2020.

[2] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen europäischen Raum für Gesundheitsdaten vom 3. Mai 2022 (2022/0140).

Diese Regelungen dürften als Blaupause für weitere Datenräume im Europäischen Raum dienen. Neben der Tatsache, dass im EHDS besonders sensible Daten verarbeitet werden, unterstreicht diese „Vorreiterrolle“ die besondere Bedeutung der EHDS-VO.

Für die Errichtung des EHDS ist das Grundrecht auf Datenschutz bzw. auf informationelle Selbstbestimmung u. a. mit dem öffentlichen Interesse an wissenschaftlicher Forschung in einen **angemessenen Ausgleich** zu bringen.[3] Hier greift der Verordnungsentwurf allerdings deutlich zu kurz.

A. Grundsätzliche Erwägungen

Betroffenenrechte

Die DSK begrüßt das Regulierungsvorhaben, soweit es die Rechte der betroffenen Patientinnen und Patienten bei der Primärnutzung von elektronischen Gesundheitsdaten – insbesondere die Portabilität – aufwertet. Sie erkennt an, dass für die grenzüberschreitende Behandlung, für Forschungszwecke sowie für öffentliche Zwecke von hoher Bedeutung Datenzugangsrechte geschaffen werden sollen. Gleichzeitig gilt insbesondere im Rahmen der Sekundärnutzung: Der Mensch muss erkennbar im Mittelpunkt stehen. Daraus folgt, dass diejenigen, deren personenbezogene Daten den wissenschaftlichen und wirtschaftlichen Mehrwerten zugrunde liegen, **eingebunden** sein und ihre **Rechte aus der DS-GVO** auf einfache Weise und granular realisieren können müssen. Ausschlüsse oder Beschränkungen von Betroffenenrechten müssen mit den Grundrechten vereinbar sein. Die Betroffenenrechte der DS-GVO dürfen nicht verkürzt werden.

Die betroffenen Personen müssen **eine effektive Kontrolle** über die Verarbeitung ihrer personenbezogenen Daten behalten. Hierfür sind präzise und leicht verständliche Informationen **der Verantwortlichen** elementar. Sämtliche Übermittlungswege und Verarbeitungsprozesse müssen für die Betroffenen **transparent** sein.

Rechtsklare Regelungen

Es bedarf rechtsklarer Regelungen, die erkennen lassen, ob und in welchem Umfang die Verarbeitung personenbezogener Daten umfasst und zulässig ist. Die Regelungen

[3] Vgl. hierzu auch: EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space vom 12. Juli 2022,

müssen konform mit den Grundrechten sein, wonach wesentliche Festlegungen, insbesondere zu Umfang, Art und Zwecken der Datenverarbeitungen, in der Verordnung selbst zu treffen sind.

Technische und organisatorische Maßnahmen

Die Verarbeitung der Gesundheitsdaten unterliegt nach der DS-GVO einem hohen Schutzbedarf, der in den technischen und organisatorischen Maßnahmen umzusetzen ist. Dazu gehören auch die **Ende-zu-Ende-Verschlüsselung, die Pseudonymisierung bzw. die Anonymisierung** sowie ein wirksames **Löschkonzept**.

Der EHDS-VO-E lässt bisher jedoch offen, wie die Daten anonymisiert werden können. Eine rechtsklare Regelung der Anforderungen an Methoden und Wirkungen der Anonymisierung könnte die rechtssichere Datennutzung unterstützen.

Die betroffenen Personen haben ein Recht auf **sichere und vertrauliche Verarbeitung** ihrer Gesundheitsdaten. Da sich bei der Verarbeitung von Gesundheitsdaten Risiken nicht gänzlich ausschließen lassen, sind geeignete Garantien mit Transparenz und durch Anwendung von Methoden im Sinne von „Data Protection by Design“ und „Data Protection by Default“ vorzusehen. Beispielsweise muss es den betroffenen Personen mittels **digitaler Management-Systeme** möglich sein, ihre elektronischen Gesundheitsdaten auch im EHDS unter angemessenen technischen und rechtlichen Bedingungen **kontrollieren** zu können.

B. Verhältnis zu anderen Rechtsakten, Begriffe und Datenkategorien

Gewährleistung des DS-GVO-Schutzniveaus

Die Vorgaben der DS-GVO zu Datenschutz und Datensicherheit dürfen durch die EHDS-VO nicht ausgehöhlt werden; sie sind Grundlage für das Vertrauen der betroffenen Personen. Die **datenschutzrechtlichen Grundsätze**, wie der Grundsatz der Datenminimierung, der Datenrichtigkeit, der Speicherbegrenzung, der Integrität und Vertraulichkeit und das Erforderlichkeitsprinzip müssen gewährleistet werden. Es ist klarzustellen, dass die EHDS-VO-E den Rechtsrahmen der DS-GVO respektiert, die dort vorgesehenen Regelungsräume also nutzt, aber nicht das Schutzniveau unterläuft. Gerade bei besonders schützenswerten Gesundheitsdaten dürfen die grundrechtlich garantierten und in der DS-GVO vorgesehenen Betroffenenrechte nicht entwertet

werden. Dies gilt auch für die Sekundärnutzung von elektronischen Gesundheitsdaten; hier ist bisher nicht erkennbar, ob und, wenn ja, inwieweit nach dem Regelungsentwurf den Betroffenen überhaupt Rechte zustehen sollen.

Verhältnis zu weiteren Rechtsakten

Zudem muss sich die EHDS-VO hinsichtlich der **Begriffe und Definitionen** sowie des Anwendungsbereichs kohärent und konsistent in das Regelungssystem der weiteren Rechtsakte wie des Data Governance Act, des Data Act und des Artificial Intelligence Act einfügen.

Im Bezug zur JI-Richtlinie[4] wird an die Problematik erinnert, die bei elektronischen Datensammlungen entsteht. Insbesondere dürfen den Strafverfolgungsbehörden durch die EHDS-VO keine Zugriffsrechte auf gesundheitsbezogene Daten ermöglicht werden. Dies ist durch eine klare Zweckbindungsregelung sicherzustellen.

Datenkategorien

Außerdem müssen die in Artikel 33 EHDS-VO-E genannten Datenkategorien begrenzt werden: Da die EHDS-Verordnung ermöglichen soll, elektronische Gesundheitsdaten für die Förderung der individuellen Gesundheit und der öffentlichen Gesundheit, insbesondere im Rahmen von Forschungsvorhaben, bereitzustellen, sollten auch **nur hierfür geeignete** personenbezogene Daten vom Anwendungsbereich der Verordnung umfasst sein. Die Datensätze insbesondere aus Wellness-Anwendungen sind aus dem Anwendungsbereich der EHDS-VO zu entfernen, da der Erkenntnisgewinn unklar bleibt. Diese Daten bieten voraussichtlich nicht die erforderliche Richtigkeitsgewähr und Qualität und können zugleich mit einer hohen Eingriffsintensität hinsichtlich des Verhaltens der betroffenen Personen verbunden sein. Die Aufnahme von Daten zu gesundheitsrelevanten Faktoren, einschließlich sozialer, umweltbedingter und verhaltensbezogener Gesundheitsfaktoren, Lebensstil, Wohlbefinden und Verhaltensdaten, ist ebenfalls kritisch zu sehen. Ihre Verarbeitung sollte nur für näher zu bestimmende Zwecke zugelassen werden. Die Regelung zur Bereitstellung von persönlichen **Genomdaten** greift in den intimsten Bereich der betroffenen Personen und ihrer Angehörigen ein und ist daher von Grundrechts wegen zu streichen.

[4] Richtlinie EU 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016.

C. Datenverarbeitung zum Primärzweck und Electronic Health Record (EHR)-Systeme

Primärzweck: Behandlung

Die **Patientensouveränität** darf durch die neuen europaweiten Regelungen nicht eingeschränkt werden. Die Datenverarbeitung für den Primärzweck, also der medizinischen Behandlung, ist nur mit der **effektiven Kontrollmöglichkeit** und einer aktiven Mitwirkung der betroffenen Personen, also der Patientinnen und Patienten zulässig. Es muss sichergestellt sein, dass sie über Verarbeitungsvorgänge und insbesondere – zur Wahrung des Patientengeheimnisses – über Übermittlungen an andere verantwortliche Stellen informiert und damit einverstanden sind.

EHR-Systeme

Electronic Health Record-Systeme (EHR-Systeme), d. h. Geräte oder Software, die vom Hersteller dazu bestimmt sind, elektronische Patientenakten zu speichern, zu vermitteln, zu importieren, zu exportieren, zu konvertieren, zu bearbeiten oder anzuzeigen, müssen von einer **unabhängigen Stelle** unter Beteiligung der Datenschutz-Aufsichtsbehörden **zugelassen** werden, bevor sie in Betrieb genommen werden, damit die nötigen hohen Anforderungen an die Sicherheit und die Ausgestaltung der Datenverarbeitung erfüllt sind. Sie müssen eine sichere Ende-zu-Ende-Verschlüsselung gewährleisten und **Anonymisierungs- und Pseudonymisierungskomponenten** enthalten. Technische und organisatorische Maßnahmen, wie die Authentifizierung, müssen ein **hohes Sicherheitsniveau** gewährleisten. Das **Management** des EHR-Systems muss **effektiv und granular** ausgestaltet sein und auch solchen betroffenen Personen zur Verfügung stehen, die keine vertieften Digitalkenntnisse oder keine mobilen Endgeräte haben. Insbesondere müssen die Patientinnen und Patienten Nutzungsbeschränkungen und Berechtigungen auf leichte Art und **barrierefrei** einrichten können.

Die **Zugriffsstrukturen** im EHR-System haben dem bei Gesundheitsdaten vermuteten hohen Risiko für die Rechte und Freiheiten natürlicher Personen Rechnung zu tragen, sodass das **Risiko** eines Missbrauchs, insbesondere mit zeitlich beschränkbaren Zugangsrechten je nach Erforderlichkeit kontinuierlich **minimiert** wird. Der Zugriff im Notfall muss auf einen definierten, strukturierten und begrenzten Datensatz erfolgen, um wirksam zu sein. Um den Zugriffschutz des restlichen EHR-Systems nicht zu unterlaufen, muss der **Notfalldatensatz technisch getrennt** vorgehalten werden.

D. Datenverarbeitung zu weiteren Zwecken (Sekundärnutzung)

Paradigmenwechsel und Patientensouveränität

Der EHDS-VO-E bedingt einen Wechsel der relevanten Grundlage für die Sekundärnutzung von erheblicher Tragweite. Es werden umfangreiche **gesetzliche Nutzungsrechte** vorgesehen, die in die Rechte der Betroffenen eingreifen. Um den Kernbereich der Grundrechte zu gewährleisten, sind daher die Betroffenen in **geeigneter Weise einzubinden**, auch dann, wenn auf eine aus datenschutzrechtlicher Sicht vorzuziehende Zustimmung (Opt-in) verzichtet wird, z. B. indem zumindest ein niederschwelliges **Widerspruchsrecht** (Opt-out) vorgesehen wird. Zur Verwaltung von Widerspruch oder Zustimmung zu bestimmten Datenverarbeitungen oder Zwecken sollten **digitale Managementsysteme** verwendet werden.[5]

Außerdem müssen zu den in Artikel 34 EHDS-VO-E genannten Zwecken **entsprechende Garantien und Bedingungen** im Sinne von Artikel 9 Abs. 2 DS-GVO festgelegt werden. Der Grundsatz der **Verhältnismäßigkeit** erfordert, dass, je sensibler persönliche Daten sind, umso strenger auch die Anforderungen an deren Verarbeitung sein müssen.

Der Zielsetzung des EHDS als Förderungsinstrument für die wissenschaftliche Forschung und die öffentlichen Interessen entsprechend muss die sekundäre Datennutzung stets dem Allgemeinwohlinteresse dienen. Die im EHDS-VO-E ausgewiesenen **Zwecke müssen im Einklang mit den Vorgaben der DS-GVO** für besonders zu schützende Daten stehen und durch entsprechende Garantien flankiert werden. Insbesondere muss die sachgerechte Prüfung der Anträge auf zulässige Zwecke und den erforderlichen Datenumfang sichergestellt sein; eine automatische Zulassung einer Datennutzung nach Ablauf der Antragsbearbeitungsfrist ist unzulässig**.**

[5] Petersberger Erklärung der DSK zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung vom 24.11.2022, S. 7.

Einwilligungsbasierte neben gesetzlich geregelter Forschung

Einwilligungsbasierte Forschung wie in klinischen Studien muss unabhängig von der EHDS-Verordnung bestehen bleiben. Die freiwillige datenschutzrechtliche Einwilligung als Grundlage für die Datennutzung kann dem hohen Gut des Rechts auf informationelle Selbstbestimmung unmittelbar Ausdruck verleihen.

Spezifische Dateninhaber

Der Begriff des Dateninhabers muss klargestellt und begrenzt werden. Dabei sind auch die Rechtsverhältnisse der Dateninhaber mit den jeweiligen betroffenen Personen und die sich aus entsprechenden **Vertrauensverhältnissen ergebenden Schweigepflichten** wie Arztgeheimnis, Berufsgeheimnis, Sozialgeheimnis, aber auch Geschäftsgeheimnisse zu berücksichtigen.

Dateninfrastruktur und Zugangsstelle für elektronische Gesundheitsdaten

Die Datenverarbeitungen in der Dateninfrastruktur und bei der Zugangsstelle für die elektronischen Gesundheitsdaten müssen den technischen und organisatorischen Maßgaben der DS-GVO entsprechend ein **hohes Sicherheitsniveau** umsetzen. Die Aufgaben und die Verfahren bei der Zugangsstelle müssen so konzipiert sein, dass insbesondere die **Grundsätze der Datenminimierung und Erforderlichkeit** gewahrt werden und die noch einzuräumenden Betroffenenrechte barrierefrei ausgeübt werden können. Die Aufgaben sollten daher auf verschiedene Verantwortliche aufgeteilt werden. So müssen unabhängige **Vertrauensstellen** die Aufgabe der **Pseudonymisierung** übernehmen, während die Zugangsstellen die Koordinierung und Verwaltung der Dateninfrastruktur und die Bearbeitung der Antragsverfahren übernehmen. Für die Bereitstellung der Daten in einer sicheren Verarbeitungsumgebung können auch unabhängige **Treuhandplattformen** eingerichtet werden.

Dabei sind die **datenschutzrechtlichen Verantwortlichkeiten** aller beteiligten Stellen **lückenlos** festzulegen, damit betroffene Personen ihre Datenschutzrechte wirksam ausüben können.

Die im Entwurf der Kommission vorgesehene **zentrale** Zusammenführung von **Klardaten**, also von Datensätzen mit identifizierenden Angaben, bei der Zugangsstelle birgt

hohe Risiken und ist **unzulässig.** Die Daten sind vor der anlassbezogenen und temporären Zusammenführung **zu pseudonymisieren oder zu anonymisieren.**[6]

[6] Vgl. Seite 3 Ziffer 3 Satz 1 der Petersberger Erklärung der DSK zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung vom 24.11.2022.