

Landtag
Nordrhein-Westfalen
18. Wahlperiode

**Information
18/99**

Alle Abgeordneten

Landesbeauftragte
für Datenschutz und Informationsfreiheit
des Landes Nordrhein-Westfalen



LDI NRW, Postfach 20 04 44, 40102 Düsseldorf

Datum: 29. November 2023

Aktenzeichen
30.6.1

An den
Präsidenten des Landtags Nordrhein-Westfalen
Herrn André Kuper
Platz des Landtags 1
40221 Düsseldorf

Telefon 0211 38424-309

per E-Mail an: praesident@landtag.nrw.de

Entschlüsseungen der 106. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)

Sehr geehrter Herr Landtagspräsident,


die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat auf ihrer letzten Sitzung mit Blick auf das Gesundheitswesen folgende zwei Entschlüsseungen gefasst:

- Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register,
- Datenschutz in der Forschung durch einheitliche Maßstäbe stärken.

Ich leite Ihnen diese Entschlüsseungen im Anhang dieser E-Mail zu Ihrer Information und zur Information der Abgeordneten weiter.

Die Entschlüsseungen sind auch zu finden unter
<https://www.datenschutzkonferenz-online.de/entschliessungen.html>.

Mit freundlichen Grüßen


Bettina Gayk

Kavalleriestraße 2-4
40213 Düsseldorf
Telefon 0211 38424-0
poststelle@ldi.nrw.de

Entschließung

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 23. November 2023

Datenschutz in der Forschung durch einheitliche Maßstäbe stärken

Medizinische Forschungsprojekte werden in Deutschland häufig nicht nur in einem Bundesland durchgeführt. Vielmehr sind zunehmend verschiedene Forschungseinrichtungen aus unterschiedlichen Ländern daran beteiligt (z. B. länderübergreifende Verbundforschung, multizentrische Studien). Je nach Forschungsstandort sind unterschiedliche datenschutzrechtliche Anforderungen zu beachten. Dies erschwert nicht nur die Forschung, sondern wirkt sich auch nachteilig auf den Datenschutz für die betroffenen Personen aus. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert den Bundesgesetzgeber und die Landesgesetzgeber daher auf, durch aufeinander abgestimmte gesetzliche Regelungen auf hohem Datenschutzniveau den Datenschutz in der länderübergreifenden Forschung zu stärken. Hierfür hat sie Eckpunkte erarbeitet. Im Einzelnen:

In vielen Ländern enthalten verschiedene Landesgesetze, die beispielsweise die Datenverarbeitungen durch Krankenhäuser und Behörden des öffentlichen Gesundheitsdienstes betreffen, konkrete Befugnisse der jeweiligen Stellen zur Verarbeitung von Gesundheitsdaten zu Forschungszwecken, die den allgemeinen Vorgaben vorgehen. Diese gesetzlichen Regelungen stellen unterschiedliche datenschutzrechtliche Anforderungen. Bei länderübergreifender Forschung müssen von den Verantwortlichen die jeweils für sie geltenden Gesetze angewandt werden. Unterschiede bestehen insbesondere in Bezug auf die Zulässigkeit der Datenverarbeitung (gesetzliche Grundlage oder Einwilligung mit jeweils unterschiedlichen Anforderungen), die Definition von Schutzbereichen (u. a. Patientinnen und Patienten, Angehörige) und zulässige Zwecke der Verarbeitung. Die rechtliche Bewertung und Umsetzung der jeweils geltenden Rechtsgrundlage führte in der Vergangenheit zu einem gesteigerten Beratungsbedarf und zu Unsicherheiten bei den Forschenden und Rechtsanwendern. Auch ergeben sich aus unterschiedlichen Regelungen Herausforderungen

für eine transparente und verständliche Informationserteilung nach Artikel 13 und 14 der Datenschutz-Grundverordnung (DSGVO).

Das Bundesgesundheitsministerium hat mit dem Gesetzentwurf eines Gesundheitsdatennutzungsgesetzes (GDNG) eine Vereinheitlichung der forschungsrelevanten Rechtsgrundlagen vorgeschlagen. Geplant ist insoweit eine Rechtsgrundlage für die „Weiterverarbeitung von Versorgungsdaten zur Qualitätssicherung, zur Förderung der Patientensicherheit und zu Forschungszwecken“ durch eine Gesundheitseinrichtung für die bei ihr rechtmäßig gespeicherten Daten.

Das Verhältnis dieser geplanten Neuregelungen zu den Landeskrankenhausgesetzen ist jedoch unklar. Mit der Gesetzgebungskompetenz der Länder für den Bereich der Krankenhäuser hat sich der Gesetzentwurf nicht auseinandergesetzt. Daher bestehen erhebliche Zweifel, dass mit diesem Gesetzentwurf eine rechtssichere und tragfähige Neuregelung erreicht wird, die die länderübergreifende Forschung erleichtert.

Die DSK hat in ihrer Stellungnahme zum GDNG-Gesetzentwurf vom 14.08.2023 hierauf hingewiesen und weiteren Korrekturbedarf aufgezeigt.¹

In dieser Stellungnahme und in der „Petersberger Erklärung“ vom 24.11.2022 hat die DSK wichtige Hinweise für gesetzliche Neuregelungen formuliert.² Sie beschreiben wesentliche Anforderungen zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung, insbesondere zu den Rechtsgrundlagen und den besonderen Einwirkungsmöglichkeiten für betroffene Personen.

Um eine weitgehende Nutzung von Gesundheitsdaten zu Forschungszwecken im Einklang mit den Grundrechten zu normieren, sind konkrete Garantien und Maßnahmen gesetzlich festzulegen. Es gilt der Grundsatz: Je höher der Schutz der betroffenen Personen durch geeignete Garantien und Maßnahmen, desto umfangreicher und spezifischer können die Daten zu Forschungszwecken genutzt werden.³ Abhängig von den jeweils verarbeiteten Datenarten – z. B. personenbezogenen Daten (Art. 4 Nr. 1 DSGVO), Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) oder genetische Daten

¹ Die Stellungnahme der DSK vom 14.08.2023 zum Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG – Stand 03.07.2023) ist abrufbar unter https://datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf.

² Die EntschlieÙung der DSK vom 24.11.2022 (Petersberger Erklärung) ist abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf.

³ Vgl. Empfehlung Nr. 2 der Petersberger Erklärung.

(Art. 4 Nr. 13 DSGVO) – bedarf es eines angemessenen Schutz- und Vertrauensniveaus und spezifischer Regelungen für die Verarbeitungen in den jeweiligen Bereichen der Forschung.

Für besondere Forschungsgegenstände, bei denen eine ausreichende Anonymisierung nicht immer gewährleistet werden kann (etwa für radiologische Bilddaten), sollten spezifische Regelungen getroffen werden, um einen angemessenen Schutz der Grundrechte der betroffenen Personen sicherzustellen, z. B. durch zusätzliche technische und organisatorische Maßnahmen.

Darüber hinaus sind die Regelungen des Art. 9 Abs. 2 lit. j i. V. m. Art. 89 Abs. 1 DSGVO zu beachten. Insbesondere müssen im Gesetz selbst angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person festgelegt werden. Diese Festlegung der spezifischen Anforderungen darf nicht an die Verantwortlichen delegiert werden. Die Umsetzung darf sich auch nicht in generalklauselartigen oder in solchen Regelungen erschöpfen, die die DSGVO ohnehin für die Datenverarbeitung vorsieht, wie etwa die Betroffenenrechte nach Art. 15 ff. DSGVO oder Maßnahmen nach Art. 32 DSGVO. Stattdessen müssen konkrete Maßnahmen benannt werden.

Angemessene und spezifische Maßnahmen in diesem Sinne können etwa sein:

- Vorgaben für die Datenschutz-Folgenabschätzung (z. B. Betrachtungstiefe, Aufgabenzuweisungen für die Durchführung),
- die Schaffung weiterer, über die in Art. 15 ff. DSGVO hinausgehender Betroffenenrechte (z. B. spezifische Widerspruchsrechte, Vernichtung von Bioproben),
- die Festlegung angemessener Sperrfristen, die den betroffenen Personen ermöglichen, ihre Rechte auszuüben, bevor mit ihren Daten geforscht werden darf (z. B. bei einem Widerspruchsrecht),
- die Einbindung einer unabhängigen Treuhandstelle insbesondere zur Verschlüsselung, Anonymisierung oder Pseudonymisierung der Daten,
- die Einrichtung von Datenintegrationszentren oder Forschungsplattformen, soweit konkrete, der DSGVO entsprechende Anforderungen an deren Ausgestaltung formuliert werden,

- die Verpflichtung beteiligter Stellen zur Verschwiegenheit und die Schaffung korrespondierender Prozessrechte wie ein Beschlagnahmeverbot und Zeugnisverweigerungsrechte,
- konkrete Festlegungen zur Ausgestaltung und Gewährleistung der Datenminimierung.

Diese Aufzählung ist nicht abschließend. Es ist die Aufgabe des Gesetzgebers, die Risiken zu erkennen, die mit einer Verarbeitung von Gesundheitsdaten verbunden sind, sie zu benennen und ihnen angemessene Schutzmaßnahmen für die Rechte und Interessen der betroffenen Personen gegenüberzustellen.

Die DSK weist darauf hin, dass medizinische personenbezogene Daten in bestimmten Fallkonstellationen dem absoluten Schutz des Kernbereichs privater Lebensgestaltung unterliegen.

Die Verarbeitung solcher menschenwürderelevanter Daten kann selbst zu Forschungszwecken nicht auf Grundlage einer gesetzlichen Regelung legitimiert werden.

Schließlich ist eine uneingeschränkte Datenschutzaufsicht in dem sensiblen Bereich der Verarbeitung von Gesundheitsdaten zu garantieren. Diese bietet Schutz für die betroffenen Personen. Etwaig bestehende Einschränkungen der Befugnisse der Datenschutzaufsichtsbehörden hinsichtlich der Verhängung von Bußgeldern und des Vollzugs gegenüber öffentlichen Stellen sind zumindest im Anwendungsbereich entsprechender Regelungen aufzuheben.

Die DSK setzt sich für die Schaffung eines hohen Datenschutzniveaus in der medizinischen Forschung durch eine aufeinander abgestimmte zeitnahe rechtsklare und systematische Neustrukturierung der entsprechenden rechtlichen Regelungen ein. Sie appelliert an die Gesetzgeber des Bundes und der Länder, durch klarstellende Regelungen einen wirksamen Kernbereichsschutz sicherzustellen.

Die Datenschutzaufsichtsbehörden bieten an, in Wahrnehmung ihrer Beratungsfunktion die Gesetzgeber vor und bei entsprechenden Gesetzesvorhaben zu unterstützen.

Entschließung

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 22./23. November 2023

Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register

Das Vorhaben der Bundesregierung, für die ausgesprochen heterogene Vielfalt medizinischer Register einen allgemeinen Rahmen und eine einheitliche Basis zu schaffen, um Daten im öffentlichen Interesse nutzen zu können, ist aus datenschutzrechtlicher Perspektive nachvollziehbar. Allerdings muss sichergestellt sein, dass auch im konkreten Anwendungsfall die datenschutzrechtlichen Vorgaben eingehalten werden und das Grundrecht auf Datenschutz stets gewährleistet ist. Sowohl für die Befüllung der Register als auch für die registerinterne Verarbeitung und die Bereitstellung sowie die mögliche Nutzung der Daten durch Dritte sind die spezifischen datenschutzrechtlichen Voraussetzungen für die Verarbeitung von Gesundheitsdaten, insbesondere aus Art. 9, 25, 32 und ggf. Art. 89 Abs. 1 DSGVO, maßgeblich.

Es gibt eine Vielzahl medizinischer Register in Deutschland in unterschiedlichen Strukturen und Formen. Wenige sind spezialgesetzlich geregelt oder basieren auf allgemeinen gesetzlichen Grundlagen. Die meisten stützen sich zur Datenverarbeitung auf Einwilligungen: verschiedene stammen aus abgeschlossenen Forschungsvorhaben, andere werden auf Patienteninitiative oder von Fachgesellschaften zu bestimmten Erkrankungen betrieben; nicht alle werden noch aktiv genutzt.

Anknüpfend an die Festlegungen im Koalitionsvertrag „Mehr Fortschritt wagen“ vom November 2021 (S. 83), wonach neben einem Gesundheitsdatennutzungsgesetz auch ein Registergesetz im Einklang mit der DSGVO geschaffen werden soll, sieht die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) Anlass, ergänzend zu ihren bisherigen Forderungen und Empfehlungen die datenschutzrechtlichen Anforderungen und Bedingungen für die Regulierung einer

Datenverarbeitung in medizinischen Registern zu präzisieren. Soweit die Datenverarbeitung den Zwecken wissenschaftlicher Forschung dient, gelten daneben die Hinweise in der „Petersberger Erklärung“ der DSK aus dem November 2022.¹

Die DSK begrüßt, dass durch das vom Bundesministerium für Gesundheit (BMG) beauftragte Gutachten zur Weiterentwicklung medizinischer Register² ein nahezu vollständiger Überblick³ über die vorhandenen Register und die darin enthaltenen Daten vorliegt. Zugleich schließt sich die DSK der darin enthaltenen Empfehlung an, durch die nun geplante Gesetzgebung ein entsprechendes Registerverzeichnis zu verstetigen und dauerhaft öffentlich zugänglich zu gestalten. Die DSK befürwortet insbesondere die Überlegungen zur Schaffung einer Zentralstelle für medizinische Register, die das Registerverzeichnis führen und die eine Auditierung und Zuordnung medizinischer Register je nach vorhandener Qualitätsstufe (im Gutachten als „Reifegrad“ bezeichnet) verantworten soll. Aufgrund der Aufgaben der Zentralstelle für medizinische Register, die maßgeblich für die weitere Verarbeitung der in den medizinischen Registern enthaltenen Daten sind, hält es die DSK für geboten, hiermit eine unabhängige Körperschaft des öffentlichen Rechts zu betrauen. Dieser Zentralstelle könnte zudem eine besondere Funktion als Ansprechpartner und Lotse für die betroffenen Personen sowie bei der Erfüllung der Betroffenenrechte zukommen.

Die DSK teilt das aus dem Koalitionsvertrag erkennbare Anliegen, durch die gesetzliche Regelung die bislang heterogene Registerlandschaft zu strukturieren und zum Aufbau fachlich qualitätsgesicherter Register beizutragen. Entsprechend den Ausführungen im Gutachten bietet es sich an, bei der Zuordnung der Register je nach Qualitätsstufe zu verschiedenen Kategorien die Datenqualität, die Datenstruktur und die Standards bei der Verarbeitung zu berücksichtigen.

Insbesondere folgende Rahmenbedingungen sind aus datenschutzrechtlicher Sicht bei der gesetzlichen Regulierung medizinischer Register vorzusehen:

- Werden personenbezogene Daten an die Register übermittelt und von diesen erhoben, die nicht unmittelbar für das Register, sondern zu einem anderen

¹ Entschließung der DSK „Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung“ vom 24. November 2022.

² Gutachten zur Weiterentwicklung medizinischer Register zur Verbesserung der Dateneinspeisung und -anschlussfähigkeit, TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. und BQS – Institut für Qualität und Patientensicherheit, 29. Oktober 2021.

³ Unter dem Link: <https://registersuche.bqs.de/search.php> sind ca. 400 Register gelistet.

Zweck erhoben worden sind, bedarf es hierfür – soweit dies nicht durch Einwilligungen gedeckt ist – klarer gesetzlicher Festlegungen zu den Voraussetzungen der zweckändernden Datenverarbeitung, die den Anforderungen aus Art. 6 Abs. 4 DSGVO entsprechen.

- Es sind rechtsklare und verhältnismäßige Regelungen über die Aufbewahrungsdauer und Löschfristen der Registerdaten unter der Maßgabe der Grundsätze der Datenminimierung und Speicherbegrenzung zu treffen.
- Eine Befugnis zur Übermittlung von personenbezogenen Gesundheitsdaten an das Register, zu deren Speicherung im Register sowie zu deren Übermittlung an Dritte unter Verzicht auf eine vorherige Einbindung der betroffenen Person bedarf mindestens der medizinisch-fachlichen Erforderlichkeit für einen der in Art. 9 Abs. 2-4 DSGVO genannten Zwecke, der gesetzlichen Definition der zu verarbeitenden personenbezogenen Daten und bei Forschungszwecken dienenden Registern eines allgemeinen, voraussetzungslosen Widerspruchsrechts.
- Bei der Festlegung von Voraussetzungen für eine datenschutzkonforme Verarbeitung von Registerdaten, insbesondere den Anforderungen für die Übermittlung an und Erhebung durch die Register, die weitere Verarbeitung der Daten in den Registern und deren Bereitstellung für Dritte, sowie einer Definition der zu verarbeitenden Einzelangaben, sind außer den Maßgaben der Öffnungsklauseln nach Art. 9 Abs. 2 DSGVO und ggf. den Garantien nach Art. 89 Abs. 1 DSGVO auch die Vorgaben des Grundrechts auf Datenschutz zu berücksichtigen. Insbesondere müssen sich wesentliche Grundrechtseinschränkungen unmittelbar aus dem Gesetz ergeben.
- Bei den gesetzlichen Regelungen sollte die Rechtmäßigkeit der Datenverarbeitung abhängig von dem jeweiligen Zweck differenziert festgelegt werden. Eine Nutzung zur wissenschaftlichen Forschung erfordert beispielsweise andere Bedingungen als eine Auswertung zu Zwecken einer – gesetzlich jeweils näher zu bezeichnenden – Qualitätssicherung. Dies muss berücksichtigt werden.
- Die DSK hält es für erforderlich, dass mit der gesetzlichen Regulierung der medizinischen Register auch Vorgaben zu technisch-organisatorischen Maßnahmen standardisiert und harmonisiert festgelegt werden. Damit wird das dem Risiko angemessene Schutzniveau für die Verarbeitungen verdeutlicht und eine effektive Datenschutzaufsicht ermöglicht. Insbesondere bei

besonderen Risiken, wie zum Beispiel einem Remotezugriff auf Gesundheitsdaten über digitale Portale, wird dem Gesetzgeber empfohlen, im Rahmen einer sog. gesetzlichen Datenschutz-Folgenabschätzung (DSFA) globale Risiken der Registersysteme zu ermitteln und so geeignete technische und organisatorische Maßnahmen zur Minimierung dieser Risiken bereits im Gesetz zu regeln. Dies kann die Verantwortlichen zwar nicht vollständig von einer eigenen DSFA entlasten, trägt aber zur Schaffung einheitlicher Mindeststandards bei.

- Die DSK empfiehlt, durch die gesetzlichen Regelungen digitale Methoden u.a. für das Einwilligungsmanagement und die Ausübung der Betroffenenrechte zu fördern sowie – beispielsweise durch Portale – eine Partizipation der Betroffenen zu ermöglichen.
- Die DSK hält es grundsätzlich für tragfähig, für qualitätsgesicherte Register ein Zulassungsverfahren vorzusehen mit dem Ziel, dass für bestimmte im Registerverzeichnis entsprechend gelistete Register bestehende oder noch zu schaffende gesetzliche Datenverarbeitungsbefugnisse herangezogen werden können. Dabei ist hinsichtlich der einzelnen Verarbeitungsschritte der Übermittlung an das Register, der Erhebung und der Bereitstellung der Daten durch das Register sowie der Verwendung bei der weiteren Nutzung der Registerdaten zu differenzieren.
- Für die Register sollten regelmäßig unabhängige Vertrauensstellen vorgesehen werden. Diese könnten eine zentrale Rolle bei der Anonymisierung und Pseudonymisierung von Gesundheitsdaten vor der Bereitstellung für Forschende und bei der Verwaltung bereichsspezifischer Kennzeichen als einheitliche Identifikatoren spielen.
- Im Zulassungsverfahren sollten relevante Aspekte des Datenschutzes (z. B. die Rechtsgrundlagen und die Gewährleistung der Betroffenenrechte) und der Informationssicherheit geprüft werden. Die DSK empfiehlt, die Festlegung des Zulassungsverfahrens mit ihr abzustimmen, um die technisch-organisatorischen Maßnahmen und die datenschutzrechtlichen Prinzipien – wie Verschlüsselung, Pseudonymisierung, Erforderlichkeitsgrundsatz, Anonymisierung, Nutzung synthetischer Daten – bei der Datenerhebung, bei der Verarbeitung innerhalb des Registers und bei der Bereitstellung der Daten durch das Register zu gewährleisten. Zugleich sollte für die Zulassung ein Verfahren vorgesehen werden, mit dem die Einhaltung der Qualitätsstandards sowie die

Angemessenheit des Schutzniveaus in regelmäßigen Abständen wiederholt geprüft und nachgewiesen wird.

- Im Zulassungsverfahren sollten auch das Verfahren, das Schutz- und Vertrauensniveau der Schnittstellen und die Voraussetzungen geprüft werden, mit denen ein Register Daten an Dritte bereitstellt oder übermittelt. Nutzungsanträge und -bewilligungen sollten aus Transparenzgründen vom Register und von der für den Nutzungsantrag zuständigen Stelle veröffentlicht werden.
- Zur Verminderung von Risiken und zur datenschutzkonformen Auswertung von Daten sollte in der gesetzlichen Regelung die Nutzung geeigneter technischer und organisatorischer Methoden einschließlich der dezentralen Speicherung und Verarbeitung gefordert werden.
- Es wird empfohlen, gesetzlich festzulegen, welche datenschutzrechtliche Rolle den beteiligten Stellen für welche Verarbeitungsvorgänge zukommt, d.h. ob eine eigene oder gemeinsame Verantwortlichkeit oder eine Auftragsverarbeitung vorliegt.
- Der datenschutzrechtliche Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b DSGVO steht der Verknüpfung von Datensätzen grundsätzlich entgegen. Sofern für Zwecke der wissenschaftlichen Forschung Datensätze verknüpft werden sollen, bedarf es im Hinblick auf das Grundrecht auf Datenschutz einer besonderen Rechtfertigung, die sich in der Regel aus einem öffentlichen Interesse und einem gesellschaftlichen Nutzen ergeben soll. Wegen der sich aus einer Verknüpfung ergebenden Risiken sollte sie nur anlassbezogen und temporär zulässig sein.
- Bei der Verwendung einheitlicher Identifikatoren sollten bereichsspezifische Kennzeichen eingesetzt werden. Im Bereich der Datenverarbeitung durch medizinische Register wäre ein spezifisches datenschutzfreundliches Identifikationssystem für den Gesundheitsbereich denkbar: So könnten beispielsweise aus einer bereits vorhandenen Krankenversicherungsnummer nicht rückrechenbare, bereichsspezifische Pseudonyme für die Register jeweils gesondert durch geschützte Verfahren gebildet und gespeichert werden, die sich nur über eine zentrale Vertrauensstelle zuordnen ließen. Soweit die Zentralstelle für medizinische Register auch datenschutzrechtliche Aspekte prüft, sollte das Verhältnis zu den Datenschutzaufsichtsbehörden unter Beachtung der Vorgaben der DSGVO gesetzlich geklärt werden.