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 Register[2] ein nahezu vollständiger Überblick[3] 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 Krankenversichertennummer 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.