REFERENTENENTWURF FÜR EINE 1. VERORDNUNG ZUR NÄHEREN REGELUNG VON VERFAHREN NACH DEM GESETZ ZUR VERBESSERTEN NUTZUNG VON GESUNDHEITSDATEN

Stellungnahme

28. November 2024

BvD e.V.

DATENSCHUTZ GESTALTEN

Gender-Hinweis:
Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen weiblich, divers und männlich (w/d/m) in diesem Text verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

BvD e.V.
DATENSCHUTZ GESTALTEN

IMPRESSUM

Herausgeber
Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.
Budapester Straße 31
10787 Berlin

T 030 . 26 36 77 60
F 030 . 26 36 77 63

bvd-gs@bvdnet.de
www.bvdnet.de

SEHR GEEHRTE DAMEN UND HERREN,

für die Möglichkeit zur Stellungnahme zum o. g. Referentenentwurf bedanken wir uns.
Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. ist die Berufsorganisation der Datenschutzbeauftragten. Die satzungsgemäße Aufgabe des BvD ist, die Interessen der betrieblichen und behördlichen Datenschutzbeauftragten im Sinne einer dem Stand der Technik angemessenen Realisierung von Datenschutz und Datensicherheit zu fördern. Die rund 2.000 Mitglieder des BvD betreuen als betriebliche und behördliche Datenschutzbeauftragte mehrere zehntausend Unternehmen, Behörden und Institutionen und sind die direkten Ansprechpartner für datenschutzrechtliche Belange bei den Unternehmen bzw. Organisationen.

Ohne Forschung gibt es keinen Fortschritt, daher begrüßen wir die Absicht, den Forschungsstandort Deutschland zu stärken ausdrücklich. Das Recht auf Datenschutz wie auch das Recht auf Forschung sind zwei Grundrechte, auch in der Charta der Grundrechte der Europäischen Union. Art. 7 („Achtung des Privat- und Familienlebens"), Art. 8 der Charta („Schutz personenbezogener Daten") und Art. 13 („Freiheit der Kunst und der Wissenschaft") sind als Grundrechte verankert. Die Grundrechte kommen im Kontext des vorliegenden Verordnungsentwurfes zur Anwendung, es besteht also eine Grundrechtskonkurrenz.

Dabei ist zu beachten, dass das dem Verordnungsentwurf zugrundeliegende Gesetz zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz, GDNG) viele unterschiedliche Ziele verfolgt, die keine Grundrechte darstellen und eine Einschränkung eines Grundrechts in diesen Fällen nur aus überwiegenden Gründen des allgemeinen Interesses unter Einhaltung entsprechend hoher Anforderungen möglich ist. Der vorliegende Referentenentwurf soll diesen Anforderungen durch Vorgaben zu den zu treffenden technischen und organisatorischen Maßnahmen im Hinblick auf den durch Art. 8 der Charta der Grundrechte der Europäischen Union geforderten Schutz personenbezogener Daten Rechnung tragen.

Auch ohne Bezug auf das Grundrecht „Datenschutz" ist es wichtig, dass das Vertrauen der Bürger durch entsprechende Maßnahmen gewonnen wird. Gerade in der medizinischen Forschung zeigte sich in der Vergangenheit immer wieder: Patienten geben ihre allerpersönlichsten Geheimnisse, die Ärzte so dringend zur erfolgreichen Behandlung benötigen, nur preis, wenn sie einen Missbrauch ausschließen können. Diese Patientengeheimnisse, die das GDNG und der darauf aufbauende Verordnungsentwurf zu nahezu beliebigen anderen Zwecken nahezu allen an diesen Daten interessierten Parteien zur Verfügung stellt, bedürfen daher entsprechender Rahmenbedingungen zum Schutz vor Missbrauch. Andernfalls wird in absehbarer Zukunft das Vertrauen der Bürgerinnen und Bürger verloren gehen, was sowohl für die Versorgung der Patientinnen und Patienten, letztlich aber auch für den Forschungsstandort Deutschland eine Katastrophe wäre.

ALLGEMEIN

Das GDNG dient entsprechend § 1 Abs. 1 GDNG der Regelung der Nutzung von Gesundheitsdaten sowohl zu gemeinwohlorientierten Forschungszwecken als auch zur datenbasierten Weiterentwicklung des Gesundheitswesens als lernendes System. Ziele des Gesetzes sind

- die Gewährleistung einer sicheren, besseren und qualitätsgesicherten Gesundheitsversorgung und Pflege (§ 1 Abs. 1 GDNG),
- die Förderung von Forschung und Innovation (§ 1 Abs. 1 GDNG),
- weitere im Gemeinwohl liegenden Zwecke (§ 1 Abs. 2), die seitens des Gesetzgebers nicht genauer definiert wurden.

Entsprechend der Rechtsprechung des EuGH ist der Schutzbedarf von personenbezogenen Daten u. a. abhängig von der Sensibilität der Daten wie auch von der Informiertheit der betroffenen Person: je weniger die betroffene Person ersehen kann, zu welchen Zwecken Daten verarbeitet werden, desto höher müssen die vorgesehenen/geplanten und natürlich auch umgesetzten technischen und organisatorischen Maßnahmen zur Gewährleistung des angemessenen Schutzes der personenbezogenen Daten sein.

Die vom GDNG andressierten Gesundheitsdaten gehören zu den in Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) genannten Datenkategorien und unterliegen dem höchstmöglichen Schutzbedarf. „Weitere im Gemeinwohl liegenden Zwecke" stellt einen so unkonkreten Verwendungszweck dar, dass auch hier ein – ohne, dass man die anderen verfolgten Ziele weiter untersuchen müsste – im Angesicht der Sensibilität der adressierten Gesundheitsdaten höchstmöglicher Schutzbedarf resultiert, sodass statt „Stand der Technik" vielleicht sogar „Stand der Wissenschaft und Technik"[1] zu fordern ist.

Entsprechend hohe Standards sind von den Vorgaben einer „Verordnung zur Umsetzung der Verfahren beim Forschungsdatenzentrum Gesundheit" (Forschungsdatenzentrum Gesundheit Verordnung – FDZGesV), welche das GDNG in Hinblick auf die zu treffenden technischen und organisatorischen Maßnahmen konkretisieren soll, zu fordern.

VORGEGEBENER DATENUMFANG (§ 3)

Kranken- und Pflegekassen müssen entsprechend § 3 des Verordnungsentwurfes u.a.

- das Geburtsjahr,
- das Geschlecht,
- die Postleitzahl des Wohnorts,
- den amtlichen Gemeindeschlüssel des Wohnorts den Vitalstatus,
- das Sterbedatum,
- den Grad der Pflegebedürftigkeit nach § 15 des Elften Buches Sozialgesetzbuch, einschließlich Beginn- und Enddatum,
- die Betriebsnummer der Krankenkasse der versicherten Person,
- Versichertenstatus,
- Betriebsstättennummer der behandelnden Einrichtung,
- lebenslange Arzt- oder Zahnarztnummer,
- Diagnosen,
- Art der Behandlung,
- Angaben zur Arbeitsunfähigkeit,
- Pharmazentralnummer des abgegebenen Arzneimittels einschließlich der vereinbarten Sonderkennzeichen,
- Verordnungsdatum,
- Institutionskennzeichen der abgebenden Apotheke und
- Aufnahme- und den Entlassungstag mit Aufnahme- und Entlassungsgrund bei stationärer Versorgung

mitteilen. In Summe führt die Verordnung 104 Merkmale über Versicherte und deren Behandler auf, welche Kranken- und Pflegekassen weiterleiten müssen.

Bei einem so konkreten und umfangreichen Satz von auch administrativen Daten reicht ein denkbar geringes Zusatzwissen aus, um einen Datensatz wieder einem konkreten Versicherten/Patienten zuzuordnen. Liegen einer Pharmafirma oder einer Forschungseinrichtung personenbezogenen Informationen aus anderer Quelle vor, ist eine Zusammenführung aufgrund der Konkretheit der Daten nahezu immer möglich und dann wird – selbst, wenn dies eigentlich nicht beabsichtigt wird – durch die Zusammenführung eine Re-Identifikation durchgeführt werden.

[1] Im Sinne des Urteils des Bundesverfassungsgerichts vom 8. August 1978 (Az. 2 BvL 8/77)

Es wird dringend zu einer Überprüfung geraten, ob wirklich alle genannten Merkmale zur Erreichung der vom GDNG adressierten Ziele erforderlich sind.

Beispielsweise werden nur Daten der gesetzlich versicherten Bürger Deutschlands von der Verordnung erfasst. Sind all die Daten zur Krankenkasse zur Erreichung der vorgesehenen Ziele hier wirklich erforderlich? Die Fachrichtung der Versorgungseinrichtung kann sicherlich von Interesse sein, aber muss die Einrichtung selbst eindeutig identifizierbar sein? Usw.

PSEUDONYMISIERUNG DURCH DEN GKV-SPITZENVERBAND (§ 5)

Gemäß § 5 Abs. 1 Verordnungsentwurf soll der Spitzenverband Bund der Krankenkassen zur Pseudonymisierung der Daten ein Verfahren nach dem Stand der Technik wählen, bei dem

- die den Leistungserbringer identifizierenden Ziffern der Betriebsstättennummer,
- die lebenslange Arztnummer und
- das Institutionskennzeichen

durch jeweils ein jahresübergreifendes Pseudonym ersetzt werden.

Auch wenn die aus den übrigen Ziffern ableitbaren Informationen zu den jeweiligen Leistungserbringern im Datensatz gesondert aufzuführen sind, wird eine Identifizierung aus den anderen Angaben eher regelhaft möglich sein.

Ausdrücklich zu begrüßen ist die Vorgabe in § 5 Abs. 2 Verordnungsentwurf, dass das anzuwendende Verfahren zur Erzeugung und Überführung der Pseudonyme im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erfolgen muss.

Gerade das Bundesamt für Sicherheit in der Informationstechnik verfügt über ausgewiesene Experten im Bereich der Kryptographie, auf deren Fachwissen in Anbetracht der Sensibilität der Daten keineswegs verzichtet werden darf.

Wünschenswert ist, dass das Bundesamt für Sicherheit in der Informationstechnik grundsätzlich bei jeder Auswahl und jedem Einsatz von Pseudonymisierung und kryptographischen Methoden im Kontext dieses Verordnungsentwurfes einbezogen wird und eine Auswahl immer im Einvernehmen mit dem Amt erfolgen muss.

Dies wird leider nicht überall in der Verordnung umgesetzt.

WIDERSPRUCH GEGEN DIE DATENAUSLEITUNG (§ 8)

Entsprechend § 8 Abs. 1 Verordnungsentwurf können Versicherte ihren Widerspruch gegenüber der Ombudsstelle nach § 342a SGB V oder über die Benutzeroberfläche eines geeigneten Endgeräts erklären.

Laut dem statistischen Bundesamt waren im Jahr 2023 rund 15 % der 65- bis 74-jährigen Personen, die im Kontext der Gesundheitsversorgung aufgrund der Häufigkeit der Erkrankungen von besonderem Interesse sind, in Deutschland sogenannte „Offliner", d.h. diese Personen nutzten noch nie das Internet.[2] 15 % dieser Personen verfügen zudem über kein entsprechendes Endgerät, mit dem ein Widerspruch eingelegt werden kann. Hier sollten Kranken- und Pflegeversicherungen angewiesen werden, dass die jeweilige Ombudsstelle nach § 342a SGB V für diese Versicherten leicht erreichbar sein muss und die Versicherten über die Möglichkeit zur Erteilung des Widerspruchs bei der Ombudsstelle zu informieren sind.

§ 8 Abs. 3 Verordnungsentwurf regelt nicht, wie mit bereits im Zeitraum zwischen Anlegen der Daten in der ePa und dem Eingang des Widerspruchs pseudonymisiert weitergegeben Daten umgegangen wird. Aufgrund der Pseudonymisierung können die Daten einem Versicherten aufgrund des Pseudonyms zugeordnet werden. Diese Daten müssen gelöscht werden. Eine Möglichkeit der Löschung könnte darin bestehen, dass die Pseudonyme gelöscht werden, sodass zumindest eine direkte Zuordnung der Daten zum Versicherten nicht mehr möglich ist. Aufgrund des Umfangs der Daten wird aber weiterhin eine Re-Identifizierung des Versicherten mit nur geringem Zusatzwissen möglich sein, sodass eine entsprechende Gefährdung für Versicherte nicht ausgeschlossen werden kann. Im Falle eines Widerspruchs besteht dieses Risiko gegen den ausdrücklichen Willen des Patienten aufgrund der Opt-Out-Regelung des deutschen Gesetzgebers, was aus Sicht der Rechtsprechung des EuGH in Bezug auf die aus der Charta der Grundrechte der Europäischen Union resultierenden Rahmenbedingungen nur schwer vertretbar sein dürfte.

Entsprechend § 8 Abs. 5 werden Informationen über Art und Umfang eines eingelegten Widerspruchs im Datencockpit (§ 13 Abs. 1 Verordnungsentwurf) protokolliert. Unklar ist, wie Versicherte ohne Endgerät die entsprechenden Informationen erhalten. Hier ist zu fordern, dass Versicherte ohne Endgerät von ihrer Kranken- bzw. Pflegekasse in Schriftform informiert werden.

INFORMATIONSPFLICHTEN UND DATENCOCKPIT (§ 13)

Informationen werden nur Versicherten bereitgestellt, die über ein Endgerät verfügen. Jedoch ist es allein schon aus dem in Art. 12 DS-GVO verankerten Transparenzgrundsatz zwingend erforderlich, dass alle Versicherte gleichermaßen informiert werden. In § 13 Verordnungsentwurf müssen Mechanismen hinterlegt werden, wie Versicherte ohne Endgerät entsprechend informiert werden.

Weiterhin fehlen alle Informationen, welche Datenempfänger Daten erhalten haben. Gerade in Anbetracht

- des durch den großen Umfang der Daten bestehenden Re-Identifizierungsrisikos,
- der aus Sicht eines Versicherten unüberschaubaren Zahl der Antragsberechtigten (kommerzielle und öffentliche Forschungseinrichtungen, Einrichtungen des Gesundheitsversorgung, Pharmaindustrie, IT-Industrie, Krankenkassen, Ministerien)
- und der unbegrenzten Zwecke, zu denen die Gesundheitsdaten der Versicherten genutzt werden dürfen wie beispielsweise die Entwicklung und Testung von Arzneimitteln oder Medizinprodukten wie auch dem Training von künstlicher Intelligenz,

ist eine entsprechende Information aus Sicht des europäischen Rechts unverzichtbar.

2] Statistisches Bundesamt: Zahl der Woche - Gut 5 % der Bevölkerung im Alter von 16 bis 74 Jahren in Deutschland sind offline. Online, verfügbar unter https://www.destatis.de/DE/Presse/Pressemitteilungen/Zahl-der-Woche/2024/PD24_15_p002.html

ZUSAMMENSETZUNG DER AG PSEUDONYMISIERUNG (§ 14)

In § 14 Abs. 2 Verordnungsentwurf wird die Zusammensetzung der AG Pseudonymisierung festgelegt. Dabei sind keine Vertreter mit ausgewiesener Kenntnis von Verfahren zur Pseudonymisierung oder zur Nutzung kryptographischer Methoden berücksichtigt worden. Es ist daher fraglich, woher die AG Pseudonymisierung das erforderliche Fachwissen bekommen soll, um ihre Aufgaben zu erledigen.

Die in § 14 Abs. 3 Verordnungsentwurf enthaltene Möglichkeit, zu einzelnen Fragen externe Beratung einzuholen, reicht sicherlich nicht aus. Um zu wissen, wo das eigene Wissen endet, braucht man zunächst entsprechende Fachexpertise innerhalb der AG Pseudonymisierung.

Es wird daher dazu geraten, dass entsprechend qualifizierte Vertreter des Bundesamtes für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit als ständige Mitglieder der AG Pseudonymisierung in § 14 Abs. 2 Verordnungsentwurf ergänzt werden, um einen Mindeststand von Fachkompetenz in der Gruppe zu gewährleisten.

AUFGABEN DER AG PSEUDONYMISIERUNG (§ 15)

Gemäß den Vorgaben in § 20 Verordnungsentwurf dürfen „standardisierte Datensätze in anonymisierter Form“ zur Verfügung gestellt werden. Unklar ist, wie medizinische Daten in einem so großen Umfang, wie es § 3 Verordnungsentwurf vorgibt, anonymisiert werden können.

Es wäre aus unserer Sicht zu begrüßen, wenn in § 15 Abs. 1 des Verordnungsentwurfs als Aufgabe der AG Pseudonymisierung neben der Erarbeitung von zuverlässigen Pseudonymisierungsverfahren auch die Erarbeitung von zuverlässigen Anonymisierungsverfahren aufgenommen wird.

Weiterhin sollten die Ergebnisse der AG Pseudonymisierung öffentlich verfügbar sein, damit die von der AG Pseudonymisierung erarbeiteten zuverlässigen Pseudonymisierungs- und Anonymisierungsver-fahren auch in anderen Bereichen angewendet werden können. Entsprechende Verfahren können analog sogar außerhalb der Gesundheitsversorgung einen wesentlichen Beitrag zur Verbesserung der aktuellen Situation und zur Verringerung von Rechtsunsicherheiten aller Wirtschaftsakteure leisten.

Wir empfehlen daher, § 15 Abs. 1 Verordnungsentwurf um einen Satz 4 zu ergänzen, in welchem festgelegt wird, dass alle Arbeitsergebnisse der AG Pseudonymisierung der Allgemeinheit kostenfrei zum Download zur Verfügung gestellt werden.

> (1) Die AG Pseudonymisierung legt zuverlässige Anonymisierungs- und Pseudonymisierungs-verfahren für Dokumente oder Datensätze in den elektronischen Patientenakten verbindlich fest. […] Die erarbeiteten zuverlässigen Anonymisierungs- und Pseudonymisierungsverfahren werden kostenlos auf der Homepage der AG Pseudonymisierung, welche von der Gesellschaft für Telematik eingerichtet wird, der Allgemeinheit zur beliebigen Verwendung Verfügung gestellt.

Entsprechend § 15 Abs. 2 Verordnungsentwurf dürfen einzelne Datenfelder nur verändert oder gelöscht werden, „wenn dies zur Entfernung des unmittelbaren Personenbezugs erforderlich ist und andernfalls ein unangemessenes Reidentifikationsrisiko besteht“.

Ein mittelbarer Personenbezug führt ebenso zur Re-Identifikation. Diese Vorgabe verhindert eine wirksame Pseudonymisierung. Kommt es aufgrund dieser Vorgabe und der daraus aus technischer Sicht unwirksamen Re-Identifizierung, stellt sich die Frage nach der Haftung und wer für den resultierenden Schadenersatz gegenüber der versicherten Person verantwortlich ist. Ein Anspruch gegen das Ministerium, welches die Vorgabe erließ, oder auch gegen die Gesellschaft für Telematik, welcher nach § 14 Abs. 4 Verordnungsentwurf die Organisation der AG Pseudonymisierung innewohnt, kann rechtlich nicht vollständig ausgeschlossen werden.

Wir empfehlen aus diesem Grund, in § 15 Abs. 2 das Wort „unmittelbar" zu löschen und den Nebensatz wie folgt zu formulieren:

> „[…] verändert oder gelöscht werden, wenn dies zur Entfernung des Personenbezugs erforderlich ist und […]"

ANTRAG ZUR DATENVERARBEITUNG (§ 17)

§ 17 Abs. 1 Verordnungsentwurf listet auf, was ein Antragsteller bei Antragstellung angeben muss. Hier fehlt insbesondere

- die Art der Verarbeitung, z.B. ob eine Cloud genutzt wird und in diesem Fall die Vorgaben des § 393 SGB V eingehalten werden;
- ein Qualifikationsnachweis des Antragstellers, mit welchem seitens des Antragstellers nachgewiesen wird, dass die fachliche Qualifikation zum Umgang mit und der Auswertung der Daten gegeben ist;
- ein Datenschutzkonzept, mit welchem der Antragsteller nachweist, wie er den Vorgaben der DS-GVO genügt;
- ein IT-Sicherheitskonzept inkl. Berechtigungskonzept, in dem beschrieben ist, wie der Stand der Technik bei der Verarbeitung eingehalten wird;
- ein Protokollierungskonzept, anhand nachvollzogen werden kann, wer wann zu welchen Zwecken die pseudonymen Daten verarbeitete;
- ein Löschkonzept, in welchem beschrieben ist, mit welchen Methoden zu welchem Datum die erhaltenen pseudonymen Daten vom Empfänger gelöscht werden;
- eine Datenschutz-Folgenabschätzung, die aufgrund des Umfangs der besonders sensiblen Daten in der Regel erforderlich sein wird.

Mit den vorliegenden Vorgaben zur Antragstellung kann das Forschungsdatenzentrum nicht überprüfen, ob der Antragsteller die Zusicherungen aus § 17 Abs. 3 Verordnungsentwurf einhält oder nicht. Entsprechend der Vorgaben der DS-GVO muss sich das Forschungsdatenzentrum aber vergewissern; alleiniger Glaube an die Einhaltung getroffener Zusagen reicht nach Rechtsprechung des EuGH nicht aus.

Entsprechend § 303a Abs. 3a Nr. 1 SGB V ist ein Antrag auch abzulehnen, wenn ein unangemessenes Risiko für den Schutz personenbezogener Daten entstehen würde und dieses Risiko nicht durch Auflagen und weitere Maßnahmen ausreichend minimiert werden kann.

§ 18 Abs. 1 Nr. 2 Verordnungsentwurf verlangt auch eine Prüfung dieses Sachverhaltes durch das Forschungsdaten-zentrum, aber die aktuellen Vorgaben bzgl. der Antragstellung erlauben dem Forschungsdatenzentrum mangels Informationen keine Bewertung.

Wir empfehlen daher, die Liste der einzureichenden Informationen bei Antragstellung entsprechend unseres Vorschlags zu ergänzen.

ANTRAGSERFASSUNG- UND PRÜFUNG (§ 18)

§ 18 Abs. 4 Verordnungsentwurf legt den Zeitraum fest, in welchem das Forschungsdatenzentrum über Anträge entscheidet, enthält aber keine Vorgaben zur Priorisierung der Bearbeitung der Anträge.

Es ist nicht unwahrscheinlich, dass das Forschungsdatenzentrum mehr Anträge erhält, als in der in § 18 angesetzten Zeitspanne aufgrund der zur Verfügung stehenden Ressourcen abgearbeitet werden können. In diesen Fällen muss das Forschungsdatenzentrum priorisieren, welche Anträge zuerst und welche später verarbeitet werden.

Durch das GDNG werden hochsensible Daten der deutschen Bürgerinnen und Bürger an beliebige Dritte „verschenkt", entsprechend sollten auch die Dritten, von deren Arbeit die Bürgerinnen und Bürger am ehesten ihrerseits profitieren bzw. die Zwecken des Gemeinwohls dienen, bevorzugt werden.

Wir empfehlen, dass im Verordnungsentwurf eine Priorisierungsvorgabe eingeführt wird, wo

1. gemeinnützige Forschungseinrichtungen, deren Forschungsergebnisse einen nachgewiesenen Nutzen für die Allgemeinheit darstellen können und somit im Allgemeininteresse stehen, an erster Stelle abgearbeitet wird.
2. Nachfolgend sollten die Anträge zu Forschungszwecken von öffentlichen Forschungseinrichtungen, deren Forschungsergebnisse einen nachgewiesenen Nutzen für die Allgemeinheit darstellen können und somit im Allgemeininteresse stehen, bearbeitet werden.
3. Danach alle anderen Forschungsanträge, deren Forschungsergebnisse einen nachgewiesenen Nutzen für die Allgemeinheit darstellen können und somit im Allgemeininteresse stehen.
4. Und erst anschließend sollten alle anderen Anträge abgearbeitet werden.

Es werden hochsensible Daten der Patientinnen und Patienten verarbeitet, daher sollten die Interessen und das Wohlergehen der Patientinnen und Patienten auch an erster Stelle stehen.

DATENBEREITSTELLUNG (§ 20)

§ 20 Abs. 1 S. 2 Nr. 1 Verordnungsentwurf enthält die Regelung, dass Daten in „anonymisierter Form" zur Verfügung gestellt werden dürfen. Vielfach ist nicht bekannt, dass der Begriff „Anonymisierung" europäisch in Art. 2 Ziff. 7 Richtlinie (EU) 2019/1024 geregelt und somit entsprechend der Rechtsprechung des EuGH europaweit einheitlich zu verwenden ist.

Wir empfehlen daher eine Ergänzung zur Klarstellung in § 20 Abs. 1 S. 2 Nr. 1 Verordnungsentwurf:

(1) „Das Forschungsdatenzentrum stellt den Nutzungsberechtigten im Anschluss an die bewilligende Entscheidung nach § 18 Absatz 3 die Daten zur Verfügung. Die Bereitstellung der Daten kann dadurch erfolgen, dass das Forschungsdatenzentrum den Nutzungsberechtigten

1. standardisierte Datensätze in anonymisierter Form zur Verfügung stellt, wobei die Anonymisierung im Sinne von Art. 2 Ziff. 7 der Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors zu verstehen ist, oder
2. […]"

§ 20 Abs. 2 Verordnungsentwurf erlaubt die Bereitstellung nur unter zwei alternativen Bedingungen, wovon die erste Bedingung lautet, dass der Empfänger der Daten unter § 203 StGB fällt. Dies ist faktisch nur der Fall, wenn § 203 Abs. 2 StGB zutrifft. Die Normadressaten von § 203 Abs. 1 StGB werden nur adressiert,

wenn das Geheimnis im Rahmen der Berufsausübung anvertraut wurde. Die pseudonymen Gesundheitsdaten werden aber nicht im Kontext einer medizinischen Betreuung von einer der in § 203 Abs. 1 StGB genannten natürlichen oder juristischen Personen erlangt, sondern außerhalb, sodass § 203 StGB in all diesen Fällen nicht zutreffen wird.

Entsprechend § 20 Abs. 2 S. 2 Nr. 2 Verordnungsentwurf wird das Forschungsdatenzentrum in den meisten Stellen eine Verpflichtung durchführen müssen, wenn pseudonyme Datensätze bereitgestellt werden. Eine Verpflichtung entsprechend dem Gesetz über die förmliche Verpflichtung nichtbeamteter Personen wird nicht möglich sein, daher stellen sich die Fragen,

a) auf welcher Rechtsgrundlage das Forschungsdatenzentrum eine Verpflichtung durchführen soll und
b) welche Konsequenzen ein Verstoß gegen die durch das Forschungsdatenzentrum vorgenommene Verpflichtung hat.

In § 20 Abs. 2 Verordnungsentwurf sollten klare Vorgaben zur Verpflichtung inkl. Rechtsfolgen für den Verpflichteten dargelegt werden.

Entsprechend § 20 Abs. 2 S. 3 Verordnungsentwurf werden pseudonymisierten Daten nur in der Sicheren Verarbeitungsumgebung des Forschungsdatenzentrums bereitgestellt. § 20 Abs. 2 S. 7 ergänzt entsprechend, dass pseudonymisierte Daten an die Nutzungsberechtigten nicht außerhalb der sicheren Verarbeitungsumgebung herausgegeben werden dürfen.

Wir empfehlen eine Ergänzung in § 20 Abs. 1 als neue Nummer 3, dass die sichere Verarbeitungsumgebung technisch eine Ausleitung („Download“) der Daten verhindern muss und ein Abfluss von Daten aus der sicheren Verarbeitungsumgebung als eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DS-GVO anzusehen ist.

(2) „Das Forschungsdatenzentrum stellt den Nutzungsberechtigten im Anschluss an die bewilligende Entscheidung nach § 18 Absatz 3 die Daten zur Verfügung. Die Bereitstellung der Daten kann dadurch erfolgen, dass das Forschungsdatenzentrum den Nutzungsberechtigten

1. standardisierte Datensätze in anonymisierter Form zur Verfügung stellt, wobei die Anonymisierung im Sinne von Art. 2 Ziff. 7 der Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors zu verstehen ist, oder
2. aggregierte Datensätze oder Einzeldatensätze in anonymisierter oder pseudonymisierter Form in einer gesicherten virtuellen Umgebung unter Kontrolle des Forschungsdatenzentrums (sichere Verarbeitungsumgebung) zu Verfügung stellt;
3. die sichere Verarbeitungsumgebung muss einen Abfluss („Download“ der darin befindlichen Gesundheitsdaten technisch verhindern, ein Abfluss von Gesundheitsdaten als eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 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 anzusehen.

EVALUATION UND WEITERENTWICKLUNG (§ 23)

§ 23 Verordnungsentwurf beinhaltet, worüber das Forschungsdatenzentrum dem Bundesministerium für Gesundheit alle drei Jahre berichten soll.

Wir empfehlen, dass auch bzgl. Kenntnis erfolgter Re-Identifizierungen durch Antragsteller/Datenempfänger berichtet wird, sofern bekannt, ergänzt durch Informationen über die Umstände, wie eine Re-Identifikation möglich war.

Aufgrund der Sensibilität und des außergewöhnlich großen Umfangs der Datenmenge – tendenziell sind die Daten aller gesetzlich versicherten Bürger betroffen – sollte ein jährlicher Bericht erfolgen.

Um den Transparenzgedanken gegenüber den deutschen Bürgerinnen und Bürgern zu entsprechen, sollte dieser jährliche Bericht – analog den Tätigkeitsberichten der Datenschutz-Aufsichtsbehörden – frei verfügbar auf einer entsprechenden Webseite des Forschungsdatenzentrums zur Einsichtnahme oder auch zum Download angeboten werden.

FEHLENDE PUNKTE

1) Meldepflichten
In der Verordnung wird nicht beschrieben, wie mit Re-Identifizierungen umgegangen wird. Dies wird regelhaft einen meldepflichtigen Umstand darstellen, sodass das Forschungsdatenzentrum bei Kenntnis die oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit informieren sollte.

Beruht die Re-Identifizierung auf einer technisch unzureichenden Methode der Pseudonymisierung oder Verschlüsselung, so sollte zusätzlich das Bundesamt für Sicherheit in der Informationstechnik informiert werden.

2) Auskunft für Versicherte
Es sollte eine Möglichkeit vorgesehen werden, wo interessierte Bürger nachsehen können, wer ihre pseudonymisierten Daten zu welchen Zwecken verarbeitetet. Aufgrund der vorhandenen Pseudonyme ist dies möglich, aufgrund der Transparenzvorgaben und der hohen Gefährdungslage für Versicherte auch angemessen. Hierzu sollte ein Antrag bei der jeweiligen Kranken- und Pflegekasse möglich sein, welche die Daten einholt und versicherten Personen zur Verfügung stellt. Um den Aufwand so gering wie möglich zu halten, sollte die Möglichkeit zur Antragstellung auf einmal pro Jahr begrenzt werden, außer es liegen außergewöhnliche Umstände wie beispielsweise eine aktuelle Berichterstattung zu Datenlecks vor.

Minimalanforderung in diesem Zusammenhang ist, dass sich betroffene Bürger an die für sie zuständige Datenschutzaufsichtsbehörde wenden können und diese auf Nachfrage verpflichtet wird, in Zusammenarbeit mit Kranken-, Pflegekasse, GKV-Spitzenverband und Forschungsdatenzentrum die gewünschten Informationen zu ermitteln und dem anfragenden Bürger zur Verfügung zu stellen.

Sehr geehrte Damen und Herren,

wir hoffen, wir konnten Ihnen mit unseren Hinweisen behilflich sein, eine Rechtslage zu schaffen, welche den Interessen aller Beteiligten an einer vertrauensvollen Umsetzung der vom Referentenentwurf adressierten Ziele genügt. Gerne stehen wir auch bei Fragen zur Verfügung.

Über den Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.

Mit über 30 Jahren Erfahrung ist der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. die älteste Interessenvertretung für betriebliche und behördliche Datenschutzbeauftragte und -berater. BvD-Mitglieder sind in allen Branchen vertreten, insbesondere IT und IKT, Industrie/Produktion, Handel/Vertrieb, Beratung sowie Gesundheits- und Sozialwesen. Als erster Ansprechpartner der Betroffenen sind die BvD-Mitglieder Anlaufstelle für etwa fünf Millionen Arbeitnehmer sowie einen Großteil der Bürger und Konsumenten. Zudem sind sie als konstruktiv lösungsorientierte Datenschutzexperten ein wichtiger Partner für die verantwortliche Unternehmensleitung. Die Verbandsvorstände, alle Leiter von Arbeitskreisen, Ausschüssen und Regionalgruppen des BvD bringen ihre praktische Erfahrung unentgeltlich in die Verbandsarbeit ein. Mit der Gründung des Europäischen Dachverbandes EFDPO (www.efdpo.eu) hat der BvD die Weichen für die verstärkte Vernetzung und Kommunikation auf EU-Ebene gestellt.

www.bvdnet.de