Ausarbeitung

Digitales-Versorgungs-Gesetz – Datentransparenz (§§ 303a ff. SGB V)

Recht auf informationelle Selbstbestimmung und Datenschutz

Digitales-Versorgungs-Gesetz – Datentransparenz (§§ 303a ff. SGB V)
Recht auf informationelle Selbstbestimmung und Datenschutz

Aktenzeichen:	WD 3 - 3000 - 180/20
Abschluss der Arbeit:	17. August 2020
Fachbereich:	WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1.	**Fragestellung**	**4**
2.	**Änderungen an den §§ 303a ff. SGB V durch das DVG**	**4**
3.	**Darstellung der Datentransfers**	**6**
4.	**Datenschutzrecht**	**7**
4.1.	Datenschutz-Grundverordnung	7
4.2.	Bundesdatenschutzgesetz	10
4.3.	Schlussfolgerungen aus dem allgemeinen Datenschutzrecht	11
4.4.	Problemstellung bzgl. einer wirksamen Einwilligung	11
4.5.	Sozialdatenschutz im SGB I und SGB X	12
4.6.	Regelungen der §§ 303a ff. SGB V	13
5.	**Grundrecht auf informationelle Selbstbestimmung**	**14**
5.1.	Schutzbereich und Eingriff	15
5.2.	Verfassungsrechtliche Rechtfertigung	16
5.2.1.	Legitimer Zweck und Geeignetheit	17
5.2.2.	Erforderlichkeit	17
5.2.3.	Angemessenheit	18
6.	**Ergebnis**	**19**

1. Fragestellung

Diese Ausarbeitung befasst sich mit der Weitergabe von Gesundheitsdaten an eine **Datensammelstelle** und eine **Forschungsdatenbank** nach dem **Digitalen-Versorgung-Gesetz (DVG)**[1]. Durch das Gesetz wurden Änderungen am Sozialgesetzbuch Fünftes Buch (SGB V) vorgenommen, nach denen die gesetzlichen Krankenversicherungen Daten ihrer Versicherten an eine Datensammelstelle weitergeben müssen. Untersucht wird, ob die zentrale Datensammlung und Weitergabe mit dem **Recht auf informationelle Selbstbestimmung** (Art. 2 Abs. 1 GG iVm Art. 1 Abs. 1 GG) und dem **Datenschutzrecht** vereinbar ist.

2. Änderungen an den §§ 303a ff. SGB V durch das DVG

Zunächst werden die Änderungen an den Regelungen zur Datentransparenz in den **§§ 303a ff. SGB V**[2] durch das Digitale-Versorgung-Gesetz dargestellt. Diese wurden am 7.11.2019 durch den Bundestag beschlossen. **Zweck** der Neuregelung ist es, den Zugang zu den Sozialdaten der Krankenkassen zu verbessern, um durch eine Analyse zur Verbesserung der Versorgung beizutragen und um eine breite wissenschaftliche Nutzung unter Wahrung des Sozialdatenschutzes zu ermöglichen. Hierfür soll die bisherige Datenaufbereitungsstelle zu einem Forschungsdatenzentrum **(FDZ)** mit einem deutlich erweiterten und aktuelleren Datenangebot weiterentwickelt werden.[3]

Die erste Änderung ist somit die Umbenennung der **„Datenaufbereitungsstelle“** in ein **„Forschungsdatenzentrum“** nach §§ 303a, 303d SGB V. Die Umbenennung begleiten sachliche Änderungen. So werden die **Aufgaben** des FDZ in § 303d Abs. 3 SGB V konkretisiert. Es soll die wissenschaftliche Erschließung der Daten fördern (§ 303d Abs. 3 Nr. 10 SGB V), jedoch auch das spezifische Reidentifikationsrisiko bewerten und unter größtmöglicher Wahrung des angestrebten wissenschaftlichen Nutzens durch geeignete Maßnahmen reduzieren (§ 303d Abs. 3 Nr. 5 SGB V). Darüber hinaus soll das FDZ anonymisierte Datensätze (sog. Public Use Files) erstellen und diese öffentlich verfügbar machen, insbesondere zu Schulungs-, Entwicklungs- und Testzwecken.[4]

Die wohl wesentlichste Änderung betrifft Herkunft und Umfang der Daten.[5] Nach § 303b SGB V a.F. stammten diese Daten vom Bundesversicherungsamt. Nun regelt § 303b Abs. 1 SGB V, dass

---

1 Gesetz für eine Verbesserung durch Digitalisierung und Innovation vom 9.12.2019 (BGBl. I S. 2562).

2 Alle Zitate der §§ 303a ff. SGB V ohne weitere Kennzeichnung beziehen sich auf den aktuellen Gesetzesstand, also nach der Änderung durch das DVG.

3 Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz - DVG), 9.8.2019, BR-Drs. 360/19, S. 34.

4 Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz - DVG), 9.8.2019, BR-Drs. 360/19, S. 79.

5 Kühling/Sackmann/Schildbach, Rechtsgutachten über den sozialdatenschutzrechtlichen Weiterentwicklungsbedarf im SGB V und SGB X im Hinblick auf Big-Data-Anwendungen, erstellt im Auftrag des Bundesministeriums für Gesundheit, 4.9.2019, S. 86, 89.

der **Spitzenverband Bund der Gesetzlichen Krankenversicherungen** (GKV-Spitzenverband) als **Datensammelstelle** fungieren soll.[6] Der **Umfang** der zu sammelnden Daten wird durch § 303b Abs. 1 SGB V explizit gesetzlich festgelegt, der tatsächlich zu übermittelnde Datenumfang in § 3 Abs. 1 Datentransparenzverordnung **(DaTraV)** abschließend bestimmt. Der Datenumfang wird im Vergleich zur früheren Rechtslage ausgeweitet.[7] Es sollen neben Leistungs- und Abrechnungsdaten unter anderem die Daten des Risikostrukturausgleichs im Sinne von § 267 SGB V gesammelt werden. Dabei handelt es sich vor allem um Daten wie Stammdaten und Informationen über ambulante und stationäre Behandlungen gesetzlich Versicherter sowie um Angaben zu den verschriebenen Arzneimitteln, § 7 Abs. 1 Risikostruktur-Ausgleichsverordnung (RSAV).[8] Durch die direkte Übermittlung der Daten vom GKV-Spitzenverband statt wie früher vermittelt durch das Bundesversicherungsamt stehen wesentlich **aktuellere Daten** zur Verfügung.[9] Erstmals werden auch Angaben zu den Leistungserbringern gesammelt.

Die Datensätze werden gemäß § 303b Abs. 1, 3 Nr. 1 SGB V **mit Lieferpseudonym** an den GKV-Spitzenverband und anschließend pseudonymisiert – ohne Lieferpseudonym – an das Forschungsdatenzentrum übermittelt. Das Pseudonymisierungsverfahren soll dem Stand der Technik entsprechen, § 5 Abs. 1 DaTraV. Die zum Lieferpseudonym gehörige Arbeitsnummer, welche das Versicherungskennzeichen vertritt, wird nach § 303b Abs. 3 Nr. 2 SGB V der Vertrauensstelle übermittelt. Zudem müssen die Daten gemäß § 303d Abs. 3 SGB V spätestens nach 30 Jahren gelöscht werden. Spezifiziert wurde auch die **Art der Datenbereitstellung** an die nutzungsberechtigten Stellen: entweder als „anonymisiert und aggregiert“ nach § 303e Abs. 3 SGB V oder als pseudonymisierte Einzeldatensätze nach § 303e Abs. 4 SGB V.

Die nutzungsberechtigten Stellen nach § 303e Abs. 1 SGB V bleiben der Sache nach unverändert.[10] Hinsichtlich der Zweckbindung wird klargestellt, dass die Aufzählung in § 303e Abs. 2 SGB V abschließend zu verstehen ist.[11] Eine erhebliche Konkretisierung wird hinsichtlich des

---

6 Kühling/Sackmann/Schildbach (Fn. 4), S. 86, 89; Platzer, NZS 2020, 289, 290.

7 Kühling/Sackmann/Schildbach, (Fn. 4), S. 86.

8 Verordnung über das Verfahren zum Risikostrukturausgleich in der gesetzlichen Krankenversicherung vom 3.1.1994 BGBl. I S. 55; zuletzt geändert durch Artikel 1 V. v. 8.6.2020 BGBl. I S. 1233; siehe auch Kühling/Schildbach, NZS 2020, 41, 42.

9 Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz - DVG), 9.8.2019, BR-Drs. 360/19, S. 78.

10 Kühling/Sackmann/Schildbach (Fn. 4), S. 87, 89; Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz - DVG), 9.8.2019, BR-Drs. 360/19, S. 80.

11 Kühling/Sackmann/Schildbach (Fn. 4), S. 89.

Antragsverfahrens einer nutzungsberechtigten Stelle vorgenommen.[12] Neu ist die Prüfung der **Erforderlichkeit der Datenverarbeitung für die Aufgabenerfüllung** der nutzungsberechtigten Stelle nach § 303e Abs. 3 S. 1 SGB V. Dabei ist das FDZ nach § 303e Abs. 3 S. 2 SGB V bei der Prüfung des Antrags hinsichtlich der Erforderlichkeit des Datenumfangs auf eine **Plausibilitätsprüfung** beschränkt.[13] Die Daten empfangende Stelle muss einer Geheimhaltungspflicht unterliegen, § 303e Abs. 4 SGB V.

Schließlich folgt erstmals auch auf Gesetzesebene ein ausdrückliches **Verbot der Zweckentfremdung, der Datenweitergabe und der Reidentifikation** durch Nutzungsberechtigte (§ 303e Abs. 5 SGB V). Die vorsätzliche Reidentifikation von Versicherten wird unter **Strafe** gestellt (§ 307b Abs. 1 Nr. 3 SGB V).

3. Darstellung der Datentransfers

Nach den §§ 303a ff. SGB V ergibt sich vereinfacht folgender Ablauf von Datenverarbeitungen und -weitergaben:

(1) Die **gesetzlichen Krankenversicherungen** liefern die Daten mit einem Lieferpseudonym der Versicherten an den **GKV-Spitzenband** als **Datensammelstelle**.
(2) Die **Datensammelstelle** liefert an zwei Stellen:
   (a) Die Daten und eine individuelle Arbeitsnummer werden an das **Forschungsdatenzentrum** überliefert.
   (b) Das Lieferpseudonym und die Arbeitsnummer werden an die **Vertrauensstelle** (§ 303c SGB V) übermittelt.
(3) Die **Vertrauensstelle** erstellt ein neues Pseudonym und liefert dieses zusammen mit der Arbeitsnummer an das **Forschungsdatenzentrum**.
(4) Das **Forschungsdatenzentrum** stellt die Daten auf verschiedene Weise den **Nutzungsberechtigten** nach ihrem jeweiligen Antrag und der Prüfung der Erforderlichkeit des Datenumfangs zur Verfügung.

Aus dieser Darstellung wird deutlich, dass bei der Datensammelstelle alle Daten der Betroffenen in einer nur pseudonymisierten Art gesammelt und verarbeitet werden. Erst auf den weiteren Ebenen der Vertrauensstelle und des Forschungsdatenzentrums erfolgen weitere Pseudonymisierungs- bzw. Anonymisierungsschritte.

---

12 Vgl. von Dewitz, in: Rolfs/Giesen/Kreikebohm/Udsching (Hrsg.), Beck'scher Online Kommentar Sozialrecht, 57. Ed. 1.6.2020, SGB V, § 303e, Rn. 5-8; Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz - DVG), 9.8.2019, BR-Drs. 360/19, S. 81.

13 Kühling/Sackmann/Schildbach (Fn. 4), S. 87.

4. Datenschutzrecht

4.1. Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (DSGVO)[14] führt seit dem Frühjahr 2018 zu einer weitgehenden Vollharmonisierung des Datenschutzrechts auf europäischer Ebene. Die Verordnung stellt aufgrund ihrer unmittelbaren Wirkung nach Art. 288 Abs. 2 Vertrag über die Arbeitsweise der Europäischen Union (AEUV) den normativen Ausgangspunkt der Betrachtungen dar.[15] Nach Art. 9 DSGVO genießen **Gesundheitsdaten** einen Schutz, der über den allgemeinen Schutz der personenbezogenen Daten hinausgeht.[16] **Art. 9 Abs. 1 DSGVO verbietet** die **Verarbeitung** personenbezogener Daten, die Gesundheitsdaten darstellen.

„Gesundheitsdaten“ sind nach Art. 4 Nr. 15 DSGVO personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Der Begriff der Gesundheitsdaten wird dabei weit ausgelegt, wie sich aus dem Erwägungsgrund 35 zur DSGVO ergibt:

> „Zu den personenbezogenen Gesundheitsdaten sollten alle Daten zählen, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen. Dazu gehören auch Informationen über die natürliche Person, die im Zuge der Anmeldung für sowie der Erbringung von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates für die natürliche Person erhoben werden, Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben, abgeleitet wurden, und Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten (…).“

„Personenbezogene Daten“ meint alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die

---

14 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

15 Kühling, MedR 2019, 611, 618.

16 Kühling, MedR 2019, 611, 612.

Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (Art. 4 Nr. 1 DSGVO).

Der Begriff der **Verarbeitung** von Daten ist weit gefasst und in Art. 4 Nr. 2 DSGVO näher definiert. „Verarbeitung" bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Das Verbot der Verarbeitung von Gesundheitsdaten gilt jedoch nicht, sofern eine Ausnahme nach Art. 9 Abs. 2 DSGVO vorliegt. In den dort normierten **Ausnahmen** sind auch Abweichungsmöglichkeiten durch die nationalen Gesetzgeber normiert. Die Vollharmonisierung besteht mithin in diesem Bereich des Datenschutzrechts nicht.[17] Eine wesentliche Ausnahme vom strengen Schutz der Gesundheitsdaten bietet die Möglichkeit der **Einwilligung** in die Verarbeitung für einen oder mehrere festgelegte Zwecke durch die betroffene Person (Art. 9 Abs. 2 lit. a DSGVO). Unter anderem zum Zwecke der **Gesundheitsversorgung** (Art. 9 Abs. 2 lit. h iVm Abs. 3 DSGVO) kann eine entsprechende Datenverarbeitung erlaubt sein. Dies steht jedoch unter der Einschränkung, dass es sich bei den Verarbeitern um **Berufsgeheimnisträger** handelt,[18] also insbesondere Ärzte. Auch die Beschäftigten von Krankenkassen und Kassenärztlichen Vereinigungen sind der Geheimhaltungspflicht – gleich einem Berufsgeheimnisträger – unterworfen.[19]

Zudem eröffnet Art. 9 Abs. 2 lit. g DSGVO allgemein die Möglichkeit der Verarbeitung der besonders geschützten Daten, wenn diese

> „auf der Grundlage des **Unionsrechts** oder des **Rechts eines Mitgliedstaats**, das in **angemessenem Verhältnis** zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und **spezifische Maßnahmen** zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen **öffentlichen Interesses erforderlich** [ist]".[20]

Insofern ist eine Abweichungsmöglichkeit von dem strengen Schutz der Gesundheitsdaten nach Art. 9 Abs. 1 DSGVO unter den spezifischen Bedingungen auch durch **nationales Recht** möglich. Diese wird durch Art. 9 Abs. 2 lit. i DSGVO noch ergänzt für Fälle, in denen

> „die Verarbeitung […] aus Gründen des **öffentlichen Interesses** im Bereich der **öffentlichen Gesundheit**, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur **Gewährleistung** hoher Qualitäts- und Sicherheitsstandards bei der

17 Kühling, MedR 2019, 611, 612.

18 Vgl. Schröder, MedR 2019, 631; Kühling, MedR 2019, 611, 612.

19 Schröder, MedR 2019, 631.

20 Hervorhebung nur hier.

> **Gesundheitsversorgung** und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des **Unionsrechts** oder des **Rechts eines Mitgliedstaats**, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich [ist]".

Insofern liegen für Gesundheitsdaten zwei Öffnungsklauseln vor, die eine nationale Regelung der Verarbeitung aus Gründen des **öffentlichen Interesses** ermöglichen oder modifizieren.[21]

Erwägungsgrund 53 S. 1 zur DSGVO führt dazu noch etwas konkreter aus:

> „Besondere Kategorien personenbezogener Daten, die eines höheren Schutzes verdienen, sollten nur dann für gesundheitsbezogene Zwecke verarbeitet werden, wenn dies für das Erreichen dieser Zwecke im Interesse einzelner natürlicher Personen und der Gesellschaft insgesamt erforderlich ist, insbesondere im Zusammenhang mit der Verwaltung der Dienste und Systeme des Gesundheits- oder Sozialbereichs, einschließlich der Verarbeitung dieser Daten durch die Verwaltung und die zentralen nationalen Gesundheitsbehörden zwecks Qualitätskontrolle, Verwaltungsinformationen und der allgemeinen nationalen und lokalen Überwachung des Gesundheitssystems oder des Sozialsystems und zwecks Gewährleistung der Kontinuität der Gesundheits- und Sozialfürsorge und der grenzüberschreitenden Gesundheitsversorgung oder Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen oder für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken, die auf Rechtsvorschriften der Union oder der Mitgliedstaaten beruhen, die einem im öffentlichen Interesse liegenden Ziel dienen müssen, sowie für Studien, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden."

Erwägungsgrund 54 S. 3 zur DSGVO ergänzt bezüglich einer weiten Auslegung des Begriffs der **öffentlichen Gesundheit**.

> „In diesem Zusammenhang sollte der Begriff ‚öffentliche Gesundheit' im Sinne der Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates ausgelegt werden und alle Elemente im Zusammenhang mit der Gesundheit wie den Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den **Bedarf an Gesundheitsversorgung**, die der Gesundheitsversorgung zugewiesenen **Mittel**, die **Bereitstellung** von Gesundheitsversorgungsleistungen und den allgemeinen Zugang zu diesen Leistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität einschließen."

Zudem regelt die DSGVO aber auch die Zulässigkeit der Weiterverarbeitung von Daten zu **Forschungszwecken**. Unterliegt die zulässige Datenverarbeitung normalerweise einer Zweckbindung, ist die Weiterverarbeitung für im **öffentlichen Interesse** liegende wissenschaftliche Forschungszwecke oder für statistische Zwecke auch mit dem ursprünglichen Erhebungszweck vereinbar (Art. 5 Abs. 1 lit. b DSGVO). Dies wird jedoch unter die speziellen Anforderungen des **Art. 89 Abs. 1 DSGVO** gestellt. Dieser besagt:

---

21 Siehe auch Kühling, MedR 2019, 611, 613.

> „Die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken unterliegt **geeigneten Garantien** für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung. Mit diesen Garantien wird sichergestellt, dass **technische und organisatorische Maßnahmen** bestehen, mit denen insbesondere die Achtung des Grundsatzes der **Datenminimierung** gewährleistet wird. Zu diesen Maßnahmen kann die **Pseudonymisierung** gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen. In allen Fällen, in denen diese Zwecke durch die Weiterverarbeitung, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, erfüllt werden können, werden diese Zwecke auf diese Weise erfüllt.“[22]

Art. 9 Abs. 2 lit. j DSGVO regelt darüber hinaus, dass das **Verbot** der Verarbeitung von **Gesundheitsdaten** nach Absatz 1 **nicht gilt**, wenn

> „die Verarbeitung […] auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische **Forschungszwecke** oder für **statistische Zwecke** gemäß Artikel 89 Absatz 1 erforderlich [ist].“

Erwägungsgrund 159 S. 4 der DSGVO betont die besondere Bedeutung der Gesundheitsforschung:[23] „Die wissenschaftlichen Forschungszwecke sollten auch Studien umfassen, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden.“

4.2. Bundesdatenschutzgesetz

Auf nationaler Ebene ist der Datenschutz allgemein im Bundesdatenschutzgesetz (BDSG)[24] geregelt. Das BDSG findet immer dann **Anwendung**, wenn in **bereichsspezifischem Fachrecht** nicht andere Regelungen für den Datenschutz vorgesehen sind (§ 1 Abs. 2 BDSG).[25] Ein solches kann auch in den Sozialgesetzbüchern liegen.

In § 27 Abs. 1 BDSG ist zudem auch ein gewisses **Forschungsprivileg** normiert, dass sich explizit auf den **Gesundheitsdatenschutz** nach Art. 9 Abs. 1 DSGVO bezieht und Abweichungen davon ermöglicht:

> „Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 auch **ohne Einwilligung** für wissenschaftliche oder historische

---

22 Hervorhebung nur hier.

23 Vgl. auch: Weichert, Big Data im Gesundheitsbereich, 2019, S. 190.

24 Bundesdatenschutzgesetz vom 30.6.2017 (BGBl. I S. 2097), das durch Artikel 12 des Gesetzes vom 20.11.2019 (BGBl. I S. 1626) geändert worden ist.

25 Kühling, MedR 2019, 611, 619.

> **Forschungszwecke** oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken **erforderlich** ist und die **Interessen** des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung **erheblich überwiegen**. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor."

§ 22 Abs. 2 BDSG regelt sodann näher die **angemessenen und spezifischen Maßnahmen** zur Wahrung der **Interessen der betroffenen Person**. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu verschiedene Maßnahmen gehören. Genannt sind zum Beispiel die **Pseudonymisierung**, **Verschlüsselung** und **technisch organisatorische Maßnahmen**. Ergänzend dazu fordert § 27 Abs. 3 BDSG, Gesundheitsdaten

> „zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert."

Insofern entspricht die Regelung jedoch wiederum weitgehend den Anforderung des Art. 89 Abs. 1 S. 2 und 3 DSGVO.[26]

§ 27 Abs. 2 BDSG beschränkt im Rahmen der Verwendung der Daten zur Forschung zudem gewisse Betroffenenrechte, wie das Recht auf **Auskunft**, **Widerspruch** oder auf **Berichtigung**.

4.3. Schlussfolgerungen aus dem allgemeinen Datenschutzrecht

Die Regelungen machen deutlich, dass Daten zur medizinischen Forschung mit **Einwilligung** des Betroffenen stets genutzt werden können. Liegt keine Einwilligung vor, so steht die Datennutzung unter dem Vorbehalt einer **Güterabwägung**, die zugunsten des Forschungszweckes ausfallen muss. Aufgrund des überragend wichtigen Zwecks der medizinischen Forschung für die Allgemeinheit kann das Recht der informationellen Selbstbestimmung der einzelnen Betroffenen zurücktreten. Für diese Fälle sind dann organisatorische und verfahrensrechtliche Vorkehrungen vorzunehmen, die die Persönlichkeitsrechte effektiv schützen.[27]

4.4. Problemstellung bzgl. einer wirksamen Einwilligung

Die **Einwilligung** ist in Art. 4 Nr. 11 DSGVO definiert. Verstanden wird darunter jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit

---

26 Weichert, Big Data im Gesundheitsbereich, 2019, S. 190.

27 Weichert, Big Data im Gesundheitsbereich, 2019, S. 191.

der die betroffene Person signalisiert, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Insbesondere für Gesundheitsdaten setzt dies voraus, dass der Einwilligende darüber **informiert** ist, welche Daten weiterverarbeitet werden und für welchen **Zweck** dies erfolgt. Besonders bezüglich der in der medizinischen Forschung mitunter bestehenden Offenheit der zu untersuchenden Fragestellungen ist eine informierte, zweckgebundene Einwilligung regelmäßig schwer zu erreichen.[28] Bezüglich Gesundheitsdaten ist zudem erforderlich, dass der Betroffene ausdrücklich einwilligt. Eine Einwilligung durch konkludentes Handeln ist also nicht möglich (Art. 9 Abs. 2 lit. a DSGVO).[29] Eine Einwilligung gegenüber staatlichen Stellen ist zudem grundsätzlich etwas problematisch, weil die Einwilligung eine gewisse Gleichordnung bzw. Augenhöhe zwischen dem Betroffenen und dem Verarbeitenden voraussetzt.[30]

Die **Freiwilligkeit** der Einwilligung in die Datenverarbeitung kann bei Gesundheitsdaten mitunter auch aufgrund spezieller Situationen nicht gegeben sein. Zum Beispiel in Fällen der Notfallmedizin kann die freie Willensbildung beeinträchtigt sein. Ein weiteres Beispiel bildet die Leistungsinanspruchnahme in unterversorgten ländlichen Gebieten oder auch die von spezialisierten Fachärzten.[31]

Gegebenenfalls können gesetzliche Regelungen hier über den Weg einer Opt-out-Lösung bei der Einwilligung auch komplexe Datenverarbeitungen und Big Data ermöglichen.[32] Dies ist nach der aktuellen Rechtslage jedoch nicht möglich.

4.5. Sozialdatenschutz im SGB I und SGB X

Im Sozialrecht ist geregelt, dass jeder einen Anspruch darauf hat, dass seine Sozialdaten von Leistungsträgern nicht unbefugt verarbeitet werden. Dieses sog. **Sozialgeheimnis** nach § 35 Abs. 1 SGB I richtet sich auch gegen Verbände und Arbeitsgemeinschaften von Leistungsträgern. Sozialdaten sind nach § 67 Abs. 2 SGB X personenbezogene Daten die von Leistungsträgern und weiteren in § 35 Abs. 1 SGB V genannten Stellen im Hinblick auf ihre Aufgaben nach SGB verarbeitet werden. Zu den Leistungsträgern zählen unter anderem die gesetzlichen Krankenversicherungen, die Kassenärztlichen Vereinigungen und die Kassenärztliche Bundesvereinigung.[33] Für diese Sozialdaten sehen §§ 67-85a SGB X ein spezielles Regelungsgeflecht vor. Da Gesundheitsdaten, zum Beispiel wenn sie von einer gesetzlichen Krankenversicherung nach den Vorgaben des

---

28 Weichert, Big Data im Gesundheitsbereich, 2019, S. 191.

29 Kühling/Sackmann/Schildbach (Fn. 4), S. 47.

30 Frenzel, in: Paal/Pauly (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 9, Rn. 24; Kühling/Sackmann/Schildbach (Fn. 4), S. 47.

31 BSG, Urt. v. 10.12.2008 – B 6 KA 37/07 R, Rn. 37; Wobbe, MedR 2019, 625, 628.

32 Weichert, Big Data im Gesundheitsbereich, 2019, S. 128 m.w.N.

33 Schröder, MedR 2019, 631, 632.

SGB V gespeichert werden, auch Sozialdaten darstellen, ist dieses Regelungsgeflecht hier besonders relevant und geht als spezialgesetzliche Regelung den allgemeinen Vorgaben vor.[34] Aufgrund des in § 35 Abs. 2 SGB I genannten **Vorrangs** der Regelungen **der DSGVO** gehen diese Regelungen dem Sozialdatenschutz vor.[35] Zudem verweisen einige Regelungen aus dem genannten Bereich des SGB X auf die Anwendung einzelner Normen des BDSG.[36]

Nach § 303a Abs. 2 SGB V unterliegen ausdrücklich auch die Vertrauensstelle und das Forschungsdatenzentrum dem Sozialgeheimnis nach § 35 SGB V.

4.6. Regelungen der §§ 303a ff. SGB V

Auch die speziellen (neuen) Regelungen in den §§ 303a ff. SGB V können die in Art. 9 Abs. 2 DSGVO eröffneten Spielräume für nationale Gesetzgeber füllen. Dazu müssen die jeweils aufgestellten Voraussetzungen geprüft werden.

Der Gesetzentwurf zum DVG gibt für die Änderungen des § 303b, § 303c und des § 303d SGB V jeweils an:

> „Es handelt sich um eine Verarbeitungsbefugnis im Sinne des Artikel 6 Absatz 1 Buchstabe e, Absatz 2 und Absatz 3 Satz 1 Buchstabe b, Satz 2 in Verbindung mit Artikel 9 Absatz 2 Buchstaben h, i und j und Absatz 4 der Verordnung (EU) 2016/679.“[37]

Es kann angenommen werden, dass die Möglichkeit der Abrufung der entsprechenden Daten durch den Kreis der **berechtigten Nutzer** bei dem **Forschungsdatenzentrum** dem Zweck der

- Gesundheitsvorsorge bzw. der Versorgung oder Behandlung im Gesundheits-/Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits-/Sozialbereich (Art. 9 Abs. 2 lit. h DSGVO),
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie der Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten (Art. 9 Abs. 2 lit. i DSGVO), oder
- im öffentlichen Interesse liegenden Archivzwecken, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke (Art. 9 Abs. 2 lit. j DSGVO)

dient. Sollte es sich bei den zu verarbeitenden Daten nicht um Gesundheitsdaten, bzw. andere nach Art. 9 Abs. 1 DSGVO besonders geschützte Daten handeln, so wäre die Öffnungsklausel des

---

34 Vgl. auch: Kühling, MedR 2019, 611, 615 f.

35 Wobbe, MedR 2019, 625, 627; Kühling, MedR 2019, 611, 619.

36 Wobbe, MedR 2019, 625, 627.

37 Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz - DVG), 9.8.2019, BR-Drs. 360/19, S. 78 f.

Art. 6 Abs. 2 iVm Abs. 1 S. 1 lit. e DSGVO einschlägig.[38] Dass die Regelungen der §§ 303a ff. SGB V entsprechende **Verarbeitungsbefugnisse** darstellen, wird auch in der (bislang übersichtlichen) Literatur so gesehen.[39] Dafür sprechen auch die in den Erwägungsgründen 53 S. 1 und 54 S. 3 zur DSGVO vorgenommenen weiten Auslegungen der Begrifflichkeiten und Zwecke. Auch das geforderte Berufsträgergeheimnis bzw. entsprechende technisch organisatorische Maßnahmen werden soweit ersichtlich in den Vorgaben der §§ 303 a ff. SGB V berücksichtigt. Demnach kommt es auch nicht auf die weiteren Zulässigkeitstatbestände des Art. 9 Abs. 2 DSGVO wie die Einwilligung an, um die Datenverarbeitung an dieser Stelle rechtmäßig zu gestalten.[40] Der dem nationalen Gesetzgeber durch die DSGVO eröffnete Gestaltungsspielraum wurde insofern genutzt.

Fraglich scheint jedoch, ob diese Rechtfertigung auch für die vorherige Übertragung der lediglich pseudonymisierten Daten von den **Krankenversicherungen** auf die **Datensammelstelle** gilt. Die Datensammlung und Prüfung durch die Datensammelstelle ist eine Datenverarbeitung, die allein als eine **vorbereitende Handlung** dazu dient, die spätere Bereitstellung der Daten an die Nutzer zu vereinfachen. Zu diesem Zeitpunkt besteht noch **kein konkretes Forschungsvorhaben oder Erkenntnisinteresse** zur Verbesserung der Gesundheitsforschung, das es ermöglicht, diese Datenverarbeitung zu begründen und auch entsprechend zu privilegieren. Es ist mithin möglich, dass im Rahmen der Datenübertragung von den ca. 73 Mio. gesetzlich Versicherten in Deutschland zahlreiche Daten an die Datensammelstelle übertragen werden, deren Inhalt nicht durch die berechtigten Nutzer abgefragt wird. Dies widerspricht insoweit auch dem in Art. 5 Abs. 1 lit. c DSGVO geregelten Grundsatz der **Datensparsamkeit** bzw. der Datenminimierung. Ob das Forschungsprivileg bereits soweit im Vorfeld Wirkung erlangt, ist insoweit **nicht eindeutig**.

Dass die §§ 303a ff. SGB V das **Recht auf Widerspruch** seitens des Betroffenen nicht berücksichtigen, entspricht der Regelung des § 27 Abs. 2 BDSG. Danach sind für die Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken bzw. für statistische Zwecke die Rechte auf Auskunft, Widerspruch oder Berichtigung beschränkt, soweit sie voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Soweit man die Zwecke, zu denen die berechtigten Nutzer eine Datenverarbeitung vornehmen, unter die Aspekte der Forschungs- oder Statistikzwecke subsumieren kann, ist mithin eine Rechtsgrundlage für die Beschränkung des Widerspruchsrechts gegeben. Diese steht normhierarchisch auch auf der gleichen Ebene wie die Regelungen der §§ 303a ff. SGB V.

5. Grundrecht auf informationelle Selbstbestimmung

Die Regelungen des nationalen Gesetzgebers müssen nicht nur die Voraussetzungen der DSGVO für abweichendes Recht beachten (siehe oben Punkt 4.6.), sondern auch die Anforderungen des

38 Kühling/Schildbach, NZS 2020, 41, 45.

39 Platzer, NZS 2020, 289, 290; Kühling/Schildbach, NZS 2020, 41, 45.

40 Kühling/Schildbach, NZS 2020, 41, 45.

Grundgesetzes. In Betracht kommt möglicherweise eine Verletzung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Aus dem allgemeinen Persönlichkeitsrecht wird auch das **Recht auf informationelle Selbstbestimmung** abgeleitet.

5.1. Schutzbereich und Eingriff

Das Recht auf informationelle Selbstbestimmung umfasst das Recht des Einzelnen, grundsätzlich selbst zu entscheiden, wann und gegenüber wem er zu welchem Zweck Lebenssachverhalte im Allgemeinen und personenbezogene Daten im Besonderen offenbart.[41] Die Übermittlung von Gesundheitsdaten – als spezielle personenbezogene Daten – an Dritte ist vom **Schutzbereich** des Grundrechts umfasst. Der grundrechtliche Schutz beginnt insoweit schon auf der Stufe der Gefährdung der Rechtsgüter, ohne dass es einer konkreten Bedrohung bedarf.[42] Die Vorfeldwirkung des Grundrechts auf informationelle Selbstbestimmung besteht also auch bereits vor der Datenverarbeitung sowie vor den schädlichen Auswirkungen auf die Betroffenen.[43] Dazu entschied das Bundesverfassungsgericht:

> „Eine derartige Gefährdungslage kann bereits im Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter entstehen, so insbesondere wenn personenbezogene Informationen in einer Art und Weise genutzt und verknüpft werden, die der Betroffene weder überschauen noch beherrschen kann. Vor allem mittels elektronischer Datenverarbeitung können aus solchen Informationen weitere Informationen erzeugt und so Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen als auch Eingriffe in seine Verhaltensfreiheit mit sich bringen können.“[44]

Zudem muss ein **Eingriff** in diesen Schutzbereich vorliegen. Im Sinne des klassischen Eingriffsbegriffs liegt ein Eingriff vor, wenn er final, unmittelbar, durch Rechtsakt sowie mit Befehl und Zwang gegenüber dem Einzelnen angeordnet bzw. durchgesetzt wird.[45] Durch den neuen Eingriffsbegriff wurde diese Definition erweitert. Nunmehr ist als Eingriff jedes staatliche Handeln umfasst, das ein grundrechtlich geschütztes Verhalten erschwert oder unmöglich macht bzw. ein grundrechtlich geschütztes Rechtsgut beeinträchtigt. Umfasst sind auch mittelbare und faktische Eingriffe.[46] Das **Bundesverfassungsgericht** hat jüngst in einem Verfahren des einstweiligen Rechtsschutzes gegen das DVG bestätigt, dass es sich bei den Datenverarbeitungs- und -übermittlungsmaßnahmen um einen Grundrechtseingriff handelt.

---

41 BVerfG, Urteil vom 4.4.2006 – 1 BvR 518/02, BVerfGE 115, 320, 341; Dreier, in: ders. (Hrsg.), Grundgesetz-Kommentar, 3. Auflage 2013, Art. 2 Abs. 1, Rn. 79.

42 BVerfG, Beschluss vom 13.6.2007 – 1 BvR 1550/03, 2357/04, 603/05, BVerfGE 118, 168, 184 f., Rn. 87.

43 Kühling/Sackmann/Schildbach (Fn. 4), S. 83.

44 BVerfG, Beschluss vom 13.6.2007 – 1 BvR 1550/03, 2357/04, 603/05, BVerfGE 118, 168, 184 f., Rn. 87.

45 Ipsen, Staatsrecht II, 21. Auflage 2018, Rn. 143; Voßkuhle/Kaiser, JuS 2009, 313.

46 Voßkuhle/Kaiser, JuS 2009, 313.

> „In den durch § 68a Abs. 5, §§ 303a ff. SGB V vorgesehenen Datenverarbeitungs- und -übermittlungsmaßnahmen liegt vor allem in Anbetracht des teils sensiblen und in hohem Maße persönlichkeitsrelevanten Charakters der genutzten Daten und der dabei breitflächigen Erhebung ein **erheblicher Grundrechtseingriff**. Verstärkt wird dieser Effekt durch die beträchtliche Menge an Daten, die erhoben, übermittelt, ausgewertet und anderweitig weiterverarbeitet werden dürfen. Insofern ist darauf zu verweisen, dass auch einzelne Daten mit scheinbar gering ausgeprägter Persönlichkeitsrelevanz in der Zusammenschau mit anderen Daten einen intensiven Persönlichkeitsbezug entfalten können […].“[47]

5.2. Verfassungsrechtliche Rechtfertigung

Das Recht auf informationelle Selbstbestimmung ist jedoch nicht schrankenlos gewährleistet. Aufgrund der Gemeinwohlbindung des Grundrechts sind Beschränkungen aus überwiegendem Allgemeininteresse möglich. Dazu ist jedoch zwingend eine gesetzliche Grundlage erforderlich, die auch dem Grundsatz der Verhältnismäßigkeit gerecht wird.[48]

Das **überwiegende Allgemeininteresse** kann vorliegend in der medizinischen Forschung und der Verbesserung der Gesundheitsversorgung gesehen werden. Diese Ziele stellen wichtige Gemeinwohlbelange dar.[49] Sie gehen auch klar aus dem Gesetzentwurf zum DVG hervor.[50]

Für die Annahme der **Verhältnismäßigkeit** eines Eingriffs bedarf es eines legitimen Zwecks, der mit der Maßnahme erreicht werden soll, wobei diese geeignet, erforderlich und angemessen sein muss, um diesen Zweck auch zu erreichen. Das Bundesverfassungsgericht deutete bzgl. der Prüfung des DVG in einem eventuellen späteren Hauptsacheverfahren an:

> „In einem gegebenenfalls durchzuführenden Hauptsacheverfahren würden sich komplexe Fragen der verfassungsrechtlichen Datenschutzdogmatik stellen, insbesondere die Frage, ob die vom Gesetzgeber mit dem Digitale-Versorgung-Gesetz verfolgten Zwecke auch durch eine in Umfang, Erhebungs- oder Verarbeitungsmodalitäten begrenzte Datennutzung (zum Beispiel durch verpflichtend einzuholende Einwilligungen oder weiter als bisher reichende Widerspruchsmöglichkeiten der Versicherten) im Ergebnis ohne nennenswerte Abstriche hinsichtlich Repräsentativität und Qualität des Datenmaterials erreicht werden könnten. […] Hierbei wird besonderes Augenmerk auf die Aspekte der Anonymisierung und Pseudonymisierung sowie auf die Vorkehrungen zur IT-Datensicherheit und auf die institutionelle Ausgestaltung der datenverarbeitenden Stellen zu richten sein.“[51]

---

47 BVerfG, Beschluss vom 19.3.2020 – 1 BvQ 1/20, Rn. 13. Hervorhebung nur hier.

48 BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83, 269/83, 362/83, 420/83, 440/83, 484/83, BVerfGE 65. 1, 43 f.; Kühling/Sackmann/Schildbach (Fn. 4), S. 84.

49 So auch BVerfG, Beschluss vom 19.3.2020 – 1 BvQ 1/20, Rn. 15.

50 Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz - DVG), 9.8.2019, BR-Drs. 360/19, S. 2.

51 BVerfG, Beschluss vom 19.3.2020 – 1 BvQ 1/20, Rn. 8.

Insofern formuliert das Bundesverfassungsgericht bereits mehrere Fragen für die Verhältnismäßigkeitsprüfung.

5.2.1. Legitimer Zweck und Geeignetheit

Dass die Datenverarbeitung der genannten Stellen einem **legitimen Zweck** dient, ergibt sich bereits aus der **Gemeinwohldienlichkeit** der Verbesserung der Gesundheitsforschung. Dies gilt sowohl für die Datenverarbeitung durch den entsprechend „forschenden" Nutzer als auch für die vorbereitenden Maßnahmen der Datensammelstelle, Vertrauensstelle und des Forschungsdatenzentrums. Denn auch die entsprechende Aufbereitung und Vorbereitung der Daten dient dem entsprechenden Zweck.

Die Datenverarbeitung durch Sammlung, Prüfung, Aggregierung, etc. ist in allen genannten Schritten auch **geeignet** den entsprechenden Zweck zu fördern.

5.2.2. Erforderlichkeit

Eine Maßnahme ist **erforderlich**, wenn keine **anderen Mittel** zur Verfügung stehen, die in gleicher oder sogar besserer Weise das Ziel erreichen könnten. Dies steht insoweit in Frage, als insbesondere in dem ersten Datenverarbeitungsschritt der Sammlung und Prüfung der Daten durch die Datensammelstelle nicht hinreichend ersichtlich ist, dass alle dort gebündelten und gesammelten Daten auch notwendig sind, um die Zwecke der berechtigten Nutzer zu erfüllen. Wenn unabhängig von dem sich erst später ergebenden Erkenntnisinteresse Daten gesammelt werden, so können sich die damit verbundenen **Grundrechtseingriffe** als **unnötig** erweisen. Dieses Verständnis kann auch der Entscheidung des Bundesverfassungsgerichts zur Verfassungswidrigkeit der Vorratsdatenspeicherung entnommen werden.[52]

Zu berücksichtigen ist jedoch auch, dass ohne die Datenübertragung an die Datensammelstelle drohen könnte, dass eben jene Daten bei einem erst später identifizierten Erkenntnisinteresse nicht mehr für die Forschung zur Verfügung stünden. Insoweit muss also einbezogen werden, wie die Daten durch die gesetzlichen Krankenversicherungen als erstes Glied in der Übertragungskette der §§ 303a ff. SGB V gespeichert werden. Die Löschfristen sind entsprechend § 304 SGB V an den unterschiedlichen Datenursprüngen ausgerichtet und betragen beispielsweise für Daten der Abrechnung ärztlicher Leistungen 10 Jahre. Diese Fristen können aber auch nach jetziger Rechtslage gem. § 287 SGB V verlängert werden, wenn die Daten für Forschungsvorhaben benötigt werden. Auch eine gesetzlich andere Ausgestaltung bei der die jeweils forschungsrelevanten Daten länger bei den gesetzlichen Krankenkassen abrufbar sind und dann über das Verfahren nach den §§ 303a ff. SGB V zur Verfügung gestellt werden können, ist denkbar. Bislang ist zudem die **Löschung der Daten** nur bei der Vertrauensstelle (nach der Übermittlung an das FDZ, § 303c Abs. 3 S. 2 SGB V) und dem Forschungsdatenzentrum (nach 30 Jahren, § 303d Abs. 3 SGB V) geregelt, nicht jedoch für die Datensammelstelle. Insofern scheinen **mildere Mittel denkbar**, die an der Stelle einer zentralen Sammlung der Daten stehen könnten.

52 BVerfG, Urteil vom 2.3.2010 – 1 BvR 256/08, 263/08, 586/08, BVerfGE 125, 260 ff.

5.2.3. Angemessenheit

Darüber hinaus bestehen auch bestimmte Bedenken gegenüber der Angemessenheit der Maßnahme. Eine Maßnahme ist nur dann angemessen, wenn die mit der Maßnahme verbundenen Nachteile nicht vollkommen außer Verhältnis zu den damit verbundenen Vorteilen stehen.

Das Bundesverfassungsgericht machte in seiner Entscheidung zur Vorratsdatenspeicherung den Aspekt der **Datensicherheit** zum Gegenstand der Verhältnismäßigkeitsabwägung des Grundrechtseingriffs.[53] Auf diesen Aspekt ging das Gericht auch im einstweiligen Rechtsschutzverfahren zum DVG ein. Es hatte insoweit zu entscheiden, ob durch die Anwendung des DVG irreversible bzw. nur sehr erschwert revidierbare Nachteile drohen würden. Dazu führte das Gericht aus:

> „Dieser Nachteil tritt aber nicht unmittelbar durch den Vollzug der angegriffenen Vorschriften ein, sondern erst dann, wenn – entgegen der gesetzlich angeordneten Pseudonymisierung oder Anonymisierung – durch die datenverarbeitenden Stellen ein Personenbezug zu bestimmten Versicherten hergestellt wurde, was das Gesetz durch verschiedene **Vorkehrungen und prozedurale Sicherungen** gerade zu verhindern sucht. Auch was die **Missbrauchsanfälligkeit größerer Datensammlungen** für den **unberechtigten Zugriff Dritter** angeht, bildet ein solches unberechtigtes Zugreifen einen – noch dazu vom Gesetz nicht gebilligten – Zwischenschritt, dessen Eintritt nicht mit hinreichender Sicherheit als unmittelbar bevorstehend angenommen werden kann. Im Hinblick auf zu Unrecht erhobene und gespeicherte Daten, die sich bei den hierzu befugten Stellen befinden, könnten hingegen Löschungsanordnungen ergehen, sodass der eingetretene Nachteil nicht irreversibel wäre.“[54]

Darüber hinaus begründet eine neuere Studie Zweifel an der tatsächlichen Anonymität bestimmter Daten oder Datensätze, da zahlreiche angeblich anonymisierte Daten nur pseudonymisiert sind und die dahinter stehenden Personen relativ leicht ermittelt werden könnten.[55] Die Reidentifikation ist hier zwar verboten und unter Strafe gestellt, zugleich macht die Formulierung in § 303d Abs. 1 Nr. 5 SGB V – nach der durch das FDZ das spezifische **Reidentifikationsrisiko** bewertet und durch geeignete Maßnahmen minimiert werden soll – deutlich, dass es nicht ausgeschlossen werden kann.[56] Jedoch muss bei einer rein rechtlichen Betrachtung davon ausgegangen

---

53 BVerfG, Urteil vom 2.3.2010 – 1 BvR 256/08, 263/08, 586/08, BVerfGE 125, 260, Rn. 221 ff.

54 BVerfG, Beschluss vom 19.3.2020 – 1 BvQ 1/20, Rn. 13. Hervorhebung nur hier.

55 Henning, Weitere Studie belegt Lüge „anonymer“ Daten, abrufbar unter: https://netzpolitik.org/2019/weitere-studie-belegt-luege-anonymer-daten/ (zuletzt aufgerufen am 14.8.2020). Kritisch auch: Digitale Gesellschaft, Stellungnahme zum Digitale Versorgung-Gesetz, vom 19.9.2019, abrufbar unter: https://digitalegesellschaft.de/2019/09/gegen-den-ausverkauf-der-gesundheitsdaten-fuer-ein-moratorium-in-der-digitalisierung-des-gesundheitswesens/ (zuletzt aufgerufen am 14.8.2020).

56 Bestätigend Sachverständiger Butz, Bundesärztekammer, Protokoll-Nr. 19/63, Ausschuss für Gesundheit, 16.10.2019, S. 21. Vgl. auch Kühling/Schildbach, NZS 2020, 41, 43 f.

werden, dass die rechtlich geforderte Anonymisierung auch rein tatsächlich vorgenommen wird sowie die Strafandrohung für die Reidentifikation eine solche auch wirksam verhindert.[57]

Inwieweit den Aspekten der IT-Datensicherheit und der ausreichenden Anonymisierung und Pseudonymisierung ausreichend Rechnung getragen wird, hat auch das Bundesverfassungsgericht der Prüfung in einem eventuellen Hauptsacheverfahren vorbehalten (siehe oben 5.2.). Dieser Prüfung kann an dieser Stelle mangels sachverständiger Erkenntnisquellen nicht vorweggegriffen werden.

6. Ergebnis

Die vorangegangene Darstellung macht deutlich, dass hinsichtlich der Verhältnismäßigkeit des mit der Datenverarbeitung in Zusammenhang stehenden Grundrechtseingriffs Bedenken bestehen. Insbesondere die Erforderlichkeit der Datenverarbeitung durch die Datensammelstelle als Ort der Datenzentralisierung im Vorfeld von eventueller Forschung ist dabei fraglich (siehe Punkt 5.2.2.).

Ebenfalls bestehen datenschutzrechtliche Bedenken. Die Datenverarbeitung durch die Datensammelstelle im Vorfeld eventueller Gesundheitsforschung kann nicht eindeutig auf bestehende Privilegierungen der Forschung als Ausnahme des strengen Schutzes von Gesundheitsdaten gestützt werden (siehe Punkt 4.6.).

***

57 Letzteres so angenommen von Kühling/Schildbach, NZS 2020, 41, 50.