Fachbereiche WD 3 und EU 6

Unions- und verfassungsrechtlicher Rahmen für einen zweckändernden Austausch von Daten über psychisch erkrankte Personen zur Prävention von Fremdgefährdungen

© 2026 Deutscher Bundestag

Unions- und verfassungsrechtlicher Rahmen für einen zweckändernden Austausch von Daten über psychisch erkrankte Personen zur Prävention von Fremdgefährdungen

Aktenzeichen:	WD 3-30000-0005-0021 und EU 6-30000-0007-0033
Abschluss der Arbeit:	12.10.2026 (zugleich letzter Abruf der Internetlinks)
Fachbereich:	WD 3: Verfassung und Verwaltung EU 6: Europa- und Völkerrecht, Auswärtiges und Sicherheit

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

Inhaltsverzeichnis

1.	**Einleitung**	**4**
2.	**Unionsrechtliche Zulässigkeit**	**5**
2.1.	Potenziell einschlägiges EU-Datenschutzregime im Überblick	6
2.2.	DS-GVO	8
2.2.1.	Art. 6 Abs. 1 und Art. 9 DS-GVO	9
2.2.1.1.	Art. 9 Abs. 2 lit. c) DS-GVO	10
2.2.1.2.	Art. 9 Abs. 2 lit. g) DS-GVO	11
2.2.1.2.1.	Erhebliches öffentliches Interesse	11
2.2.1.2.2.	Wesensgehaltgarantie und Verhältnismäßigkeit	12
2.2.1.2.3.	Angemessene und spezifische Schutzmaßnahmen	15
2.2.1.3.	Folgerungen im Auftragskontext	16
2.2.2.	Zweckänderung	16
2.2.2.1.	Anforderungen an eine mitgliedstaatliche Rechtsgrundlage	18
2.2.2.2.	Zweckänderung hinsichtlich sensibler Daten	18
2.2.3.	Zwischenergebnis zur DS-GVO	19
2.3.	JI-RL	19
2.3.1.	Art. 4 ff. JI-RL	19
2.3.2.	Art. 10 JI-RL	20
2.3.3.	Folgerungen zur JI-RL im Auftragskontext	23
3.	**Verfassungsrechtliche Zulässigkeit**	**24**
3.1.	Verbandskompetenz des Bundes	24
3.1.1.	Gesetzgebungskompetenz aus Art. 71, 73 Abs. 1 Nr. 10 Buchst. a GG	24
3.1.2.	Doppeltür-Modell des BVerfG	26
3.1.3.	Gesetzgebungskompetenzen des Bundes für Teilbereiche	27
3.1.3.1.	Sicherheitsrecht / Gefahrenabwehrrecht	27
3.1.3.2.	Gesundheitsrecht	27
3.1.3.3.	Waffenrecht	28
3.2.	Vereinbarkeit mit dem Grundrecht auf informationelle Selbstbestimmung	29
3.2.1.	Eingriff in den Schutzbereich	29
3.2.2.	Verfassungsrechtliche Rechtfertigung	30
3.2.2.1.	Bestimmtheit und Normenklarheit	30
3.2.2.2.	Besonderheiten bei Zweckänderungen	31
3.2.2.3.	Verhältnismäßigkeit	32

1. Einleitung

Die Wissenschaftlichen Dienste des Deutschen Bundestages wurden gebeten, zu prüfen, welche unionsrechtlichen und verfassungsrechtlichen Gesichtspunkte zu berücksichtigen wären, wollte man Gesundheitsdaten und Behandlungsdaten mit anderen Datensätzen verknüpfen und so für Zwecke nutzen, für die sie nicht erhoben wurden, beispielsweise für die Verbrechensbekämpfung. Bezug genommen wurde auf eine **Entschließung des Bundesrates**, mit der die Bundesregierung aufgefordert wird, den **staatlichen Informationsaustausch über Menschen mit schweren psychischen Erkrankungen** zu regeln und die **medizinische und rehabilitative Versorgung** dieser Menschen **nachhaltig zu verbessern.**

In der am 30. Januar 2026 auf Antrag des Landes Niedersachen[1] beschlossenen Entschließung[2] fordert der Bundesrat die Bundesregierung anlässlich verschiedener Vorfälle von Gewalttaten, die in der jüngeren Zeit durch psychisch Erkrankte begangen wurden, dazu auf, den **Informationsaustausch zwischen staatlichen Stellen** in Fällen eines erkennbaren erhöhten Fremdgefährdungspotenzials **ressortübergreifend zu verbessern**. So heißt es in der Entschließung:

> „Vor diesem Hintergrund fordert der Bundesrat die Bundesregierung auf, insbesondere den Austausch von Gesundheitsdaten und den Erkenntnissen der Gefahrenabwehrbehörden unter datenschutzrechtlichen Vorgaben zu prüfen und hier zügig zu Anpassungen im Sinne eines modernen Daten- und Informationsmanagements sowie einer besseren bundesweiten Vernetzung der Erkenntnisse zwischen Sicherheits-, Gesundheits-, Waffen- und gegebenenfalls anderen relevanten Behörden zu kommen, um Risikopotentiale bei Personen mit psychischen Auffälligkeiten möglichst frühzeitig zu erkennen […].“

Des Weiteren fordert der Bundesrat die Bundesregierung auf, die **medizinische und rehabilitative Versorgung** von Menschen mit schweren psychischen Erkrankungen nachhaltig zu verbessern und verweist dazu auf die Maßnahmen, die der „Dialog zur Weiterentwicklung der Hilfen für psychisch erkrankte Menschen“ im Auftrag des Bundesministeriums der Gesundheit (BMG) vorgelegt hat.

Die zunächst erfolgende EU-rechtliche Betrachtung beleuchtet den unionsrechtlichen Rahmen für eine zweckändernde Weiterverarbeitung von Gesundheitsdaten. Dazu wird zunächst ein Überblick über die im Auftragskontext potenziell relevanten EU-Sekundärrechtsakte gegeben (vgl. Ziff. 2.1.). Anschließend werden diese auf mögliche Vorgaben in Bezug auf eine Verknüpfung der Gesundheitsdaten bzw. ihre Verwendung für einen anderen als den Erhebungszweck untersucht (vgl. Ziff. 2.2. und Ziff. 2.3.). Auftragsgemäß wird dabei im Wesentlichen auf datenschutzrechtliche Bestimmungen des unionalen Sekundärrechts eingegangen. Eine Prüfung unmittelbar am Maßstab der Grundrechte aus der Grundrechtecharta (GRCh) erfolgt aufgrund der

---

1 Antrag des Landes Niedersachsen vom 01.12.2025, BR-Drs. 717/25.

2 Beschluss des Bundesrates, Plenarprotokoll 1061 vom 30.01.2026, S. 28.

weitgehend sekundärrechtlichen Determinierung der EU-Datenschutzordnung nicht.[3] Die anschließende verfassungsrechtliche Prüfung (vgl. Ziff. 3) geht zunächst der Frage nach, inwieweit dem Bund eine Gesetzgebungskompetenz zusteht, die es ihm erlauben würde, den Datenaustausch insgesamt oder zumindest für bestimmte materielle Teilbereiche zu regeln (vgl. Ziff. 3.1.). Im Anschluss wird dargestellt, welche Vorgaben das Bundesverfassungsgericht (BVerfG) dem Gesetzgeber für die Ausgestaltung gesetzlicher Bestimmungen gemacht hat, die – wie im Fall der Regelungen über den Datenaustausch – in das Recht auf informationelle Selbstbestimmung eingreifen (vgl. Ziff. 3.2.).

Da die Entschließung des Bundesrates offenlässt, in welcher Art und Weise der Datenaustausch genau erfolgen soll und welche staatlichen Stellen im Einzelnen in welcher Weise daran beteiligt sein könnten, werden im Verlauf der Bearbeitung sowohl verstetigte Varianten (Datencluster/Verbunddatei) als auch ein ad hoc-Austausch von Informationen angesprochen. Dabei wird davon ausgegangen, dass die Informationen zusammengeführt werden sollen, um eine wie auch immer im Einzelnen geartete Prognose über die von einer psychisch kranken Person ausgehenden Fremdgefährdung zu erstellen. Mangels eines konkreten Regelungsvorschlags können vor allem die vom Gesetzgeber zu beachtenden Vorgaben und Leitlinien dargestellt werden. Eine genaue Beurteilung der unions-/datenschutzrechtlichen und verfassungsrechtlichen Zulässigkeit kann nur anhand einer konkreten, bereits vorliegenden Regelung erfolgen.

2. Unionsrechtliche Zulässigkeit

Der folgende Abschnitt befasst sich mit den unionsrechtlichen Rahmenbedingungen für eine mitgliedstaatliche Regelung zur Verknüpfung von Gesundheits- und Behandlungsdaten[4] mit anderen Datensätzen und deren Verwendung für Zwecke, für die sie nicht erhoben wurden (insbesondere Verbrechensbekämpfung[5]).

3 Die Grundrechte (insbesondere Art. 7 und 8 GRCh) kommen bei der Prüfung nationaler Rechtsakte durch den EuGH im Wesentlichen als Prüfungs- und zunehmend auch Interpretationsmaßstab des Sekundärrechts zur Anwendung, vgl. nur Kühling, in: Pechstein/Nowak/Häde, Frankfurter Kommentar EUV/GRC/AEUV, 2. Aufl. 2023, Art. 8 GRCh Rn. 1.

4 Nachfolgend wird allein der Begriff der Gesundheitsdaten verwendet, da dieser gemäß Art. 4 Nr. 15 EU-Datenschutzgrundverordnung Daten über die Erbringung von Gesundheitsdienstleistungen und damit Behandlungsdaten umfasst.

5 Dem nachfolgenden Abschnitt liegt ein weites Verständnis des Begriffs der Verbrechensbekämpfung zugrunde. Demnach umfasst dieser sowohl präventive als auch repressive Maßnahmen zur Verhütung bzw. Verfolgung von Straftaten.

2.1. Potenziell einschlägiges EU-Datenschutzregime im Überblick

Die auftragsgegenständliche Maßnahme wäre insbesondere am unionalen Datenschutzsekundärrecht zu messen. Im Einzelnen kommen vorliegend die Datenschutz-Grundverordnung[6] (im Folgenden: DS-GVO) sowie die Richtlinie (EU) 2016/680[7] (im Folgenden: JI-RL) in Betracht.[8]

Die DS-GVO dient gemäß ihrem Art. 1 Abs. 1 insbesondere dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und bildet das EU-datenschutzrechtliche Fundament.[9] Die von der Europäischen Kommission Ende 2025 vorgeschlagenen Änderungen der DS-GVO sind noch nicht verabschiedet.[10] Nach aktuellem Stand hätten sie keine Auswirkungen auf die auftragsgegenständliche Frage. Demgegenüber regelt die JI-RL gemäß ihrem Art. 1 Abs. 1 speziell die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten[11] oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

Für die Abgrenzung der Anwendungsbereiche der DS-GVO und der JI-RL im Auftragskontext ist Art. 2 Abs. 2 lit. d) DS-GVO maßgeblich. Danach findet die DS-GVO keine Anwendung auf die in

---

6 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 (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1 ff. (berichtigte Fassung v. 4. Mai 2016).

7 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 v. 4. Mai 2016, S. 89 ff. (berichtigte Fassung v. 4. Mai 2016).

8 Die Gesundheitsdaten-VO (Verordnung (EU) 2025/327 des Europäischen Parlaments und des Rates vom 11. Februar 2025 über den europäischen Gesundheitsdatenraum sowie zur Änderung der Richtlinie 2011/24/EU und der Verordnung (EU) 2024/2847, ABl. L, 2025/327 v. 5. März 2025) regelt hingegen den europäischen Gesundheitsdatenraum i. e. S. und enthält allein Vorgaben für die Sekundärnutzung von Gesundheitsdaten innerhalb des Gesundheitsdatenraums, vgl. Art. 53 f. VO 2024/2847. Darüber hinaus ist das Kapitel IV über die Sekundärnutzung erst ab dem 26. März 2029 anwendbar, vgl. Art. 105 Abs. 5 VO 2024/2847. Auf die Daten-Governance-VO (Verordnung (EU) 2022/868), welche u. a. Bedingungen für die innerunionale Weiterverwendung von Daten bestimmter Datenkategorien festlegt, die im Besitz öffentlicher Stellen sind, wird nicht eingegangen, da ihre Vorgaben gemäß Art. 1 Abs. 3 S. 2 Daten-Governance-VO insbesondere unbeschadet der hier beleuchteten DS-GVO und JI-RL gelten und diese Rechtsakte gemäß Art. 1 Abs. 3 S. 3 Daten-Governance-VO im Falle eines Normkonflikts Vorrang genießen.

9 Selmayr/Ehmann, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl. 2024, Einleitung Rn. 3.

10 Vgl. Art. 3 des Kommissionvorschlags für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnungen (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 und der Richtlinien 2002/58/EG, (EU) 2022/2555 und (EU) 2022/2557 hinsichtlich der Vereinfachung des digitalen Rechtsrahmens und zur Aufhebung der Verordnungen (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 und der Richtlinie (EU) 2019/1024 (Digital-Omnibus-Verordnung), KOM(2025) 837 endg., 19. November 2025. Der Kommissionsvorschlag wird derzeit im Rat beraten, s. EU Law Tracker zu 2025/0360(COD).

11 Zum autonom-unionsrechtlich zu interpretierenden Begriff der Straftat siehe Bäcker, in: BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg, 56. Edition, Stand: 01.08.2023, Art. 2 DS-GVO Rn. 25.

den Anwendungsbereich der JI-RL fallende Verarbeitung personenbezogener Daten. Sofern also eine Datenverarbeitung „**durch die zuständigen Behörden** zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von **Straftaten** oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die **öffentliche Sicherheit**“ erfolgt, ist diese vorrangig an dem spezielleren Regime der **JI-RL** zu messen. Folglich müssen zwei Voraussetzungen erfüllt sein, damit eine Datenverarbeitung unter die JI-RL und nicht die DS-GVO fällt:[12]

– Es muss sich um eine Datenverarbeitung handeln, die den Zwecken der JI-RL unterfällt (Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit) und

– es muss sich bei dem Verantwortlichen der Verarbeitung i. S. v. Art. 4 Nr. 8 JI-RL um eine „zuständige Behörde“[13] im Sinne des Art. 2 Abs. 2 DS-GVO handeln. Auf andere Fälle der Datenverarbeitung (d. h. bei Datenverarbeitungen durch **Behörden für andere Zwecke** oder bei Datenverarbeitungen durch **Private unabhängig vom Zweck**) findet die **DS-GVO** Anwendung.[14]

Eine Schnittstelle zwischen den beiden Rechtsakten entsteht bei Datenübermittlungen (nebst vorgesehener Weiterverarbeitung) zwischen einer Stelle, deren Datenverarbeitungen unter die DS-GVO fallen, und einer unter die JI-RL fallenden Behörde. In diesen Fällen bestimmt sich die Zuordnung der einzelnen Datenverarbeitungen im Übermittlungsprozess nach der jeweils handelnden Stelle und ggf. dem Zweck der Datenverarbeitung (sog. Doppeltürmodell, wonach insbesondere zwischen Übermittlung und Abruf der betreffenden Daten zu differenzieren ist[15]).[16] Um das einschlägige Regelungsregime zu bestimmen, ist daher eine Betrachtung der einzelnen Verarbeitungsschritte und der jeweils verantwortlichen Akteure notwendig.

Nachfolgend werden die DS-GVO und die JI-RL daraufhin untersucht, welche Vorgaben sie für nationale Regelungen treffen, die auf die Verknüpfung von Gesundheitsdaten mit anderen

---

12 EuGH, Urteil vom 21. Juni 2022, Rs. C-817/19, Ligue des droits humains, Rn. 67.

13 Hierbei handelt es sich gemäß dem auch auf die DS-GVO Anwendung findenden Art. 3 Nr. 7 JI-RL (vgl. EuGH, Urteil vom 22. Juni 2021, Rs. C-439/19, Latvijas Republikas Saeima, Rn. 69) um a) eine staatliche Stelle, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständig ist, oder b) eine andere Stelle oder Einrichtung, der durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, übertragen wurde.

14 Vgl. zur Abgrenzung zw. der DS-GVO und der JI-RL sowie den Anforderungen an die nationale Gesetzgebung: EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti, Rn. 61 ff.

15 Vgl. hierzu grundlegend BVerfG, Beschluss vom 24. Januar 2012, 1 BvR 1299/05, Rn. 123.

16 EuGH, Urteil vom 21. Juni 2022, Rs. C-817/19, Ligue des droits humains, Rn. 77 ff. Vgl. auch das Urteil des EuGH vom 4. Juli 2023, Rs. C-252/21, Meta Platforms Inc, Rn. 91 ff., in welchem dieser eine Datenverarbeitung durch ein Unternehmen zum Zweck der Information von Strafverfolgungs- und Strafvollstreckungsbehörden ohne Weiteres an Art. 6 DS-GVO gemessen hat.

Datensätzen und deren Verwendung für vom ursprünglichen Erhebungszweck abweichende Zwecke (insbesondere Verbrechensbekämpfung) abzielen.

2.2. DS-GVO

Die DS-GVO enthält allgemein Vorgaben für die Verarbeitung personenbezogener Daten und spezifische Regelungen für bestimmte Datenkategorien, wozu insbesondere auch Gesundheitsdaten i. S. v. Art. 4 Nr. 15 DS-GVO zählen.

Die Verarbeitung von Daten i. S. d. DS-GVO umfasst gemäß Art. 4 Nr. 2 DS-GVO

> „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".

Die hier in Rede stehende Datenverknüpfung bzw. -weitergabe zwischen verschiedenen Verwendern stellt folglich – unter den Gesichtspunkten der Verknüpfung, Übermittlung bzw. Bereitstellung sowie Organisation und der Speicherung – im Ausgangspunkt eine an der DS-GVO zu messende Datenverarbeitung dar (vorbehaltlich der Einschlägigkeit der JI-Richtlinie, vgl. Art. 2 Abs. 2 lit. d) DS-GVO).

Die Verarbeitung personenbezogener Daten muss den in Art. 5 Abs. 1 DS-GVO niedergelegten Grundsätzen genügen. Hierzu zählen insbesondere die „**Rechtmäßigkeit**, Verarbeitung nach Treu und Glauben und Transparenz" der Datenverarbeitung (Art. 5 Abs. 1 lit. a), die „**Zweckbindung**" der Datenverarbeitung gemäß Art. 5 Abs. 1 lit. b)[17] sowie der Grundsatz der **Datenminimierung** gemäß Art. 5 Abs. 1 lit c). Nach dem Grundsatz der Zweckbindung müssen personenbezogene Daten für **im Vorhinein festgelegte**, eindeutige und legitime **Zwecke erhoben** werden und dürfen **nicht** in einer mit diesen Zwecken **unvereinbaren Weise weiterverarbeitet** werden. **Datenerhebung** meint die aktive und zielgerichtete Datenbeschaffung als Beginn eines Datenverarbeitungsvorgangs.[18] Das Prinzip der Datenminimierung gibt vor, dass personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen.

Die Anforderungen an die Rechtmäßigkeit der Verarbeitung personenbezogener Daten werden in Art. 6 ff. DS-GVO konkretisiert. Im Auftragskontext sind insbesondere Art. 6 DS-GVO und Art. 9 DS-GVO relevant. Art. 6 Abs. 1 DS-GVO regelt die allgemeinen Rechtmäßigkeitsanforderungen für die Verarbeitung personenbezogener Daten. Art. **6 Abs. 4 DS-GVO** enthält Anforderungen an

---

17 Siehe zur Zweckänderung unten, Ziff. 2.2.2.

18 Vgl. zur Definition der Erhebung: Bäcker, in: Kühling/Buchner, DS-GVO BDSG, 4. Aufl. 2024, Art. 13 DS-GVO Rn. 12, Datenerhebung lässt sich danach definieren als die „Handlung, mit der ein bestimmter Verantwortlicher auf bestimmte personenbezogene Daten erstmals zielgerichtet zugreift, um sie weiterzuverarbeiten". Siehe auch: Ernst, in: Paal/Pauly, DS-GVO BDSG, 4. Auflage 2026, Art. 4 DS-GVO Rn. 23; Reimer, in: Sydow/Marsch, DS-GVO | BDSG, 3. Aufl. 2022, Art. 4 DS-GVO Rn. 55.

eine **Zweckänderung** bei der Weiterverarbeitung bereits erhobener Daten. **Art. 9 DS-GVO** regelt spezielle Rechtmäßigkeitsanforderungen an die Verarbeitung bestimmter Datenkategorien, einschließlich **Gesundheitsdaten**. Art. 9 DS-GVO schließt die Anwendung von Art. 6 Abs. 1 DS-GVO nicht aus, sondern überlagert ihn (teilweise).[19] Nachfolgend werden zunächst die Anforderungen aus Art. 6 Abs. 1 DS-GVO und Art. 9 DS-GVO skizziert (Ziff.2.2.1.), bevor auf die Frage der Zweckänderung und dabei insbesondere auf Art. 6 Abs. 4 DS-GVO eingegangen wird (Ziff. 2.2.2.).

2.2.1. Art. 6 Abs. 1 und Art. 9 DS-GVO

Nach Art. 6 Abs. 1 DS-GVO ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn mindestens eine der in Art. 6 Abs. 1 UAbs. 1 lit. a) – f) DS-GVO abschließend[20] aufgezählten Grundlagen für die Datenverarbeitung vorliegt. Dies sind

- die Einwilligung der betroffenen Person (lit. a)),
- die Vertragserfüllung auf Anfrage der betroffenen Person (lit. b)),
- die Erfüllung einer rechtlichen Verpflichtung (lit. c)),
- der Schutz lebenswichtiger Interessen der betroffenen oder einer anderen Person (lit. d)),
- die Wahrnehmung einer Aufgabe im öffentlichen Interesse bzw. in Ausübung öffentlicher Gewalt (lit. e)), sowie
- die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Datenschutzinteressen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (lit. f)). Diese Verarbeitungsgrundlage gilt nach Art. 6 Abs. 1 UAbs. 2 DS-GVO nicht für Behörden.

Diese Anforderungen werden in **Art. 9 DS-GVO** in Bezug auf bestimmte Datenkategorien (sogenannte sensible Daten) konkretisiert bzw. strenger ausgestaltet.[21] Art. 9 Abs. 1 DS-GVO unterwirft diese Daten einem grundsätzlichen **Verarbeitungsverbot**:

---

19 Zum Verhältnis der beiden Vorschriften siehe Albers/Veit, in: BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg, 57. Edition, Stand: 1.8.2026, Art. 9 DS-GVO Rn. 11 sowie Weichert, in: Kühling/Buchner, DS-GVO BDSG, 4. Aufl. 2024, Art. 9 DS-GVO Rn. 4.

20 EuGH, Urteil vom 11. November 2020, Rs. C-61/19, Orange România SA, Rn. 34; EuGH, Urteil vom 22. Juni 2021, Rs. C-439/19, Latvijas Republikas Saeima (Points de pénalité), Rn. 99; EuGH, Urteil vom 8. Dezember 2022, Rs. C-180/21, Rn. 83; m. w. N. aus der Rspr.: Albers/Veit, in: BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg, 57. Edition, Stand: 1.8.2026, Art. 6 DS-GVO Rn. 22.

21 Weichert, in: Kühling/Buchner, DS-GVO BDSG, 4. Aufl. 2024, Art. 9 DS-GVO Rn. 4.

> „[…] **die Verarbeitung von** genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, **Gesundheitsdaten** oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person **ist untersagt**.“[22]

Art. 9 Abs. 2 DS-GVO sieht zehn Ausnahmen von diesem grundsätzlichen Verarbeitungsverbot vor. Bei einer Verarbeitung von Gesundheitsdaten zur Verbrechensbekämpfung erscheinen prima facie Art. 9 Abs. 2 lit. c) und g) DS-GVO von Bedeutung.[23]

2.2.1.1. Art. 9 Abs. 2 lit. c) DS-GVO

Gemäß Art. 9 Abs. 2 lit. c) DS-GVO gilt das Verarbeitungsverbot nicht für den Fall, dass

> „die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich [ist] und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande [ist], ihre Einwilligung zu geben“.

Art. 9 Abs. 2 lit. c) DS-GVO verengt den Rechtmäßigkeitstatbestand des Art. 6 Abs. 1 UAbs. 1 lit. d) DS-GVO, dem Art. 9 Abs. 2 lit. c) DS-GVO ansonsten in Bezug auf die Verarbeitung sensibler Daten entspricht.[24] Die Datenverarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person wird der weiteren zwingenden Voraussetzung unterworfen, dass die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben.[25] Die Norm zielt auf Einzelfall-Notsituationen ab.[26]

Unter Berücksichtigung dieser Voraussetzungen dürfte Art. 9 Abs. 1 lit. c) DS-GVO als Grundlage für das auftragsgegenständliche Vorhaben ausscheiden. Denn dieses stellt erkennbar nicht auf die fehlende Einwilligungsfähigkeit der betroffenen Person ab und dürfte einzelfallunabhängig, jedenfalls aber in einer Vielzahl von Fällen zur Anwendung kommen, um ein verstetigtes Datencluster bzw. einen systematischen Datenaustausch zum Zweck der Verbrechensbekämpfung zu schaffen.

---

22 Hervorhebungen und Auslassungen durch Verf.

23 Eine weitere spezifische Regelung in Bezug auf Gesundheitsdaten enthält Art. 9 Abs. 4 DS-GVO, der es den Mitgliedstaaten erlaubt, zusätzliche Bedingungen, einschließlich Beschränkungen, einzuführen oder aufrechtzuerhalten, soweit die Verarbeitung von Gesundheitsdaten betroffen ist. Aufgrund des klaren Wortlauts der Vorschrift erscheint es fernliegend, dass diese den Mitgliedstaaten erlauben könnte, die Rechtmäßigkeitsanforderungen an die Verarbeitung sensibler Daten abzusenken (vgl. dazu Albers/Veit, in: BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg, 57. Edition, Stand: 1.8.2026, Art. 9 DS-GVO Rn. 110).

24 Albers/Veit, in: BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg, 57. Edition, Stand: 1.8.2026, Art. 9 DS-GVO Rn. 66.

25 Albers/Veit, in: BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg, 57. Edition, Stand: 1.8.2026, Art. 9 DS-GVO Rn. 67.

26 Vgl. nur Weichert, in: Kühling/Buchner, DS-GVO BDSG, 4. Aufl. 2024, Art. 9 DS-GVO Rn. 62 f.

2.2.1.2. Art. 9 Abs. 2 lit. g) DS-GVO

Art. 9 Abs. 2 lit. g) DS-GVO enthält eine Ausnahme für den Fall, dass

> „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, aus Gründen eines **erheblichen öffentlichen Interesses** erforderlich [ist]“.[27]

Art. 9 Abs. 2 lit. g) DS-GVO sieht folglich eine Ausnahme vom Verbot der Verarbeitung sensibler Daten in den Fällen vor, in denen die Verarbeitung auf der Grundlage des Unionsrechts oder des **Rechts eines Mitgliedstaats** aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist. Die Bestimmung normiert eine **Öffnungsklausel** für mitgliedstaatliche Regelungen, sofern diese ein erhebliches öffentliches Interesse verfolgen und weitere Anforderungen erfüllen.[28] Die Norm geht über die Anforderungen aus Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO hinaus. Da der Auftragsgegenstand die Schaffung eines entsprechenden Regimes im nationalen Recht zum Gegenstand hat, werden diese Anforderungen nachfolgend überblicksartig skizziert.[29]

2.2.1.2.1. Erhebliches öffentliches Interesse

Zunächst muss die gesetzliche Ausnahme vom Verbot der Verarbeitung sensibler Daten „aus Gründen eines **erheblichen öffentlichen Interesses**“ erfolgen (anders als bei sonstigen Datenkategorien, bei denen nach Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO ein öffentliches Interesse ausreicht). Öffentliches Interesse meint, dass die jeweilige Regelung der Allgemeinheit als solcher und nicht einzelnen Partikular- bzw. Privatinteressen dient.[30] „Ein „erhebliches“ Interesse liegt nur vor, wenn es um besonders schützenswerte Interessen des Gemeinwohls geht, deren Durchsetzung gegenüber dem Persönlichkeitsrecht des Betroffenen Vorrang genießt.[31] Damit sind Maßnahmen ausgeschlossen, die zwar der Allgemeinheit dienen, für diese aber nicht so gewichtig sind, dass sie ohne die in Rede stehende Maßnahme ernsthaft beeinträchtigt wäre.[32] Im **Gefahrenabwehrrecht** ist dem Erfordernis nicht bereits bei einer Gefahr für ein beliebiges Rechtsgut genügt, sondern erst bei Gefahren für **hochrangige, besonders schützenswerte Rechtsgüter**, die durch den

---

27 Herv. hinzugefügt.

28 Frenzel, in: Paal/Pauly, DS-GVO BDSG, 4. Aufl. 2026, Art. 9 DS-GVO Rn. 38.

29 Auf die Frage, ob einzelne Datenverarbeitungen auch unmittelbar auf Art. 9 Abs. 2 lit. g) DS-GVO gestützt werden können, wird vorliegend aufgrund des fehlenden Bezugs zur Auftragsfrage, welche auf einen verstetigten Datenabgleich abzielt, nicht näher eingegangen. Nach einer Literaturauffassung sei der Rechtsprechung des EuGH eine solche Befugnis anzunehmen, siehe Schiff, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl. 2024, Art. 9 DS-GVO Rn. 52 unter Verweis auf EuGH, Urteil vom 24. September 2019, Rs. C-136/17, GC u.a. (Auslistung sensibler Daten), Rn. 66.

30 Schiff, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl. 2024, Art. 9 DS-GVO Rn. 53.

31 Dalby, in: Spindler/Schuster/Kaesling, Recht der elektronischen Medien, 5. Aufl. 2026, Art. 9 DS-GVO Rn. 16.

32 Schiff, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl. 2024, Art. 9 DS-GVO Rn. 53.

Gesetzgeber **hinreichend konkret benannt** werden müssen.[33] Dem Europäischen Gerichtshof (EuGH) zufolge bedarf insbesondere eine anlasslose, vom Verhalten der betroffenen Person unabhängige Übermittlung sensibler Daten einer besonderen Rechtfertigung. Diese muss präzise und besonders fundiert sein, wobei ein Rekurs auf den Schutz der öffentlichen Sicherheit vor Terrorismus und grenzübergreifender schwerer Kriminalität für sich genommen nicht ausreicht.[34] Die **Abwehr von Gefahren für Leib und Leben**, die sonst zu **unumkehrbaren Schäden** führen würden, dürfte in der Regel unter den Begriff des erheblichen öffentlichen Interesses fallen.[35]Auch eine effektive **Ahndung von Straftaten** dürfte grundsätzlich als erhebliches öffentliches Interesse einzuordnen sein, wobei die Verarbeitung jedoch auch im **Einzelfall verhältnismäßig** sein muss, sodass Bagatellkriminalität oder Delikte von untergeordneter Bedeutung von vornherein nicht dem Erfordernis des erheblichen öffentlichen Interesses genügen.[36]

2.2.1.2.2. Wesensgehaltgarantie und Verhältnismäßigkeit

Darüber hinaus verlangt Art. 9 Abs. 2 lit. g) DS-GVO, dass die Rechtsgrundlage in einem **angemessenen Verhältnis zum verfolgten Ziel** (Verhältnismäßigkeit) steht, den **Wesensgehalt des Rechts auf Datenschutz** wahrt und **angemessene und spezifische Maßnahmen** zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht.

Die Wahrung des **Wesensgehalts des Rechts auf Datenschutz** bezieht sich insbesondere auf Art. 7 (Privatsphäre) und Art. 8 (Datenschutz i. e. S.) GRCh. Nach der Rechtsprechung des EuGH stellt diese Wesensgehaltsgarantie eine eigenständige Eingriffsschranke dar.[37] Sie verbietet Eingriffe, die den Kernbereich des betreffenden Grundrechts dergestalt aushöhlen, dass es zur „leeren Hülle“ wird.[38] Nach der EuGH-Rechtsprechung verletzt eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt von Art. 7 GRCh.[39]

---

33 Schiff, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl. 2024, Art. 9 DS-GVO Rn. 55.

34 EuGH, Gutachten v. 26. Juli 2017, Gutachten 1/15 (PNR-Abkommen), Rn. 165. Demnach ist die anlasslose Übermittlung von sensiblen Fluggastdaten an Drittstaaten mit den Art. 7, 8, 21 GRCh unvereinbar.

35 Frenzel, in: Paal/Pauly, DS-GVO BDSG, 4. Aufl. 2026, Art. 9 DS-GVO Rn. 39.

36 Unter Rekurs auf Art. 8 Abs. 2 EMRK: Schiff, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl. 2024, Art. 9 DS-GVO Rn. 55. In seinem Urteil zur Vorratsdatenspeicherung vom 8. April 2014, verb-Rs. C-293/12 und C-594/12, Digital Rights Ireland u. a., hat der EuGH die Bekämpfung des internationalen Terrorismus sowie die Bekämpfung schwerer Kriminalität zur Gewährleistung der öffentlichen Sicherheit jedenfalls als „dem Gemeinwohl dienende“ Zielsetzungen eingestuft.

37 Jarass, in: Jarass, Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 52 Rn. 28 unter Verweis auf EuGH, Urteile vom 22. Januar 2013, Rs. C-283/1, Sky Österreich, Rn.48 ff. sowie vom 8. April 2014, verb. Rs. C-293/12 und C-594/12, Digital Rights Ireland u. a., Rn. 39 f., 45 ff.

38 Jarass, in: Jarass, Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 52 Rn. 28; Schiff, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl. 2024, Art. 9 DS-GVO Rn. 56.

39 EuGH, Urteil vom 6. Oktober 2015, Rs. C-362/14, Schrems, Rn. 94 unter Verweis auf EuGH, Urteil vom 8. April 2014, verb. Rs. C-293/12 und C-594/12, Digital Rights Ireland u. a., Rn. 39.



Das Kernstück der Vorgaben aus Art. 9 Abs. 2 lit. g) DS-GVO bildet der Grundsatz der **Verhältnismäßigkeit**, dem jede Verarbeitung sensibler Daten im Einzelfall (und somit auch die jeweilige Eingriffsnorm in abstrakter Hinsicht) zu genügen hat.[40] Die Maßnahme muss demnach ein erhebliches öffentliches Interesse (s. o.) zum Ziel haben und zu dessen Förderung **geeignet** sein. Sie muss zudem **erforderlich** sein, was bedeutet, dass kein gleich geeignetes, milderes Mittel zur Verfügung steht. Zudem muss der Grundrechtseingriff einem **angemessenen Verhältnis** zum damit verfolgten Ziel stehen.[41]

Für die **Geeignetheit** verlangt der EuGH, dass Rechtsvorschriften über die Datenverarbeitung objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Die vom nationalen Gesetzgeber ausgewählten zu verarbeitenden Gesundheitsdaten müssten also bei objektiver Beurteilung geeignet sein, zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beizutragen.[42] Im Hinblick die prüfungsgegenständliche verstetigte Verknüpfung von Gesundheitsdaten wäre dieser Zusammenhang anhand der konkret in Rede stehenden Daten darzulegen.

Eine Verarbeitung sensibler Daten ist nach der Rechtsprechung des EuGH **erforderlich**, wenn das mit der betreffenden Datenverarbeitung verfolgte Ziel nicht in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden kann, die weniger stark in Art. 7, Art. 8 GRCh eingreifen.[43] Nach ständiger Rechtsprechung des EuGH verlangt der Schutz des Grundrechts auf Achtung des Privatlebens aus Art. 7 GRCh, dass sich Einschränkungen **auf das absolut Notwendige**

40 Grundlegend zur Verhältnismäßigkeitsprüfung im Datenverarbeitungskontext: EuGH, Urteil vom 21. Juni 2022, Rs. C-817/19, Ligue des droits humains; vgl. Schiff, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl. 2024, Art. 9 DS-GVO Rn. 57.

41 Vgl. Jarass, in: Jarass, Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 8 GRCh, Rn. 17; Kingreen, in: Calliess/Ruffert, EUV/AEUV, 6. Aufl. 2022, Art. 52 GRCh, Rn. 65 ff., jeweils m. N. aus der Rechtsprechung.

42 EuGH, Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 55 m. w. N.

43 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 126 unter Verweis auf EuGH, Urteil vom 1. August 2022, Rs. C-184/20, Vyriausioji tarnybínes etikos komisija, Rn. 85 und die dort angeführte Rechtsprechung.

beschränken.[44] Dies ist durch bestimmte Garantien sicherzustellen.[45] Die Anforderungen an die Erforderlichkeitsprüfung sind nach der Rechtsprechung des EuGH umso strenger, je schwerer der jeweilige Eingriff in Art. 7, Art. 8 GRCh wiegt. Bei der Prüfung der Erforderlichkeit eines Eingriffs kommt es folglich entscheidend auf die **Eingriffsschwere** an.[46] Bei der Ermittlung der Eingriffsintensität durch eine Datenübermittlung bezieht der EuGH insbesondere ein, ob diese systematisch, kontinuierlich und automatisch erfolgt, welche Informationstiefe die Daten vermitteln (insbesondere, ob **sensible Daten** betroffen sind), welche Verwendung beabsichtigt ist und wie lange die Daten gespeichert werden.[47] In Bezug auf die Verarbeitung besonderer Datenkategorien i. S. v. Art. 9 Abs. 1 DS-GVO hat der EuGH ausgeführt, dass diese aufgrund der **Sensibilität** dieser Daten einen **besonders schweren Eingriff** darstellen kann.[48] Besonders eingriffsintensiv sind grundsätzlich auch automatisierte Datenverarbeitungen.[49] So hat der EuGH eine systematisch-automatisierte Übermittlung von Fluggastdaten als „fraglos schwerwiegenden" Eingriff bewertet und dabei insbesondere darauf abgestellt, dass sensible Daten über die Fluggäste enthalten sein können.[50] Im Falle der Verarbeitung sensibler Daten muss sich der für die Verarbeitung Verantwortliche daher insbesondere vergewissern, **dass das verfolgte Ziel nicht durch die Heranziehung anderer (nicht sensibler) Datenkategorien erreicht werden kann**.[51] Von Bedeutung für die sicherheits- und polizeirechtliche Datenverarbeitung sind im Rahmen der Erforderlichkeitsprüfung vor allem die Grundsätze des Vorrangs der **unmittelbaren vor der mittelbaren** sowie des Vorrangs der **offenen vor der verdeckten** Datenerhebung.[52] Insbesondere der letztere Grundsatz ist nach

---

44 EuGH, Gutachten v. 26. Juli 2017, Gutachten 1/15 (PNR-Abkommen), unter Verweis auf EuGH, Urteile vom 16. Dezember 2008, Rs. C-73/07, Satakunnan Markkinapörssi und Satamedia, Rn. 56, vom 8. April 2014, verb. Rs. C-293/12 und C-594/12, Digital Rights Ireland u. a., Rn. 51 und 52; vom 6. Oktober 2015, Rs. C-362/14, Schrems, Rn. 92; und vom 21. Dezember 2016, verb. Rs. C-203/15 und C-698/15, Tele2 Sverige und Watson u. a., Rn. 96 und 103.

45 EuGH, Urteil vom 21. Juni 2022, Rs. C-817/19, Ligue des droits humains, Rn. 117.

46 EuGH, Urteil vom 21. Juni 2022, Rs. C-817/19, Ligue des droits humains, Rn. 116 unter Verweis auf EuGH, Urteile vom 2. Oktober 2018, Rs. C-207/16, Ministerio Fiscal, Rn. 55 und die dort angeführte Rechtsprechung, sowie vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána u. a., Rn. 53 und die dort angeführte Rechtsprechung.

47 EuGH, Urteil vom 1. August 2022, Rs. C-184/20, Vyriausioji tarnybinės etikos komisija, Rn. 99; EuGH, Urteil vom 21. Juni 2022, Rs. C-817/19, Ligue des droits humains, Rn. 98 ff.

48 EuGH, Urteil vom 24. September 2019, Rs. C-136/17, GC u.a. (Auslistung sensibler Daten), Rn. 67.

49 EuGH, Urteil vom 21. Juni 2022, Rs. C-817/19, Ligue des droits humains, Rn. 117 unter Verweis auf EuGH, Gutachten v. 26. Juli 2017, Gutachten 1/15 (PNR-Abkommen), Rn. 141, und Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 132 und die dort angeführte Rechtsprechung

50 EuGH, Urteil vom 21. Juni 2022, Rs. C-817/19, Ligue des droits humains, Rn. 100, 111.

51 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 126.

52 Kingreen, in: Calliess/Ruffert, EUV/AEUV, 6. Aufl. 2022, Art. 8 GRCh Rn. 17

Auffassung in der Literatur bei der Verarbeitung von sensiblen Daten aufgrund deren besonders schutzwürdigen Charakters von besonderer Relevanz.[53]

Im Rahmen der **Angemessenheitsprüfung** ist die Eingriffsschwere gegen das Gewicht der durch den Eingriff verfolgten Ziele abzuwägen („Zweck-Mittel-Relation"), wobei insbesondere die Bedeutung der jeweiligen Rechtsposition in der EU in den Blick zu nehmen ist.[54] Dabei kommt es auch darauf an, welche Rechte und Freiheiten anderer durch die Maßnahmen geschützt werden. Bei Maßnahmen wie der hiesigen kommen insofern insbesondere das Recht auf Sicherheit aus Art. 6 GRCh sowie – im Zusammenhang mit dem Opferschutz bei der Kriminalitätsbekämpfung – staatliche Schutzverpflichtungen aus Art. 7 GRCh sowie aus Art. 3, 4 GRCh hinsichtlich des Schutzes der körperlichen und geistigen Unversehrtheit in Betracht.[55]

Soweit ersichtlich hat der EuGH eine spezifisch Gesundheitsdaten betreffende Datenclusterung bzw. -weitergabe zum Zwecke der Verbrechensbekämpfung bislang nicht am Maßstab des Art. 9 DS-GVO auf ihre Verhältnismäßigkeit hin geprüft.[56] Gleichwohl befand er ein Abkommen zwischen einem Mitgliedstaat und einem Drittstaat über Fluggastdaten für unverhältnismäßig, welches deren Übermittlung pauschal gestattet, also keine Differenzierung hinsichtlich besonders sensibler Daten vornimmt.[57] Auch eine Offenlegung von u. a. namensbezogenen Daten über den Ehegatten, Lebensgefährten oder Partner der betroffenen Person oder über ihr nahestehende oder bekannte Personen mit dem Zweck der Korruptionsbekämpfung erachtete der EuGH für unangemessen.[58]

2.2.1.2.3. Angemessene und spezifische Schutzmaßnahmen

Die mitgliedstaatliche Regelung müsste schließlich gemäß Art. 9 Abs. 2 lit. g) DS-GVO **angemessene und spezifische Maßnahmen** zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsehen. Hierbei handelt es sich um eine im Einzelfall ausfüllungsbedürftige Anforderung, da betreffende spezifische Maßnahmen und deren Angemessenheit vom Verarbeitungskontext, Verarbeitungsverfahren und -techniken und der kontextspezifischen Schutzbedürftigkeit der betroffenen Person abhängen.[59] Jedenfalls dürfte hierunter ein Aufklärungserfordernis gegenüber der betroffenen Person bezüglich der Verarbeitung sowie deren Anlass und Zweck fallen, damit diese eigenständig und informiert entscheiden kann, ob und inwiefern sie gegen die Verarbeitung

---

53 Schiff, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl. 2024, Art. 9 DS-GVO Rn. 58.

54 EuGH, Urteil vom 1. August 2022, Rs. C-184/20, Vyriausioji tarnybinės etikos komisija, Rn. 106 ff.

55 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 63 ff.; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 48 f. m. w. N.

56 Auf die Rechtssache C-205/21 wird unter Ziff. 2.3.2. näher eingegangen, da dieser eine Prüfung am Maßstab des Art. 10 JI-RL zugrunde liegt, der ebenfalls die Verarbeitung sensibler Daten zum Gegenstand hat.

57 EuGH, Gutachten v. 26. Juli 2017, Gutachten 1/15 (PNR-Abkommen), Rn. 164 ff.

58 EuGH, Urteil vom 1. August 2022, Rs. C-184/20, Vyriausioji tarnybinės etikos komisija, Rn. 116.

59 Albers/Veit, in: BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg, 57. Edition, Stand: 1.8.2026, Art. 9 DS-GVO Rn. 86.

vorgehen will.[60] Daraus dürfte zudem das Erfordernis der Einrichtung von **Instrumenten folgen**, mittels derer die betroffene Person eine Verarbeitung beim Verantwortlichen rügen kann.[61]

2.2.1.3. Folgerungen im Auftragskontext

Im Hinblick auf den Auftragsgegenstand lässt sich festhalten, dass Art. 9 Abs. 1 DS-GVO eine Verarbeitung von Gesundheitsdaten im Grundsatz verbietet, den Mitgliedstaaten aber gemäß Art. 9 Abs. 2 lit. g) DS-GVO die Möglichkeit zur Schaffung entsprechender Ausnahmetatbestände eröffnet. Diese mitgliedstaatlichen Regelungen werden gleichwohl engen Grenzen unterworfen und müssen insbesondere dem Grundsatz der Verhältnismäßigkeit genügen. Hierbei wäre zu berücksichtigen, dass die Verarbeitung sensibler Daten – wie Gesundheitsdaten – in der Regel einen besonders schwerwiegenden Eingriff in Art. 7 und 8 GRCh darstellt, was in besonderem Maße bei automatisierten Abgleichen gelten dürfte. Daher dürfte unter Einbeziehung der Rechtsprechung des EuGH ein besonders strenger Maßstab anzulegen sein. Die Verhältnismäßigkeit bzw. Vereinbarkeit mit Art. 9 Abs. 2 lit. g) DS-GVO einer solchen Vorschrift hinge gleichwohl entscheidend vom Verarbeitungskontext, den Verarbeitungsverfahren und -techniken und der kontextspezifischen Schutzbedürftigkeit der betroffenen Personen und somit von ihrer konkreten Ausgestaltung im Einzelfall ab.

2.2.2. Zweckänderung

Nach dem Auftrag zugrunde liegenden Szenario sollen **bereits für medizinische Zwecke erhobene** Gesundheitsdaten für andere Zwecke (insbesondere Verbrechensbekämpfung) **weiterverarbeitet** werden. Es geht darum, **keine neue Erhebung** dieser Daten durchzuführen.

Verarbeitungen personenbezogener Daten unterliegen gemäß Art. 5 Abs. 1 lit. b) DS-GVO dem Gebot der **Zweckbindung**. Demnach müssen personenbezogene Daten für im Vorhinein[62] **festgelegte**, eindeutige und legitime Zwecke erhoben werden. Eine Weiterverarbeitung personenbezogener Daten zu einem anderen als dem Erhebungszweck ist nur gestattet, sofern der neue Zweck mit dem Erhebungszweck vereinbar ist. Die Rechtmäßigkeit einer solchen Weiterverarbeitung richtet sich im Einzelnen nach **Art. 6 Abs. 4 DS-GVO**.[63] Dieser sieht vor:

> „Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder **auf einer Rechtsvorschrift** der Union oder **der Mitgliedstaaten,** die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche – um festzustellen,

60 Schiff, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl. 2024, Art. 9 DS-GVO Rn. 59.

61 Unter Rekurs auf die Instrumente der DS-GVO, insbesondere das Beschwerderecht nach Art. 77 und den gerichtlichen Rechtsbehelf nach Art. 79 DS-GVO: Schiff, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl. 2024, Art. 9 DS-GVO Rn. 59.

62 Vgl. EuGH, Urteil vom 24. Februar 2022 Rs. C-175/20, Valsts ieņēmumu dienests, Rn. 64.

63 EuGH, Urteil vom 20. Oktober 2022, Rs. C-77/21, Digi, Rn. 35.

ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, **vereinbar ist** – unter anderem

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,

c) die Art der personenbezogenen Daten, insbesondere **ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet** werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,

d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,

e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.“[64]

Weiterverarbeitungen sind somit nur gestattet, wenn sie (1.) für bestimmte privilegierte Zwecke i. S. v. Art. 5 Abs. 1 lit. b) Hs. 2 DS-GVO erfolgen,[65] (2.) auf einer Einwilligung der betroffenen Person beruhen, (3.) auf Grund des in Art. 6 Abs. 4 DS-GVO vorgegebenen Bewertungsvorgans mit dem Erhebungszweck vereinbar sind, oder (4.) auf einer **mitgliedstaatlichen Rechtsvorschrift** beruhen, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz eines der in Art. 23 Abs. 1 DS-GVO aufgeführten Ziele darstellt. Art. 23 DS-GVO nennt u. a. **Maßnahmen zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten**.[66]

Nachfolgend werden zunächst die an eine solche nationale Regelung zu stellenden Anforderungen aus Art. 6 Abs. 4 DS-GVO skizziert (Ziff. 2.2.2.1.). Anschließend wird das Verhältnis zwischen Art. 9 DS-GVO und Art. 6 Abs. 4 DS-GVO beleuchtet, um Aufschluss zu der Frage der Zweckänderung bzw. Zweckbindung bei sensiblen Daten zu geben (Ziff. 2.2.2.2.).

64 Hervorh. durch Verf.

65 Gemäß Art. 5 Abs. 1 lit. b) Hs. 2 DS-GVO sind Weiterverarbeitungen für Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke (privilegierte Zwecke) vom grundsätzlichen Zweckbindungsgebot ausgenommen.

66 Die Frage, ob es sich bei Art. 6 Abs. 4 DS-GVO um eine eigenständige Öffnungsklausel handelt oder (allein oder ergänzend) Art. 23 DS-GVO heranzuziehen ist, ist in der Literatur umstritten, m. w. N. Taeger, in: Taeger/Gabel, DSGVO – BDSG – TDDDG, 5. Aufl. 2026, Art. 6 DS-GVO Rn. 201. Der Streit wird hier offengelassen und Art. 23 Abs. 1 DS-GVO als Maßstab herangezogen, da die Ansichten im Auftragskontext zum selben Ergebnis kommen dürften.

2.2.2.1. Anforderungen an eine mitgliedstaatliche Rechtsgrundlage

Die mitgliedstaatliche Rechtsvorschrift muss gemäß Art. 6 Abs. 4 DS-GVO „in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Art. 23 Abs. 1 DS-GVO genannten Ziele“ darstellen.

Konkreter Maßstab für eine entsprechende mitgliedstaatliche Vorschrift ist Art. 23 Abs. 1 DS-GVO,[67] welcher sowohl (abschließend) taugliche Zwecke auflistet und wonach die Vorschrift den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zur Verfolgung des ausgewiesenen Zwecks darstellen muss.

Hinsichtlich der erfassten Zwecke bezieht Art. 23 Abs. 1 lit. d) DS-GVO ausdrücklich „die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“ in den Kanon der legitimen Ziele ein. Die hier in Rede stehende Zielsetzung der Verbrechensbekämpfung dürfte folglich grundsätzlich darunterfallen.

Hinsichtlich der Erfordernisse der Wesensgehaltsgarantie und der Verhältnismäßigkeit gelten die Ausführungen unter Ziff. 2.2.1.2.2. Danach sind insbesondere die Eignung der Zweckänderungserlaubnis zur Zielförderung in den Blick zu nehmen und die Eingriffsintensität im Einzelfall gegen das verfolgte Ziel der Verbrechensbekämpfung abzuwägen. Dies könnte allein anhand eines hinreichend konkreten Maßnahmenkonzepts ggf. unter Einbeziehung empirischer Daten und abschließend allein durch den EuGH erfolgen.

2.2.2.2. Zweckänderung hinsichtlich sensibler Daten

Art. 9 DS-GVO selbst enthält keine Aussage dazu, ob und unter welchen Voraussetzungen die Weiterverarbeitung bereits erhobener sensibler Daten zu geänderten Zwecken rechtmäßig ist. Diese Frage ist in der Literatur umstritten. Teilweise wird vertreten, die Rechtmäßigkeit richte sich allein nach Art. 9 DS-GVO. Danach bedürfe es einer erneuten Datenerhebung mit einem festgelegten, eindeutigen und legitimen Zweck (Art. 5 DS-GVO). Die zweckändernde Weiterverarbeitung sei ausgeschlossen.[68] Dem wird entgegengehalten, dass Art. 6 Abs. 4 lit. c) DS-GVO ausdrücklich besondere Kategorien personenbezogener Daten i. S. v. Art. 9 DS-GVO benenne und damit bereits tatbestandlich voraussetze, dass eine auch sensible Daten betreffende zweckändernde Verarbeitung grundsätzlich zulässig sein solle.[69] Dafür spreche auch Erwägungsgrund (ErwG) 51 S. 5 DS-GVO, da dieser ausdrücklich von der Anwendbarkeit der allgemeinen

---

67 Culik/Döpke: Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen, ZD 2017, 226, 229.

68 Schiff, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl. 2024, Art. 9 DS-GVO Rn. 12 unter Verweis auf ErwG 51, Satz 4.

69 Schulz/Petersen, in: Gola/Heckmann/Rost, DS-GVO BDSG, 4. Aufl. 2026, Art. 9 DS-GVO Rn. 7; Albers/Veit, in: BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg, 57. Edition, Stand: 1.8.2026, Art. 9 DS-GVO Rn. 12.

Grundsätze und Rechtmäßigkeitsanforderungen ausgehe..[70] Nach wohl überwiegender Literaturauffassung ist eine zweckändernde Weiterverarbeitung sensibler Daten daher möglich, sofern zum einen die **Voraussetzung von Art. 6 Abs. 4 DS-GVO** vorliegen und zum anderen eine **Rechtsgrundlage für die (Weiter-)Verarbeitung i. S. v. Art. 9 Abs. 2 DS-GVO** gegeben ist.[71]

Im Hinblick auf den Auftragskontext lässt sich daher festhalten, dass eine mitgliedstaatliche Erlaubnisnorm hinsichtlich einer zweckändernden Weiterverarbeitung von Gesundheitsdaten über Art. 6 Abs. 4 DS-GVO hinaus den unter Ziff. 2.2.1.2. dargestellten Anforderungen aus Art. 9 Abs. 2 lit. g) DS-GVO Rechnung tragen muss.[72]

2.2.3. Zwischenergebnis zur DS-GVO

Die hier zur Überprüfung gestellte Weiterverwendung von Gesundheitsdaten müsste insbesondere den Anforderungen aus Art. 6 Abs. 4 und Art. 9 DS-GVO genügen, sofern der Anwendungsbereich der EU-Datenschutzgrundverordnung für die jeweilige Verarbeitung eröffnet ist (s. Ziff. 2.1. zur Abgrenzung zur JI-Richtlinie). Art. 9 DS-GVO sieht ein grundsätzliches Verarbeitungsverbot hinsichtlich sensibler Daten vor, eröffnet den Mitgliedstaaten in Art. 9 Abs. 2 lit. g) DS-GVO aber die Möglichkeit, Rechtsgrundlagen für die rechtmäßige Verarbeitung sensibler Datenkategorien zu schaffen. Solche nationalen Regelungen müssen einem erheblichen öffentlichen Interesse dienen und dem Grundsatz der Verhältnismäßigkeit genügen. Art. 6 Abs. 4 DS-GVO normiert zusätzliche Anforderungen an die zweckändernde Weiterverarbeitung bereits erhobener Daten. Eine konkrete Prüfung der Unionsrechtskonformität wäre nur anhand eines hinreichend konkreten Maßnahmenentwurfs möglich, wobei dem EuGH die letztverbindliche Auslegung des EU-Rechts obliegt.

2.3. JI-RL

Soweit die datenverarbeitende Stelle als zuständige Behörde zu Zwecken der Straftatenverhütung (oder -verfolgung) tätig wird, findet die JI-RL Anwendung (s. o., Ziff. 2.1.). Im Auftragskontext dürfte dies in der Regel auf die datenempfangende Stelle zutreffen. Nachfolgend werden die sich aus der JI-RL im Auftragskontext ergebenden Anforderungen skizziert.

2.3.1. Art. 4 ff. JI-RL

Die JI-RL enthält mit der DS-GVO vergleichbare Vorgaben. Als Richtlinie i. S. v. Art. 288 Abs. 3 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) gilt sie – anders als die DS-GVO – aber nicht unmittelbar in den Mitgliedstaaten. Sie bedarf der Umsetzung in nationales Recht.

---

70 Schulz/Petersen, in: Gola/Heckmann/Rost, DS-GVO BDSG, 4. Aufl. 2026, Art. 9 DS-GVO Rn. 7.

71 Weichert, in: Kühling/Buchner, DS-GVO BDSG, 4. Aufl. 2024, Art. 9 DS-GVO Rn. 4a; Schulz/Petersen, in: Gola/Heckmann/Rost, DS-GVO BDSG, 4. Aufl. 2026, Art. 9 DS-GVO Rn. 7; Albers/Veit, in: BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg, 57. Edition, Stand: 1.8.2026, Art. 9 DS-GVO Rn. 12.

72 Dies entspricht dem Verständnis des deutschen Gesetzgebers, vgl. § 23 Abs. 2, § 24 Abs. 2 Bundesdatenschutzgesetz.

Art. 4 JI-RL normiert Datenschutzgrundsätze, die im Wesentlichen denen aus Art. 5 DS-GVO entsprechen. Dazu gehören u. a. die Rechtmäßigkeit, Zweckbindung und Datenminimierung.

Art. 4 Abs. 2 JI-RL stellt klar, dass Zweckänderungen der Verarbeitung von Daten, die für einen der Zwecke i. S. v. Art. 1 Abs. 1 JI-RL erhoben wurden (Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten etc.) und für einen anderen dieser Zwecke verarbeitet werden sollen, unter bestimmten Voraussetzungen erlaubt sind. Dies dürfte indes keine Relevanz für den Auftragskontext haben, da die betreffenden Daten gerade nicht zu den Zwecken der JI-RL erhoben werden. Dasselbe gilt für die Zweckänderungsregelung des Art. 9 Abs. 1 JI-RL, welcher die Verarbeitung von für Zwecke der JI-RL erhobenen Daten für Zwecke außerhalb der JI-RL regelt.

Art. 6 JI-RL ordnet an, dass die Mitgliedstaaten vorsehen, dass der Verantwortliche gegebenenfalls und so weit wie möglich zwischen den personenbezogenen Daten **verschiedener Kategorien betroffener Personen** klar **unterscheidet**. Dazu zählen Verdächtige (Art. 6 lit. a) JI-RL), Verurteilte (Art. 6 lit. b) JI-RL), Opfer einer Straftat (Art. 6 lit. c) JI-RL) sowie andere Parteien im Zusammenhang mit einer Straftat (bspw. Personen, die als Zeugen in Betracht kommen, die Hinweise zur Straftat geben können, oder die mit Verdächtigen oder Opfern in Verbindung stehen, Art. 6 lit. d) JI-RL) zählen.

Art. 8 JI-RL regelt die Rechtmäßigkeit der Verarbeitung. Art. 8 Abs. 1 JI-RL ordnet an, dass die Mitgliedstaaten vorsehen, dass die Verarbeitung nur dann rechtmäßig ist, wenn und soweit diese Verarbeitung für die **Erfüllung einer Aufgabe** erforderlich ist, die von der zuständigen Behörde zu den in Art. 1 Abs. 1 JI-RL genannten Zwecken wahrgenommenen wird, und auf Grundlage des Unionsrechts oder **des Rechts der Mitgliedstaaten** erfolgt. Art. 8 Abs. 2 JI-RL trifft Vorgaben hinsichtlich des mitgliedstaatlichen Rechts und sieht vor, dass im Recht der Mitgliedstaaten, das die Verarbeitung innerhalb des Anwendungsbereichs der JI-RL regelt, zumindest die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung angegeben werden.

2.3.2. Art. 10 JI-RL

Kernbestimmung im Auftragskontext ist Art. 10 JI-RL. Dieser stellt an die Verarbeitung sensibler Daten, zu denen auch Gesundheitsdaten gehören, besondere Voraussetzungen. Demnach ist die

> „Verarbeitung […] von […] **Gesundheitsdaten** nur erlaubt, wenn sie **unbedingt erforderlich ist** und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt und
>
> a) wenn sie nach dem Unionsrecht oder dem **Recht der Mitgliedstaaten zulässig** ist,
>
> b) der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dient oder

c) wenn sie sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat.“[73]

Der EuGH hat diese Vorgaben in der **Rechtssache C-205/21** konkretisiert. In diesem Fall wollte das vorlegende nationale Gericht wissen, ob ein nationales Gesetz den Rechtmäßigkeitsanforderungen der JI-RL genügt, das die **systematische Erhebung biometrischer und genetischer Daten** aller Personen, die einer vorsätzlichen Offizialstraftat beschuldigt werden, anordnet. Die nationale Regelung bezweckte die Registrierung dieser Personen, ohne die zuständige Behörde zu verpflichten, zu bestimmen und nachzuweisen, dass diese Erhebung für die Erreichung der **konkret verfolgten Ziele erforderlich** sei und dass die verfolgten Ziele nicht durch die Erhebung nur eines Teils der betreffenden Daten erreicht werden könnten.[74] Der Rechtssache C-205/21 lag folglich eine Regelung zur Datenverarbeitung zugrunde, die sich auf bereits beschuldigte Personen beschränkte und in Zusammenhang zu einer konkreten Straftat stand In der auftragsgegenständlichen Konstellation dürfte der Zusammenhang zur Verhütung bzw. Bekämpfung von Straftaten grundsätzlich schwerer herstellbar sein.

Der EuGH führte aus, dass Art. 10 JI-RL einen erhöhten Schutz gegen eine Verarbeitung solcher Daten gewährleisten soll, die aufgrund der besonderen Sensibilität des Verarbeitungskontexts erhebliche Risiken für durch die Art. 7 und 8 der GRCh garantierten Grundrechte und Grundfreiheiten bergen könnten.[75] Dass die Verarbeitung „**nur**“ dann erlaubt ist, „**wenn sie unbedingt erforderlich ist**“, verdeutliche, dass im Vergleich zur Verarbeitung nicht sensibler Datenkategorien verschärfte Anforderungen gelten.[76] Aus der Formulierung „nur, wenn sie unbedingt erforderlich ist“ folge, (1) dass lediglich eine Verarbeitung einer **begrenzten Zahl von Fällen** als erforderlich angesehen werden könne, dass (2) die **Erforderlichkeit besonders streng zu beurteilen** sei,[77] und dass (3) die Einhaltung des **Grundsatzes der Datenminimierung** besonders streng kontrolliert werden müsse.[78] Um eine Prüfung der unbedingten Erforderlichkeit zu ermöglichen, müssten die Zwecke der Verarbeitung biometrischer und genetischer Daten in einer gesetzlichen Bestimmung hinreichend genau und konkret definiert werden. Zu allgemeine Begriffe reichten nicht aus.[79]

---

73 Hervorh. durch Verf.

74 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 114.

75 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 116 unter Verweis auf ErwG 37 JI-RL sowie EuGH, Urteil vom 24. September 2019, Rs. C-136/17, GC u. a. (Auslistung sensibler Daten), Rn. 44.

76 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 117 ff.

77 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 118.

78 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 125.

79 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 124.

Die Erforderlichkeit sei im Grundsatz erfüllt, wenn das verfolgte Ziel nicht in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden könne, die weniger stark in die Grundrechte der betroffenen Personen, insbesondere in Art. 7, Art. 8 GRCh, eingreifen.[80] Insbesondere müsse sich der für die Verarbeitung Verantwortliche im Hinblick auf den erhöhten Schutz von Personen bei der Verarbeitung sensibler Daten vergewissern, **dass dieses Ziel nicht durch die Heranziehung anderer Datenkategorien erreicht werden könne**.[81]

Zweitens ergebe sich aus dem Kriterium der „unbedingten Erforderlichkeit" in Anbetracht der erheblichen Risiken, die mit einer Verarbeitung sensibler Daten im strafrechtlichen Kontext einhergingen, dass der Verarbeitungszweck eine **besondere Bedeutung** aufweisen müsse.[82] Diese Bedeutung könne u. a. anhand der **Art des verfolgten Ziels** beurteilt werden. So könne bspw. darauf rekurriert werden, dass die Verarbeitung einem konkreten Zweck diene, der mit der Verhütung von Straftaten oder einer Bedrohung der öffentlichen Sicherheit von einem **gewissen Schweregrad**, der Verfolgung solcher Straftaten oder dem Schutz vor einer solchen Bedrohung zusammenhänge. Es seien dabei stets **die besonderen Umstände** zu berücksichtigen, unter denen die Verarbeitung erfolge.

Nach Auffassung des EuGH verstoßen nationale Rechtsvorschriften, die die **systematische Erhebung biometrischer und genetischer Daten** aller Personen vorsehen, die einer vorsätzlichen Offizialstraftat beschuldigt werden, grundsätzlich gegen das Kriterium der unbedingten Erforderlichkeit gemäß Art. 10 JI-RL.[83] Solche Rechtsvorschriften könnten nämlich **unterschiedslos und allgemein** zur Erhebung biometrischer und genetischer Daten der meisten beschuldigten Personen führen, da der Begriff „vorsätzliche Offizialstraftat" besonders allgemein gehalten sei und auf eine große Zahl von Straftaten unabhängig von ihrer Art und Schwere angewendet werden könne.[84] Die allgemeine Beschränkung auf Verdächtige i. S. v. Art. 6 lit. a) JI-RL reiche nicht aus, um die Verarbeitung sensibler Datenkategorien im Hinblick auf die damit verfolgten Zwecke – unter Berücksichtigung der der damit verbundenen Eingriffe in Art. 7, Art. 8 GRCh – als unbedingt erforderlich anzusehen.[85] So könne es zum einen Fälle geben, in denen die Erhebung sowohl biometrischer als auch genetischer Daten für die Zwecke des laufenden Strafverfahrens

80 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 126 unter Verweis auf EUGH, Urteil vom 1. August 2022, Rs. C-184/20, Vyriausioji tarnybínes etikos komisija, Rn. 85 und die dort angeführte Rechtsprechung

81 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 126.

82 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 127

83 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 128

84 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 129

85 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 130

nicht konkret erforderlich sei.[86] Zum anderen könne die Wahrscheinlichkeit, dass die biometrischen und genetischen Daten einer beschuldigten Person im Rahmen anderer Verfahren als dem, in dessen Rahmen die Beschuldigung erfolgt ist, unbedingt erforderlich sind, **nur unter Berücksichtigung aller relevanten Faktoren** bestimmt werden, wie etwa **Art und Schwere der mutmaßlichen Straftat**, der sie beschuldigt wird, der **besonderen Umstände dieser Straftat**, des etwaigen **Zusammenhangs der Straftat mit anderen laufenden Verfahren**, der **Vorstrafen** oder des **individuellen Profils der betreffenden Person**.[87]

Es lässt sich daher festhalten, dass eine mitgliedstaatliche Vorschrift zur Verarbeitung sensibler Daten im strafrechtlichen Kontext grundsätzlich **nur dann den Anforderungen** des Art. 10 JI-RL genügen kann, wenn sie sicherstellt, dass die **Erforderlichkeit der Datenverarbeitung** stets im Hinblick auf den **jeweiligen Einzelfall** geprüft wird. Es erscheint eher fernliegend, dass eine Regelung zur systematischen Weiterverarbeitung von Gesundheitsdaten zur allgemeinen Verbrechensbekämpfung diesen Anforderungen gerecht würde, sofern sie unterschiedslos und allgemein auf einen breiten Personenkreis und (bestimmte) Erkrankungen rekurriert.

2.3.3. Folgerungen zur JI-RL im Auftragskontext

Ein mitgliedstaatlich vorgesehener zwischenbehördlicher Abgleich bzw. Austausch von Gesundheitsdaten zu Zwecken der Verbrechensbekämpfung könnte insbesondere an Art. 10 JI-RL zu messen sein. Nach der Rechtsprechung des EuGH wäre die unbedingte Erforderlichkeit im Rahmen des Art. 10 JI-RL streng zu beurteilen, da diese nur in einer begrenzten Zahl von Fällen bejaht werden könne. Insbesondere wäre zu prüfen, ob die Datenverarbeitung im Einzelfall erforderlich ist und nicht ebenso wirksam durch Rückgriff auf nicht sensible Daten erreicht werden kann. Daraus folgt nach der Rechtsprechung des EuGH, dass die unbedingte Erforderlichkeit anhand aller Umstände des jeweiligen Einzelfalls zu ermitteln ist. Eine Regelung, die die systematische Erhebung sensibler Daten von Beschuldigten vorsieht, ohne die zuständige Behörde zu verpflichten, die unbedingte Erforderlichkeit im Einzelfall zu prüfen und nachzuweisen, wird diesen Anforderungen dem EuGH zufolge nicht gerecht und verstößt daher gegen Art. 10 JI-RL. Dies dürfte **erst recht** für eine Regelung gelten, die sich **nicht auf Beschuldigte einer Straftat beschränkt**, sondern unterschiedslos und allgemein an das Merkmal einer Erkrankung bzw. eines bestimmten Erkrankungstypus anknüpft und diesbezüglich eine systematisch-automatisierte Verarbeitung bzw. einen systematischen Abgleich von Gesundheitsdaten anordnet. Inwieweit demgegenüber eine Regelung zum nicht-systematischen Datenabgleich mit Art. 10 JI-RL vereinbar wäre, sofern sie sicherstellen würde, dass die Erforderlichkeit der betreffenden Datenverarbeitung stets im Hinblick auf den jeweiligen Einzelfall geprüft wird, hinge entscheidend von ihrer konkreten Ausgestaltung im Einzelfall ab.

---

86 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 131

87 EuGH, Urteil vom 26. Januar 2023, Rs. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Rn. 132.

3. Verfassungsrechtliche Zulässigkeit

In verfassungsrechtlicher Hinsicht erscheinen vor allem die Verbandskompetenz des Bundes und die Vereinbarkeit der geforderten Regelungen mit dem Grundrecht auf informationelle Selbstbestimmung problematisch.

3.1. Verbandskompetenz des Bundes

Zunächst müsste der **Bund** für die vom Auftrag erfassten Maßnahmen überhaupt **zuständig** sein.

Gefordert wird, die datenschutzrechtlichen Vorgaben für den Austausch von Gesundheitsdaten und den Erkenntnissen der Gefahrenabwehrbehörden so anzupassen, dass die Erkenntnisse von Sicherheits-, Gesundheits-, Waffen- und anderen betroffenen Behörden bundesweit besser vernetzt und Risikopotenziale von Menschen mit psychischen Erkrankungen frühzeitig erkannt werden können.

Mit der Anpassung datenschutzrechtlicher Vorgaben geht es um ein **legislatives Tätigwerden**, so dass dem Bund die dafür nötige **Gesetzgebungskompetenz** zustehen müsste. Offen ist, wie genau das postulierte Ziel einer besseren bundesweiten Vernetzung der bei unterschiedlichen Behörden vorliegenden Erkenntnisse über psychisch kranke Personen mit Fremdgefährdungspotenzial erreicht werden soll. In seiner Entschließung verlangt der Bundesrat die **„Anpassung der datenschutzrechtlichen Vorgaben für den Austausch von Gesundheitsdaten und den Erkenntnissen der Gefahrenabwehrbehörden“**. Daraus allein wird nicht deutlich, **wie** der geforderte Datenaustausch **in der Praxis ausgestaltet** und umgesetzt werden soll. Diese Ausgestaltung und Umsetzung ist maßgeblich für die Frage, ob und inwieweit ein **Bedarf für die Anpassung datenschutzrechtlicher Vorgaben** besteht. Daher kann die Frage, ob dem Bund die erforderliche Gesetzgebungskompetenz zusteht, auf dieser Grundlage **nicht mit Gewissheit beantwortet** werden. Im Folgenden wird daher dargestellt, für welche Handlungsoptionen des Bundes eine Gesetzgebungskompetenz theoretisch gegeben sein könnte.

Gemäß Art. 70 Abs. 1 Grundgesetz (GG)[88] haben die **Länder** das **Recht der Gesetzgebung**, soweit das GG nicht dem Bund Gesetzgebungsbefugnisse verleiht. Die **Abgrenzung** der Zuständigkeit zwischen Bund und Ländern bemisst sich gemäß Art. 70 Abs. 2 GG im Einzelnen nach den Vorschriften über die **ausschließliche** (Art. 71, 73 GG) und die **konkurrierende** (Art. 72, 74 GG) Gesetzgebung.

3.1.1. Gesetzgebungskompetenz aus Art. 71, 73 Abs. 1 Nr. 10 Buchst. a GG

In Betracht kommt zunächst die ausschließliche Gesetzgebungskompetenz des Bundes für die **Zusammenarbeit von Bund und Ländern in der Kriminalpolizei** gemäß Art. 71, 73 Abs. 1 Nr. 10 Buchst. a GG.

88 Grundgesetz für die Bundesrepublik Deutschland (GG) in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 22. März 2025 (BGBl. 2025 I Nr. 94) geändert worden ist.

Zusammenarbeit ist eine auf Dauer angelegte Form der Kooperation, die die laufende gegenseitige Unterrichtung und Auskunftserteilung, die wechselseitige Beratung sowie gegenseitige Unterstützung und Hilfeleistung in den Grenzen der je eigenen Befugnisse umfasst und funktionelle und organisatorische Verbindungen, gemeinschaftliche Einrichtungen und **gemeinsame Informationssysteme** erlaubt.[89] Dabei hält der Bund zentrale Dienste für die Länder vor[90], z.B. die **Verbunddateien** INPOL und NADIS, in die jeweils von den Ländern und von Bundesbehörden in eigener Zuständigkeit erhobene Daten dezentral eingespeist und für alle Verbundteilnehmer zum Abruf bereitgehalten werden.[91]

Die **Kompetenz für die Zusammenarbeit** zwischen den verschiedenen Polizeibehörden bezieht sich **ausdrücklich** auf die „**Kriminalpolizei**". Da mit Art. 73 Abs. 1 Nr. 10 GG insgesamt die Möglichkeit geschaffen werden soll, föderale Zuständigkeitsgrenzen bei der Erfüllung repressiver und präventiver Aufgaben zu lockern, ist mit dem Begriff **keine Beschränkung auf** den Bereich der **Strafverfolgung** verbunden; vielmehr kann der Bund auf dieser kompetenziellen Grundlage auch eine Zusammenarbeit zur **Verhinderung von Straftaten** regeln.[92] Dabei muss es allerdings um **Straftaten von einigem Gewicht** gehen, so dass Vorschriften über eine Zusammenarbeit zur allgemeinen Gefahrenabwehr oder zur Bekämpfung von Kleinkriminalität und Ordnungswidrigkeiten nicht auf Art. 73 Abs. 1 Nr. 10 GG gestützt werden können.[93] Welche Straftaten als hinreichend gewichtig anzusehen sind, unterliegt der **Einschätzungsprärogative des Gesetzgebers**, so dass eine entsprechende Regelung nur darauf untersucht werden könnte, ob es sich um Straftatbestände handelt, bei denen es **vertretbarerweise** einer **behördlichen Zusammenarbeit bedarf** bzw. **eine solche naheliegt**.[94] Die Kompetenz aus Art. 73 Abs. 1 Nr. 10 Buchst. a) GG erstreckt sich des Weiteren auf alle gesetzlichen Regelungen, die für eine Zusammenarbeit mit den Ländern auf dem Gebiet der Kriminalpolizei erforderlich sind, insbesondere Bestimmungen über die genauen Aufgabenkreise innerhalb dieses Gebiets, auf denen die Zusammenarbeit stattfinden soll.[95] Nicht festlegen kann der Bund dagegen, welche Landesbehörden im Einzelnen mit dem Bund zusammenarbeiten, da die Zuständigkeit für den Erlass gesetzlicher Bestimmungen über Einrichtung und Auswahl der kooperierenden Landesbehörden sowie über deren Struktur und Verfahrensweise weiterhin bei den Ländern liegt.[96]

Fraglich ist, ob die Verbesserung des **Austausches von Gesundheitsdaten** und von **Erkenntnissen der Gefahrenabwehrbehörden** über psychisch erkrankte Personen, von denen eine

89 BVerfG, Urt. v. 24. April 2013 – 1 BvR 1215/07 (= BVerfGE 133, 277 (Rn. 97)).

90 Heintzen, in: Huber/Voßkuhle, GG, 8. Auflage 2024, Art. 73 Rn. 110.

91 Uhle, in: Dürig/Herzog/Scholz, GG, Werkstand: 110. El. März 2026, Art. 73 Rn. 231; Graulich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, BKAG § 13 Informationssysteme des Bundes Rn. 3.

92 BVerfG, Urt. v. 24. April 2013 – 1 BvR 1215/07 (= BVerfGE 133, 277 (Rn. 98)).

93 BVerfG, ebd.; BVerfG, Beschl. v. 10. November 2020 – 1 BvR 3214/15 (= BVerfGE 156, 11 (Rn. 77)); Wittreck, in: Dreier, GG, 3. Auflage 2015, Art. 73 Rn. 72.

94 Uhle, in: Dürig/Herzog/Scholz, GG, Werkstand: 110. El. März 2026, Art. 73 Rn. 239.

95 Uhle, in: Dürig/Herzog/Scholz, GG, Werkstand: 110. El. März 2026, Art. 73 Rn. 233.

96 Uhle, in: Dürig/Herzog/Scholz, GG, Werkstand: 110. El. März 2026, Art. 73 Rn. 233.

Fremdgefährdung ausgeht, unter dem Gesichtspunkt der **Verhinderung von Straftaten** auf die **Kompetenz aus Art. 73 Abs. 1 Nr. 10 Buchst. a GG** gestützt werden könnte, oder ob sie dem **allgemeinen Gefahrenabwehrrecht** und damit der **allgemeinen Gesetzgebungskompetenz der Länder** aus Art. 70 Abs. 1 GG zuzuordnen wäre. Durch den Datenaustausch sollen die Behörden in die Lage versetzt werden, rechtzeitig einzuschreiten, um künftige Gewalttaten psychisch kranker Personen zu verhindern. Es könnte dabei also sowohl um die Verhinderung von Straftaten als auch um die Gefahrenabwehr gehen. Bei solchen sog. **doppelfunktionalen Regelungen** erfolgt eine Zuordnung zum Bereich der Verhinderung von Straftaten oder zum Bereich der Gefahrenabwehr nach dem **Schwerpunkt des verfolgten Zweckes**; lässt sich ein solcher Schwerpunkt nicht bestimmen, so steht dem Gesetzgeber ein Entscheidungsspielraum für die Zuordnung zu, so dass entsprechende Befugnisse unter Umständen sowohl auf Bundes- als auch auf Landesebene geregelt werden können.[97]

Vorliegend sollen Gesundheitsdaten und Erkenntnisse von Gefahrenabwehrbehörden ausgetauscht werden, um künftigen Gewalttaten psychisch kranker Personen zuvorzukommen. Es wird dabei also zumeist um Personen gehen, die aufgrund ihrer psychischen Erkrankung **nicht oder nur eingeschränkt schuldfähig** sind und ihre Handlungen daher **nicht oder nur bedingt strafbar** sind. Es geht also nicht in erster Linie darum, die Begehung einer Straftat zu verhindern und die betreffende Person der Strafverfolgung zuzuführen. Der Schwerpunkt liegt vielmehr darin, die Verletzung von Rechtsgütern Dritter zu verhindern und die Allgemeinheit vor den im Einzelfall von einer psychisch kranken Person ausgehenden Gefahren zu schützen. Somit geht es hier im Schwerpunkt **nicht um die Verhinderung von Straftaten**, sondern um die **allgemeine Gefahrenabwehr**. Es ist daher **nicht** die **Zusammenarbeit von Bund und Ländern** auf dem Gebiet der **Kriminalpolizei** betroffen. Für diesen Befund spricht zudem der Umstand, dass der Datenaustausch auch Gesundheitsdaten umfassen soll. Solche Daten liegen typischerweise bei den **sozialpsychiatrischen Diensten** vor, die aber – ebenso wie die **Gefahrenabwehrbehörden** – gerade **nicht** zur **Kriminalpolizei** gehören.

Der Bund könnte die vom Bundesrat verlangten Regelungen daher **nicht** auf die **Kompetenz aus Art. 71, 73 Abs. 1 Nr. 10 Buchst. a GG** stützen.

3.1.2. Doppeltür-Modell des BVerfG

Eine weitere **Gesetzgebungskompetenz**, die dem Bund erlaubt, **insgesamt** die **Zusammenarbeit** oder den **Datenaustausch** zwischen Behörden von Bund und Ländern als solchen zu regeln, ist **nicht ersichtlich**. Dies bedeutet jedoch nicht zwingend, dass der Bund gar keine Vorschriften im Zusammenhang mit der Erleichterung des Austauschs von Gesundheitsdaten und von Erkenntnissen der Gefahrenabwehrbehörden erlassen könnte. Der Gesetzgeber müsste dabei jedoch die **Maßgaben** beachten, die das **BVerfG** zum sog. **Doppeltür-Modell** entwickelt hat:

> „Bei der Regelung eines Datenaustauschs zur staatlichen Aufgabenwahrnehmung ist darüber hinaus aber auch zwischen der Datenübermittlung seitens der auskunftserteilenden Stelle und dem Datenabruf seitens der auskunftsuchenden Stelle zu unterscheiden. Ein Datenaustausch vollzieht sich durch die einander korrespondierenden Eingriffe von Abfrage und Übermittlung, die jeweils einer eigenen Rechtsgrundlage bedürfen. Der Gesetzgeber muss, bildlich

97 BVerfG, Beschl. v. 18. Dezember 2018 – 1 BvR 142/15 (= BVerfGE 155, 244 (Rn. 72)).

> gesprochen, nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten. Dies schließt - nach Maßgabe der Kompetenzordnung und den Anforderungen der Normenklarheit - nicht aus, dass beide Rechtsgrundlagen auch in einer Norm zusammengefasst werden können."[98]

Soll der Austausch bestimmter Daten über psychisch kranke Personen rechtlich erleichtert werden, so müssten also **sowohl Vorschriften** über **die Abfrage bzw. Annahme** der Daten **als auch** über das **Senden bzw. Übermitteln** der Daten angepasst bzw. erlassen werden. Inwieweit der Bundesgesetzgeber entsprechende Regelungen treffen kann, hängt davon ab, inwieweit er **für die jeweilige Regelung** eine **Gesetzgebungskompetenz** besitzt. Dies hat zur Folge, dass der **Bund** unter Umständen **nur eine Seite des Datenaustausches** (z.B. die Übermittlung oder Abfrage durch eine bestimmte Behörde) regeln kann, während es für die Teilnahme **anderer Behörden** an dem Austausch einer **entsprechenden Regelung** durch die **Länder** bedürfte.

3.1.3. Gesetzgebungskompetenzen des Bundes für Teilbereiche

Auftragsgemäß wird vom gesetzgeberischen Ziel ausgegangen, durch Anpassung entsprechender Vorschriften die **bundesweite Vernetzung** der Erkenntnisse zwischen **Sicherheits-, Gesundheits-, Waffen-** und **gegebenenfalls anderen relevanten Behörden** zu verbessern. Auch wenn dem Bund, wie oben dargelegt (vgl. Ziff. 3.1.1.) hier keine Kompetenz zur umfassenden Regelung der Zusammenarbeit von Bund und Ländern zukommt, könnte er gleichwohl in einzelnen Teilbereichen, für die er eine Gesetzgebungskompetenz besitzt, die Übermittlung oder Abfrage von Daten regeln.

3.1.3.1. Sicherheitsrecht / Gefahrenabwehrrecht

Im Bereich des **Sicherheitsrechts** kommen dem **Bund** zwar **vereinzelt Gesetzgebungskompetenzen** mit gefahrenabwehrrechtlicher Ausrichtung zu (z.B. Art. 71, 73 Abs. 1 Nr. 5 GG für die bundespolizeiliche Tätigkeit im Zoll- und Grenzschutz), er besitzt jedoch **keine allgemeine Kompetenz** für das **Gefahrenabwehrrecht**. Diese liegt vielmehr gemäß **Art. 70 Abs. 1 GG** bei den **Ländern**.

3.1.3.2. Gesundheitsrecht

Auch im **Gesundheitsrecht** kann sich der Bund auf verschiedene Gesetzgebungskompetenzen berufen, so z.B. **Art. 72 Abs. 1, 74 Abs. 1 Nr. 19 GG**, wonach der Bund Regelungen treffen kann über „Maßnahmen gegen **gemeingefährliche** oder übertragbare **Krankheiten** bei Menschen und Tieren, Zulassung zu ärztlichen und anderen Heilberufen und zum Heilgewerbe, sowie das Recht des Apothekenwesens, der Arzneien, der Medizinprodukte, der Heilmittel, der Betäubungsmittel und der Gifte". Dieser Kompetenztitel dürfte hier jedoch **nicht einschlägig** sein. **Gemeingefährliche Krankheiten** zeichnet aus, dass sie sowohl eine bestimmte Schwere der Gesundheitsbeeinträchtigung beim Erkrankten aufweisen als auch vermehrt, über Einzelfälle hinausreichend auftreten, so dass eine „**überindividuelle Betroffenheit**" vorliegt.[99] Psychische Erkrankungen als

---

98 BVerfG, Beschl. v. 24. Januar 2012 – 1 BvR 1299/05 (= BVerfGE 130, 151 (184)).

99 Uhle, in: Dürig/Herzog/Scholz, GG, Werkstand: 110. El. März 2026, Art. 74 Rn. 423.

solche erfüllen dieses quantitative Merkmal nicht. Auch für den Bereich der Gesundheitsbehörden steht dem Bund daher nicht die hier erforderliche **Gesetzgebungskompetenz** zu. Diese fällt insoweit wiederum gemäß **Art. 70 Abs. 1 GG** den **Ländern** zu.

3.1.3.3. Waffenrecht

Dagegen liegt das **Waffenrecht** gemäß **Art. 71, 73 Abs. 1 Nr. 12 GG** in der **ausschließlichen Gesetzgebungskompetenz** des Bundes. Grundsätzlich kann der Bund daher in diesem Bereich **materiellrechtliche Regelungen** über Voraussetzungen und Grenzen des Umgangs mit Waffen und Munition erlassen.

Allerdings ist zu beachten, dass die **Länder** gemäß **Art. 84 Abs. 1 Satz 1 GG** u.a. das **Verwaltungsverfahren selbst regeln**, wenn sie die **Bundesgesetze als eigene Angelegenheiten** ausführen. Mangels abweichender Regelung im Grundgesetz ist dies nach des **Art. 83 GG**, wonach die Länder die Bundesgesetze grundsätzlich als eigene Angelegenheiten ausführen, beim Waffengesetz (WaffG)[100] der Fall. In diesem Bereich kann gemäß **Art. 84 Abs. 1 Satz 2 GG** auch der **Bund Regelungen** treffen; macht der Bund von dieser Möglichkeit Gebrauch und erlässt eine Regelung, steht nun **wiederum** den **Ländern** ein **Abweichungsrecht** zu. Hat ein Land abweichende Regelungen erlassen, so kann der **Bund** diese gemäß **Art. 84 Abs. 1 Satz 3 GG** erneut **ändern**, allerdings treten diese Änderungen **frühestens sechs Monate nach ihrer Verkündung in Kraft**, soweit nicht mit Zustimmung des Bundesrates anderes bestimmt ist. Gemäß **Art. 84 Abs. 1 Satz 5 GG** kann der **Bund** in Ausnahmefällen wegen eines **besonderen Bedürfnisses nach bundeseinheitlicher Regelung** das **Verwaltungsverfahren ohne Abweichungsmöglichkeit für die Länder** regeln. Diese Gesetze bedürfen gemäß Art. 84 Abs. 1 Satz 6 GG der Zustimmung des Bundesrates.

Welche Art von Regelungen i.S.d. Art. 84 Abs. 1 GG das **Verwaltungsverfahren** betreffen, hat das BVerfG wie folgt definiert:

> „Vorschriften über das Verwaltungsverfahren im Sinne von Art. 84 Abs. 1 GG sind danach jedenfalls gesetzliche Bestimmungen, die die Tätigkeit der Verwaltungsbehörden im Blick auf die Art und Weise der Ausführung des Gesetzes einschließlich ihrer Handlungsformen, die Form der behördlichen Willensbildung, die Art der Prüfung und Vorbereitung der Entscheidung, deren Zustandekommen und Durchsetzung sowie verwaltungsinterne Mitwirkungs- und Kontrollvorgänge in ihrem Ablauf regeln […].“[101]

Eine **Verfahrensregelung** ist also dadurch gekennzeichnet, dass das Gesetz **verbindlich** die **Art und Weise** sowie die **Form der Ausführung** eines **Bundesgesetzes** bestimmt, so z.B. auch dann, wenn materiellrechtliche Regelungen des Gesetzes nicht lediglich die Verwaltungsbehörden zum Handeln auffordern, sondern zugleich ein **bestimmtes verfahrensmäßiges Verwaltungshandeln** festlegen.[102] **Behördliche Datenabfragen und -übermittlungen** stellen **verwaltungsinterne Mitwirkungsvorgänge** dar. Würde der Gesetzgeber solche Abfragen und Übermittlungen im WaffG

---

100 Waffengesetz (WaffG) vom 11. Oktober 2002 (BGBl. I S. 3970, 4592; 2003 I S. 1957), das zuletzt durch Artikel 2 Absatz 10 des Gesetzes vom 20. März 2026 (BGBl. 2026 I Nr. 95) geändert worden ist.

101 BVerfG, Urt. v. 10. Dezember 1980 – 2 BvF 3/77 (= BVerfGE 55, 274 (320 f.)) [Auslassung durch Verf.].

102 BVerfG, Urt. v. 17. Juli 2002 – 1 BvF 1, 2/01 (= BVerfG 105, 313 (331)).

regeln, so müsste er dabei auch festlegen**, unter welchen Voraussetzungen** und **unter Beachtung welcher Verfahrensschritte** die Behörden Angaben über psychisch Erkrankte und von ihnen ausgehende Fremdgefährdungen an andere Behörden übermitteln oder von anderen Behörden entgegennehmen können. Bei den Vorschriften über die Übermittlung und Anforderung würde es sich somit um **Verfahrensregelungen i.S.d. Art. 84 Abs. 1 GG** handeln. Der **Bund** kann solche Regelungen gemäß **Art. 84 Abs. 1 Satz 2 GG** treffen. Wollte er verhindern, dass einzelne oder alle Länder Vorschriften erlassen, die von der Bundesregelung abweichen, müsste der Bund gemäß Art. 84 Abs. 1 Satz 5 GG **wegen eines besonderen Bedürfnisses nach bundeseinheitlicher Regelung** das Verwaltungsverfahren **ohne Abweichungsmöglichkeit für die Länder** regeln. Ob ein solches Bedürfnis vorliegend gegeben wäre, entzieht sich im Rahmen dieser Bearbeitung einer abschließenden Beurteilung.

Festzuhalten ist somit, dass der Bund für die Regelung des Datenaustausches über psychisch erkrankte Personen, von denen eine Fremdgefährdung ausgeht, nur im Bereich des Waffenrechts eine Sachgesetzgebungskompetenz aus Art. 71, 73 Abs. 1 Nr. 12 GG besitzt. Für waffenrechtliche Bundesgesetze kann der Bund gemäß Art. 84 Abs. 1 Satz 2 GG Regelungen über das Verwaltungsverfahren treffen, wozu auch Vorschriften über die Übermittlung und die Abfrage von Daten gehören. Dabei kann er grundsätzlich wegen eines besonderen Bedürfnisses nach bundeseinheitlicher Regelung eine Abweichungsmöglichkeit der Länder ausschließen.

Für andere Verwaltungsbehörden, etwa die Gefahrenabwehrbehörden der Länder oder die sozialpsychiatrischen Dienste, kann der Bund mangels Sachgesetzgebungskompetenz keine Regelungen über das Verwaltungsverfahren treffen. Hier müssen die Länder im Rahmen ihrer Regelungskompetenz aus Art. 70 Abs. 1 GG ihrerseits Vorschriften über Übermittlung und Abfrage der Daten erlassen.

3.2. Vereinbarkeit mit dem Grundrecht auf informationelle Selbstbestimmung

Regelungen des Bundes über die Übermittlung und Abfrage von Daten über psychisch Erkrankte müssten auch mit dem materiellen Verfassungsrecht, insbesondere den Grundrechten vereinbar sein. Solche Regeln könnten in das Recht auf informationelle Selbstbestimmung eingreifen.

3.2.1. Eingriff in den Schutzbereich

Das BVerfG leitet in ständiger Rechtsprechung aus **Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG** ein **Recht auf informationelle Selbstbestimmung** als Teil des allgemeinen Persönlichkeitsrechts her. Das Grundrecht gewährleistet die Befugnis des Individuums, grundsätzlich **selbst über die Preisgabe und Verwendung der eigenen personenbezogenen Daten zu bestimmen**.[103] Dies umfasst generell die Entscheidung darüber, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, weshalb auch alle entsprechenden Dokumentationen – etwa **Tagebücher und private Aufzeichnungen**[104] oder Unterlagen über den Gesundheitszustand und soziale

103 BVerfG, Urt. v. 15. Dezember 1983 – 1 BvR 209/83 – 1 BvR 269/83 – 1 BvR 362/83 – 1 BvR 420/83 – 1 BvR 440/83 – 1 BvR 484/83 (= BVerfGE 65, 1 (Rn 147)).

104 BVerfG, Beschl. v. 14. September 1989 – 2 BvR 1062/87 (= BVerfG, NJW 1990, 563 (564)).

Beziehungen, wie z.B. **Krankenakten**[105], Informationen einer **Suchtberatungsstelle**[106], Unterlagen zur **Entmündigung**[107], Akten eines **Sozialarbeiters**[108], Befunde über die **seelische Verfassung** und den **Charakter** des Einzelnen[109] oder Informationen über **genetische Merkmale** einer Person[110] – in den Schutzbereich des Grundrechts fallen.[111] Die staatliche Erhebung, Speicherung, (zweckändernde) Verwendung und Weitergabe solcher Daten stellen mithin typische Eingriffe in das Grundrecht auf informationelle Selbstbestimmung dar.[112]

Würde der Bund also die **Übermittlung und die Abfrage personenbezogener Daten** über psychisch Erkrankte **zur Erstellung von Fremdgefährdungsprognosen** regeln, lägen darin **Eingriffe** in das Grundrecht auf informationelle Selbstbestimmung.

3.2.2. Verfassungsrechtliche Rechtfertigung

Das Recht auf informationelle Selbstbestimmung gilt nicht schrankenlos, sondern unterliegt der sog. **Schrankentrias in Art. 2 Abs. 1 GG**, sodass Eingriffe grundsätzlich zugunsten der **verfassungsmäßigen Ordnung,** der **Rechte anderer** oder des **Sittengesetzes** gerechtfertigt werden können.[113] Praktisch bedeutsam ist dabei insbesondere die Schranke der verfassungsmäßigen Ordnung, bei der es sich der Sache nach um einen **Gesetzesvorbehalt** handelt. Dies bedeutet, dass Eingriffe stets einer **gesetzlichen Grundlage** bedürfen, mit der der **parlamentarische Gesetzgeber** alle **wesentlichen Entscheidungen** über Begrenzung von Art und Umfang der Datenverarbeitung selbst trifft, und dies nicht durch die Exekutive im Wege einer Rechtsverordnung erfolgt.[114]

3.2.2.1. Bestimmtheit und Normenklarheit

In inhaltlicher Hinsicht muss die gesetzliche Grundlage **hinreichend bestimmt** und **normenklar** abgefasst sein, um zu gewährleisten, dass die Exekutive im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfindet, die Gerichte eine wirksame Rechtskontrolle durchführen können und betroffene Personen die Möglichkeit erhalten, sich auf mögliche belastende Maßnahmen

105 BVerfG, Besch. v. 8. März 1972 – 2 BvR 28/71 (BVerfG, NJW 1972, 1123 (1124)).

106 BVerfG, Beschl. v. 24. Mai 1977 – 2 BvR 988/75 (=BVerfG, NJW 1977, 1489 (1490)).

107 BVerfG, Beschl. v. 09. März 1988 – 1 BvL 49/86 (=BVerfG, NJW 1988, 2031 (2031)).

108 BVerfG, Beschl. v. 19. Juli 1972 – 2 BvL 7/71 (=BVerfG, NJW 1972, 2214 (2215)).

109 BVerfG, Besch. v. 24. Juni 1993 – 1 BvR 689/92 (=BVerfG, NJW 1993, 2365 (2365 f.)).

110 BVerfG, Urt. v. 13. Februar 2007 – 1 BvR 421/05 (= BVerfG, NJW 2007, 753 (Rn. 66)).

111 Schmidt/Ahrendt, in: Erfurter Kommentar zum Arbeitsrecht, 26. Auflage 2026, GG Art. 2 Rn. 43.

112 BVerfG, Urt. v. 15. Dezember 1983 – 1 BvR 209/83 – 1 BvR 269/83 – 1 BvR 362/83 – 1 BvR 420/83 – 1 BvR 440/83 – 1 BvR 484/83 (= BVerfGE 65, 1 (Rn 147)).

113 Barczak, in: Dreier, GG, 4. Auflage 2023, Art. 2 Abs. 1 Rn. 105.

114 BVerfG, Urt. v. 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 (= BVerfGE165, 363 (Rn. 112)).

einzustellen.[115] Dabei steigen die Anforderungen an den **Grad der Bestimmtheit** mit zunehmender **Schwere des Eingriffs** an.[116] Für Eingriffe in das Recht auf informationelle Selbstbestimmung bedeutet dies, dass Anlass, Zweck und Umfang des Eingriffs **bereichsspezifisch, präzise und normenklar** festgelegt werden müssen.[117] Besonders streng sind die Anforderungen an die Bestimmtheit der gesetzlichen Grundlage bei **heimlichen Datenerhebungen und -verarbeitungen**, die weit in die Privatsphäre hineinreichen können, da solche Maßnahmen den Betroffenen kaum zur Kenntnis gelangen und daher von ihnen nur selten im Rechtsweg angegriffen werden können; der Gehalt der gesetzlichen Regelung kann in diesen Fällen nur eingeschränkt im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden, was der Gesetzgeber durch die hinreichende Bestimmtheit der jeweiligen Normen auffangen muss.[118]

3.2.2.2. Besonderheiten bei Zweckänderungen

Sollen bei den Behörden bereits vorliegende personenbezogene Daten zu einem **anderen als dem ursprünglichen Erhebungszweck verwendet** werden (wie bei der Erstellung von Prognosen über das Fremdgefährdungspotenzial einer bestimmten psychisch kranken Person), so muss der Gesetzgeber bei der Ausgestaltung der gesetzlichen Grundlage für die neue Verwendung weitere Vorgaben des BVerfG beachten:

> „Speicherung und Verwendung personenbezogener Informationen und Daten sind grundsätzlich an den Zweck und an das Verfahren gebunden, für die sie erhoben wurden […]. Eine Zweckänderung bedarf einer formell und materiell verfassungsgemäßen Rechtsgrundlage und muss durch Allgemeinbelange gerechtfertigt sein, die die grundrechtlich geschützten Interessen überwiegen […]. Der neue Verwendungszweck muss sich auf die Aufgaben und Befugnisse der Behörde beziehen, der die Daten übermittelt werden, und hinreichend klar geregelt sein. Schließlich dürfen der Verwendungszweck, zu dem die Erhebung erfolgt ist, und der veränderte Verwendungszweck nicht miteinander unvereinbar sein […]. Eine solche Unvereinbarkeit läge vor, wenn mit der Zweckänderung grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Erhebungsmethoden umgangen würden, die Informationen also für den geänderten Zweck nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen („hypothetischer Ersatzeingriff“ […]). Zur Sicherung der Zweckbindung muss eine gesetzliche Verpflichtung zur Kennzeichnung und Protokollierung bestehen […]. Zu gewährleisten ist die Erfüllung dieser Anforderungen durch Vorschriften des Normgebers, der für den Erlass der Vorschriften über die Datenerhebung zuständig ist […].“[119]

---

115 BVerfG, Urt. v. 11. März 2008 – 1 BvR 2074/05, 1 BvR 1254/07 (= BVerfGE 120, 378 (407 f.)).

116 BVerfG, Urt. v. 11. März 2008 – 1 BvR 2074/05, 1 BvR 1254/07 (= BVerfGE 120, 378 (408)).

117 BVerfG, Urt. v. 24. Januar 2012 –1 BvR 1299/05 (= BVerfGE 130, 151 (202)).

118 BVerfG, Urt. v. 01. Oktober 2024 – 1 BvR 1160/19 (= BVerfGE 169, 332 (Rn. 95)).

119 BVerfG, Beschl. v. 07. Dezember 2011 – 2 BvR 2500/09, 2 BvR 1857/10 (= BVerfGE 130, 1 (33 f.)) [Auslassungen durch Verf.]

In einer späteren Entscheidung hat sich das BVerfG auf diese Passage bezogen und klarstellend ausgeführt:

> „Das Kriterium der Datenneuerhebung gilt allerdings nicht schematisch abschließend und schließt die Berücksichtigung weiterer Gesichtspunkte nicht aus […]. So steht die Tatsache, dass die Zielbehörde bestimmte Datenerhebungen, zu denen die Ausgangsbehörde berechtigt ist, ihrerseits wegen ihres Aufgabenspektrums nicht vornehmen darf, einem Datenaustausch nicht prinzipiell entgegen […]. Auch können Gesichtspunkte der Vereinfachung und der Praktikabilität bei der Schaffung von Übermittlungsvorschriften es rechtfertigen, dass nicht alle Einzelanforderungen, die für die Datenerhebung erforderlich sind, in gleicher Detailliertheit für die Übermittlung der Daten gelten. Das Erfordernis einer Gleichgewichtigkeit der neuen Nutzung bleibt hierdurch jedoch unberührt.“[120]

3.2.2.3. Verhältnismäßigkeit

Welche Anforderungen im Einzelnen an die Rechtfertigung von Eingriffen im Rahmen der **Verhältnismäßigkeitsprüfung** zu stellen sind, hängt von Art, Umfang und denkbaren Verwendungen der erhobenen Daten sowie der Gefahr ihres Missbrauchs ab.[121] Grundsätzlich ist eine Maßnahme verhältnismäßig, wenn sie **zur Erreichung eines legitimen Zwecks geeignet, erforderlich und angemessen** ist.[122]

Ob diese Anforderungen bei der Verarbeitung von Daten über psychisch kranke Personen zur Erstellung von Fremdgefährdungsprognosen erfüllt wären, kann auf der hier diskutierten hypothetischen Grundlage **nicht abschließend bewertet** werden. Zwar dürfte die Erstellung der Prognosen dem Schutz der Rechtsgüter von Leben und körperlicher Unversehrtheit aus Art. 2 Abs. 2 GG und somit besonders hochrangigen Rechtsgütern dienen. Allerdings **variieren** die **verfassungsrechtlichen Anforderungen** an die Rechtfertigung von (automatisierten) **Datenanalysen und -auswertungen** nach der Rechtsprechung des BVerfG in Abhängigkeit von der **gesetzlichen Ausgestaltung** des Eingriffs. Zu den Kriterien, anhand derer sich das Eingriffsgewicht einer Datenanalyse bemisst, und den daraus jeweils folgenden Verhältnismäßigkeitsanforderungen führt das Gericht aus:

> „Dabei ist unter anderem bedeutsam, wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind und unter welchen Voraussetzungen dies geschieht, insbesondere ob diese Personen hierfür einen Anlass gegeben haben. Maßgebend sind also die Gestaltung der Eingriffsschwellen, die Zahl der Betroffenen und die Intensität der individuellen Beeinträchtigung im Übrigen. Für das Gewicht der individuellen Beeinträchtigung ist erheblich, ob die Betroffenen als Personen anonym bleiben, welche persönlichkeitsbezogenen Informationen erfasst werden und welche Nachteile den Grundrechtsträgern aufgrund der Maßnahmen drohen oder von ihnen nicht ohne Grund befürchtet werden. Dabei führt insbesondere die Heimlichkeit einer staatlichen Eingriffsmaßnahme ebenso zur Erhöhung ihrer Intensität wie die

120 BVerfG, Urt. v. 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 (= BVerfG, NJW 2016, 1781 (Rn 287)).

121 BVerfG, Urt. v. 15. Dezember 1983 – 1 BvR 209/83 – 1 BvR 269/83 – 1 BvR 362/83 – 1 BvR 420/83 – 1 BvR 440/83 – 1 BvR 484/83 (= BVerfGE 65, 1 (Rn. 152)).

122 BVerfG, Urt. v. 2. März 2006 – 2 BvR 2099/04 (= BVerfG, NJW 2006, 976 (Rn. 97)).

> faktische Verwehrung vorherigen Rechtsschutzes und die Erschwerung nachträglichen Rechtsschutzes, wenn er überhaupt zu erlangen ist […].[123]

Das BVerfG stellt bei der Verhältnismäßigkeit grundsätzlich auch auf die **Nähe der Daten** zum unantastbaren Bereich privater Lebensgestaltung, der sog. **Intimsphäre**, ab; **der Schutz ist umso intensiver, je näher die Daten dieser Sphäre stehen**.[124] Befunde über die **psychische Gesundheit** oder den **Charakter** einer Person hat das BVerfG im Vergleich zu rein medizinischen Feststellungen als der **Intimsphäre näherstehend** bewertet.[125] **Klientenakten** einer Suchtberatungsstelle mit den Aufzeichnungen des Beraters über Gespräche, Tests, therapeutische Maßnahmen und den eigenen schriftlichen Äußerungen des Ratsuchenden betreffen nach Ansicht des BVerfG jedoch eindeutig nicht die Intim- sondern die **Privatsphäre** des Klienten.[126] Gleiches soll für **ärztliche Karteikarten (Krankenblätter)** mit Angaben über Anamnese, Diagnose und therapeutische Maßnahmen[127], und die Informationen, die ein **Sozialarbeiter** im Zuge einer Beratung von dem Klienten über diesen erhält[128], gelten.

Die **verfassungsrechtliche Zulässigkeit,** der vom Auftrag umfassten Rechtsänderungen hängt somit **maßgeblich** von der **Ausgestaltung der konkreten Vorschriften** ab, wobei den **Eingriffsschwellen**, den **Voraussetzungen** für eine **zweckändernde Verwendung**, den konkret **verwendeten Daten**, dem Rang der zu **schützenden Rechtsgüter** sowie der **Reichweite und des Umfangs** der Datenanalyse und -auswertung und der daraus folgenden **Belastung der betroffenen Personen** entscheidende Bedeutung zukommt.

***

123 BVerfG, Urt. v. 15. Dezember 1983 – 1 BvR 209/83 – 1 BvR 269/83 – 1 BvR 362/83 – 1 BvR 420/83 – 1 BvR 440/83 – 1 BvR 484/83 (= BVerfGE 65, 1 (Rn. 152)).

124 BVerfG, Besch. v. 24. Juni 1993 – 1 BvR 689/92 (=BVerfG, NJW 1993, 2365 (2365)); BVerfG, Urt. v. 15. Dezember 1983 – 1 BvR 209/83 – 1 BvR 269/83 – 1 BvR 362/83 – 1 BvR 420/83 – 1 BvR 440/83 – 1 BvR 484/83 (= BVerfGE 65, 1 (Rn. 99)).

125 BVerfG, Besch. v. 24. Juni 1993 – 1 BvR 689/92 (=BVerfG, NJW 1993, 2365 (2366)).

126 BVerfG, Beschl. v. 24. Mai 1977 – 2 BvR 988/75 (=BVerfG, NJW 1977, 1489 (1490)).

127 BVerfG, Besch. v. 8. März 1972 – 2 BvR 28/71 (BVerfG, NJW 1972, 1123 (1124)).

128 BVerfG, Beschl. v. 19. Juli 1972 – 2 BvL 7/71 (=BVerfG, NJW 1972, 2214 (2215)).