universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„Die Auslegung der Anonymisierung in ausgewählten Rechtsakten unter besonderer Berücksichtigung der Forschung“

verfasst von / submitted by

Mag[a] iur Jessica Tara Einzinger

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2021 / Vienna 2021

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 942
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Informations- und Medienrecht
Betreut von / Supervisor:	Ao. Univ.Prof. Dr. iur. Dietmar Jahnel

Vorwort

Die vorliegende Masterarbeit wurde als Abschlussarbeit für den Universitätslehrgang Informations- und Medienrecht 2019/2020 verfasst.

Im Interesse einer besseren Lesbarkeit wurden in dieser Arbeit überwiegend geschlechtsneutrale Formulierungen gewählt und auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich, divers (m/w/d) verzichtet. Dies bedeutet in keiner Weise eine Diskriminierung eines Geschlechts. Alle Leser*innen sollen sich gleichermaßen angesprochen fühlen, unabhängig ihres Geschlechts.

Inhaltsverzeichnis

1. Einleitung

Der Schutz der Persönlichkeitsrechte aller Menschen in der Europäischen Union ist ein hohes Gut. Unter diesen Schutz fällt die Verarbeitung von Daten, die sich auf diese Personen beziehen, sogenannte personenbezogene Daten.[1] Bei der Verarbeitung personenbezogener Daten sind die Datenschutz-Grundverordnung (DSGVO)[2] und die jeweils geltenden anwendbaren nationalen Regelungen zu beachten. Aufgrund der verschiedenen Rechtssystemen in den einzelnen Mitgliedstaaten, kulturellen und wirtschaftlichen Unterschieden wurde die Richtlinie 95/46/EG (EU-Datenschutzrichtline oder DS-RL) unterschiedlich ausgelegt und implementiert.[3] Auch die DSGVO wird im Bezug auf anonyme und anonymisierte Daten[4] unterschiedlich interpretiert und gelebt. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDi) nahm die unklare Rechtslage zum Anlass ein öffentliches Konsultationsverfahren, zwei Jahre nach in Krafttreten der DSGVO (2020), in die Wege zu leiten. Eine Anonymisierung kann einen Weg zu einer Verarbeitung eröffnen, wenn eine Datenverarbeitung ansonsten unzulässig wäre. Die Anonymisierung sei ein technischer Vorgang, welcher es zum Ziel hat jeglichen Personenbezug zu entfernen.[5] Die DSGVO selbst gibt keine technischen Vorgaben, wie die Anonymisierung erreicht werden kann.[6] Die tatsächliche rechtliche Möglichkeit einer Anonymisierung komme durch den Erwägungsgrund 26 zum Ausdruck, da die Anonymisierung nicht explizit in die DSGVO Eingang gefunden hätte.[7]

---

[1] Art 4 Z 1 VO (EU) 2016/679 „"personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;"

[2] 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 2016/119, 1 idF L 2016/314.

[3] *Custers*, Scope and Context, in T.M.C. ASSER PRESS, EU Personal Data Protection in Policy and Practice (2019) 3.

[4] Siehe dazu *Hödl* in Knyrim (Hrsg), DatKomm Art 4 DSGVO RN 17 (Stand 1.12.2018).

[5] *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,* Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 2 (2,3) <https://www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-Anonymisierung-TK/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=2> (letzter Aufruf 20.07.20).

[6] *Schneider*, § 15 Datenschutz in der Informationstechnik, in Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht (2019) RN 1 (65).

[7] *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,* Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 2 (2 f) <https://www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-

Insbesondere durch die Digitalisierung und internationale Vernetzung verschwimmen die Grenzen zwischen akademischen und privatwirtschaftlichen Forschungszwecken.[8] Erklärtes Ziel der Europäischen Kommission war es, die Grundfreiheit der Privatsphäre zu wahren und gleichzeitig Wirtschaftswachstum, Digitalisierung und den freien Verkehr personenbezogener Daten zu ermöglichen.[9] Datenschutzrechtliche Bestimmungen sollen ein Sicherheitsnetz für die betroffenen Personen sein, deren Daten verarbeitet werden. Die Frage der Abgrenzung zwischen personenbezogenen Daten und nicht-personenbezogenen Daten, die den Anwendungsbereich des Datenschutzrechts bestimmen soll, stellt sich immer wieder, da sie unterschiedliche rechtliche Implikationen mit sich bringt. Die Verarbeitung anonymisierter Daten ermöglicht es Datenverarbeitern sich mit der DSGVO und den jeweiligen länderspezifischen Datenschutzbestimmungen nicht auseinandersetzen zu müssen.

In dieser Arbeit werden bereichsspezifische Bestimmungen untersucht, die insbesondere auf die Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken anwendbar sind und im Zusammenhang mit der Bestimmbarkeit des Personenbezugs zu Unklarheiten in der Auslegung führen. Um den von der europäischen Sichtweise abweichenden Ansatz der Anonymisierung zu veranschaulichen, werden die De-Identifizierungsmethoden im US-Gesetz („Health Insurance Portability and Accountability Act“ - HIPAA) vorgestellt. Darüber hinaus wird die spezielle Problematik der Anonymisierung genetischer Daten untersucht und diskutiert, ob die Anonymisierung von Daten noch ein ausreichendes Schutzkonzept sein kann, das den technischen Entwicklungen des 21. Jahrhunderts und den damit verbundenen Anforderungen an den Schutz der Betroffenen und ihrer Daten gerecht wird.

2. Anonymisierung

Die seit dem 25.05.2018 unmittelbar geltende *Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr*, sollte den

---

Anonymisierung-TK/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=2> (letzter Aufruf 20.07.20).

[8] *European Data Protection Supervisor*, A Preliminary Opinion on data protection and scientific research, 2 <https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf> (letzter Aufruf 17.07.20).

[9] MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN Der Schutz der Privatsphäre in einer vernetzten Welt Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM (2012) 9 endg.

Grundstein für ein einheitliches Datenschutzrecht in Europa legen und das Ziel des freien Datenflusses innerhalb des Binnenmarkts absichern. Die EU-Bürger sollten mehr Vertrauen in die Internetdienste und durch die verpflichtende Information über ihre Rechte, mehr Kontrolle in Bezug auf die Verarbeitung ihrer personenbezogenen Daten erhalten. Bei der europäischen Datenschutzreform geht es jedoch nicht nur um den Schutz der Grundrechte und -freiheiten des Einzelnen. Die DSGVO sollte auch das Potenzial des digitalen Binnenmarkts vorantreiben und für Wirtschaftswachstum, Innovation und Arbeitsplätze sorgen.[10] Vor allem aufgrund der steigenden Anzahl von Menschen mit Zugang zu Internetdiensten, die ihre personenbezogenen Daten im Internet hinterlassen, sei es beim Online-Einkauf oder beim Surfen im Internet, und der technischen Maßnahmen, die zur Datenerfassung eingesetzt werden, sei eine Datenschutzreform notwendig geworden.[11]

Im Erwägungsgrund 6 der DSGVO heißt es: *„Rasche technologische Entwicklungen und die Globalisierung haben den Datenschutz vor neue Herausforderungen gestellt. Das Ausmaß der Erhebung und des Austauschs personenbezogener Daten hat eindrucksvoll zugenommen. Die Technik macht es möglich, dass private Unternehmen und Behörden im Rahmen ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zurückgreifen. Zunehmend machen auch natürliche Personen Informationen öffentlich weltweit zugänglich. Die Technik hat das wirtschaftliche und gesellschaftliche Leben verändert und dürfte den Verkehr personenbezogener Daten innerhalb der Union sowie die Datenübermittlung an Drittländer und internationale Organisationen noch weiter erleichtern, wobei ein hohes Datenschutzniveau zu gewährleisten ist.“*[12] Die Grundlage eines derartigen Konzepts ist der Begriff der personenbezogenen Daten und die Abgrenzung zu den nicht-personenbezogenen Daten.[13]

Die Definition in Artikel 4 Z 1 und Erwägungsgrund 26 der DSGVO sind die einzigen direkten Anhaltspunkte für die Bestimmung einer solchen Abgrenzung.

---

[10] *Europäische Kommission*, Pressemitteilung Kommission schlägt umfassende Reform des Datenschutzrechts vor, um Nutzern mehr Kontrolle über ihre Daten zu geben und die Kosten für Unternehmen zu verringern, <https://ec.europa.eu/commission/presscorner/detail/de/IP_12_46> (letzter Aufruf 23.01.21)

[11] BERICHT DER KOMMISSION Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46), KOM (2003) 265 endg.

[12] ErwGr 6 VO (EU) 2016/679.

[13] MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM (2010) 609 endg.

2.1 Die Definition personenbezogener Daten

Personenbezogene Daten sind gemäß Artikel 4 Z 1 DSGVO „*alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;“*

Die Formulierungen der DSGVO im Gegensatz zur DS-RL, die einerseits *„bestimmt"* oder *„bestimmbar"* und nun *„identifiziert"* oder *„identifizierbar"* und andererseits *„alle Informationen über eine* [...] *natürliche Person"* und nun „*alle Informationen die sich auf eine* [...] *natürliche Person* [...] *beziehen“* anführt, sind lediglich sprachlicher Natur.[14] In der DSGVO werden die Begriffe Daten und Informationen gleichbedeutend benutzt, auch wenn dies aus informationstechnischer Sicht unpräzise erscheint. Da die Begriffe in der DSGVO selbst einander umschreiben, ist die Unterscheidung allerdings lediglich akademisch.[15]

Informationen sind weit auszulegen und umfassen personenbezogene Daten in jeglicher Form. Sie können alphabetisch (ein Name), numerisch (z.B. Identifikationsnummer wie eine Sozialversicherungsnummer) oder in Form von Videos oder Bildern auftreten. Personenbezogene Daten können objektiver Natur sein (wie die Angabe über eine Substanz im Körper) als auch subjektiv, wie Auskünfte, Meinungen und Bewertungen. Artikel 4 Z 1 DSGVO bezieht sich auf „*Informationen*" und nicht nur auf Daten was darauf hindeutet, dass Daten einen gewissen Informationswert erfordern.[16] Durch die DSGVO wurde der Begriff der „*Kennung*“ eingeführt, welcher mit einer Liste von Informationen einhergeht, welche als Kennung gelten sollen. Insbesondere aufgrund des technologischen Fort-

[14] *Krügel*, Das personenbezogene Datum nach der DS-GVO, ZD 2017, 455.
[15] *Bergauer in* Knyrim (Hrsg), Datenschutz-Grundverordnung DSGVO 43 f. (2016); Eingehend zu den unterschiedlichen Begrifflichkeiten siehe *Haase*, Datenschutzrechtliche Fragen des Personenbezugs (2015) 120 ff.
[16] *Finck/Pallas*, They who must not be identified—distinguishing personal from non-personal data under the GDPR, International Data Privacy Law 2020, 11 (13); siehe auch: *Hödl* in Knyrim (Hrsg), DatKomm Art 4 DSGVO RN 9 (Stand 1.12.2018).

schritts wurden Standortdaten und Online-Kennung in die Liste mitaufgenommen, welche zur Identifizierbarkeit einer betroffenen Person beitragen.[17]

Informationen müssen sich auf eine natürliche Person beziehen, mit ihr in Verbindung stehen oder von ihr abstammen. Die Informationen müssen geeignet sein, eine Person zu identifizieren oder identifizierbar zu machen. Die Feststellung, wann eine Person identifizierbar ist, ist bereits ein weiterer Prüfschritt, der damals wie heute mit Hilfe von Erwägungsgrund 26 ermittelt werden muss.[18]

2.2 Erwägungsgrund 26 DS-RL

Erwägungsgründe zu Gemeinschaftsrechtsakten sind Erklärungen im Sinne von Erläuterungen zu einzelnen Bestimmungen. Sie sind integraler Bestandteil europäischer Rechtsvorschriften, ohne Teil des Normtextes zu sein. Sie beinhalten weder Tatbestandsmerkmale noch Rechtsfolgen und haben im Gegensatz zum Richtlinien- und Verordnungstext, selbst keine Rechtswirkung. Dennoch werden sie unter anderem von Gerichten zur Begründung von Entscheidungen und in der Praxis, Forschung und Lehre als Definitionsmerkmal herangezogen.[19]

In Erwägungsgrund 26 der DS-RL wird der Prüfschritt der Identifizierbarkeit mit „*allen Mitteln*“ verknüpft, die berücksichtigt werden müssen und die „[...] *vernünftigerweise entweder von einem für die Verarbeitung Verantwortlichen oder einem Dritten* [...]*“* verwendet werden könnten, um eine Person zu identifizieren. Die Artikel-29-Datenschutzgruppe führte in ihrer Stellungnahme dazu aus, dass eine rein hypothetische Möglichkeit, aufgrund der DS-RL, nicht ausreiche um eine Person zu bestimmen und somit diese als *„bestimmbar“* anzusehen. Grundlegendes Kriterium sind „*alle Mittel“* die zu berücksichtigen sind, welche *„vernünftigerweise“* von dem *„Verantwortlichen oder einem Dritten“* benutzt werden um eine Person zu bestimmen. Wenn diese Mittel nicht vorliegen, kann eine Person nicht be-

[17] *Klabunde* in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] Art 4 Z 1 Rz 15 (2017).
[18] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 261.
[19] *Paal/Pauly,* in Paal/Pauly (Hrsg), Datenschutz-Grundverordnung (2017); Siehe zur rechtlichen Qualität von Erwägungsgründen: EuGH 19.06.2014, C‑345/13 (Karen Millen Fashions Ltd.) Rz 31; EuGH 13.09.2018, C-287/17 (Ceska pojistovna a.s.) Rz 33; siehe auch: EuGH 24.11.2005, C-136/04 (Deutsches Milch-Kontor GmbH) Rz 32.

stimmt werden und somit auch nicht bestimmbar sein.[20] Damit eine natürliche Person als bestimmbar angesehen werden kann, muss die Möglichkeit der Identifizierung gegeben sein. Dies ergibt sich bereits aus dem Wortteil "bar".[21] Fraglich ist, ob ein Name bereits als bestimmt oder bestimmbares Merkmal gilt. Je nach den Umständen kann ein Name bereits so eindeutig sein, dass damit eine Person bestimmt ist, es kann aber auch nur ein bestimmbares Merkmal sein, wenn ein Name nur mit zusätzlichen Informationen zur einer Identifizierbarkeit einer Person führen kann.[22] Ein Beispiel: Sebastian Kurz ist Bundeskanzler der Republik Österreich. Der Bundeskanzler ist namentlich unmittelbar identifiziert. Ohne Namen ist er identifizierbar, da es nur einen Bundeskanzler in Österreich gibt.

Der Begriff "vernünftigerweise" wurde aus der englischen Fassung der DS-RL von "reasonably likely" übersetzt. Übersetzt man „reasonably likley“ bekommt man unter anderem Synonyme wie "relativ wahrscheinlich“, ziemlich wahrscheinlich", "wahrscheinlich" oder "mit hoher Wahrscheinlichkeit".[23] Die damalige Übersetzung mit "vernünftigerweise" führte dazu, dass eine Prognoseentscheidung der Mittel im Sinne einer risikobasierten Bewertung mit Kriterien der Vernunft verbunden wurde.[24] Umgekehrt bedeutet dies, dass rechtlich nicht zugelassene Mittel nicht vernünftigerweise eingesetzt werden, denn illegale Mittel einzusetzen kann nicht mit einem vernünftig handelnden Maßmenschen gleichgesetzt werden. Es geht viel mehr um die tatsächliche Wahrscheinlichkeit, mit welchen Mitteln eine Person identifiziert werden kann, aber es entbehrt jeglicher Lebenserfahrung, wenn davon ausgegangen wird, dass der Einsatz illegaler Mittel nicht zur Identifizierung einer Person genutzt wird. De facto würde diese Annahme bedeuten, dass der Verantwortliche, wenn er sich illegal Informationen beschafft, um einen Personenbezug herzustellen, keine Datenschutzverletzung begeht, da die Daten für ihn faktisch anonym wären.[25] Dies

[20] *Art-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff »personenbezogene Daten« WP 136 01248/07/DE, 17 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_de.pdf>. (letzter Aufruf 09.08.20).
[21] *Art-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff »personenbezogene Daten« WP 136 01248/07/DE, 14 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_de.pdf>. (letzter Aufruf 09.08.20).
[22] *Art-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff »personenbezogene Daten« WP 136 01248/07/DE, 15 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_de.pdf>. (letzter Aufruf 09.08.20).
[23] <https://www.deepl.com/translator#en/de/reasonably%20likely%7Cziemlich%20wahrscheinlich> (letzter Aufruf 25.10.20).
[24] *Haase*, Datenschutzrechtliche Fragen des Personenbezugs (2015) 263; *Kotschy*, Replik zu den Anmerkungen von Dietmar Jahnel zu den Auswirkungen der Vorabentscheidung des EuGH 19. 10. 2016, C-582/14 (Breyer) auf den Begriff der "personenbezogenen Daten" nach § 4 Z 1 DSG 2000, jusIT 2017, 27 (29).
[25] *Kotschy*, Replik zu den Anmerkungen von Dietmar Jahnel zu den Auswirkungen der Vorabentscheidung des EuGH 19. 10. 2016, C-582/14 (Breyer) auf den Begriff der "personenbezogenen Daten" nach § 4 Z 1 DSG 2000, jusIT 2017, 27 (29).

wiederum würde das geltende Datenschutzrecht ad absurdum führen, da die Beschaffung von Informationen im Sinne einer Verarbeitung[26], die sich auf eine natürliche Person beziehen, schon damals wie heute einer Rechtsgrundlage bedarf. Da eine strafbare Handlung zur Erhebung personenbezogener Daten niemals eine Rechtsgrundlage für deren Verarbeitung sein kann, kann es nicht die Absicht des Gesetzgebers gewesen sein, dass die Verarbeitung der rechtswidrig erlangten Daten wiederum keiner Rechtsgrundlage nach europäischem Datenschutzrecht für die Verarbeitung personenbezogener Daten erfordert.

Es sind die Mittel zu betrachten, die von dem für die Verarbeitung Verantwortlichen oder einem Dritten zur Identifizierung verwendet werden könnten. Unter einem Dritten kann jede juristische oder natürliche Person verstanden werden, die nicht der Verantwortliche oder die betroffene Person ist.[27] Durch die Angabe eines Dritten, zusätzlich zum Verantwortlichen, wird indiziert, dass es nicht nur auf die Fähigkeiten und Möglichkeiten des Verantwortlichen allein ankommt.[28]

Die Schutzprinzipien sollen nicht auf Daten anwendbar sein, die aufgrund der Anonymisierung keinen Bezug mehr zu einer Person enthalten. Der Erwägungsgrund selbst setzt eine Unmöglichkeit der Identifizierbarkeit voraus. Dies impliziert der letzte Satz *„*[...] *Die Verhaltensregeln im Sinne des Artikels 27 können ein nützliches Instrument sein, mit dem angegeben wird, wie* ***sich die Daten in einer Form anonymisieren*** *und aufbewahren lassen,* ***die die Identifizierung der betroffenen Person unmöglich macht****."* [Hervorhebungen durch die Verfasserin] Im Erwägungsgrund selbst wird allerdings nicht definiert, welcher Vorgang zur einer tatsächlichen unumkehrbaren Anonymisierung führen soll.[29] Eine Unmöglichkeit impliziert einen absoluten Anspruch. Die Unmöglichkeit der Identifizierbarkeit kann rechtlicher oder technischer Natur sein. Die rechtliche Unmöglichkeit der Identifizierbarkeit beruht auf der Auslegung des Gesetzes. Die Verarbeitung von anonymen oder anonymisierten Daten fällt nicht in den Anwendungsbereich der DSGVO. Dies ist ein

[26] Siehe Art 4 Z 2 VO (EU) 2016/679 „Verarbeitung" 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;"

[27] *Haase*, Datenschutzrechtliche Fragen des Personenbezugs (2015) 262.

[28] *Pahlen-Brandt*, Datenschutz braucht scharfe Instrumente Beitrag zur Diskussion um „personenbezogene Daten", DuD (2008), 34 (38).

[29] *Art-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken WP 216 0829/14/DE, 6 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf> (letzter Aufruf 20.07.20).

rechtliches Faktum. Etwas kann nach einer rechtlichen Definition unmöglich sein, aber faktisch möglich. Ein anonymer Datensatz kann rechtlich unmöglich zu einer Identifizierbarkeit einer natürlichen Person führen, aber technisch möglich sein.

Der europäische Gesetzgeber wählte hier bewusst einen Ansatz der Möglichkeiten offen ließ, insbesondere für Gegebenheiten, die nach der DS-RL nicht vorhersehbar waren. Wie er allerdings selbst erkannte, löste dieser Ansatz eine weitverbreitete Unsicherheit aus, wann, wer, wo, und wie der Datenschutz einzuhalten ist.[30] Der europäische Datenschutzbeauftragte wies im Jahr 2011 in seiner Stellungnahme zum Gesamtkonzept des Datenschutzes in der Europäischen Union darauf hin, dass sich die Technologie kontinuierlich und unaufhaltsam weiterentwickelt. Die Europäische Union müsse daher einen rechtlichen Rahmen schaffen, der diesen Fortschritt berücksichtigt und auch nach Jahren rechtliche Gültigkeit haben kann, womit eine technologieneutrale Regelung geschaffen werden muss. Allerdings sind diese in Einklang zu bringen mit einem Rahmen der Rechtssicherheit für Datenverarbeiter und Betroffene, weshalb die Regelungen *„präzise“* sein müssen.[31]

2.3 Erwägungsgrund 26 DSGVO

Erwägungsgrund 26 der DSGVO lautet wie folgt: *„Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürli-*

[30] MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM (2010) 609 endg.

[31] *Der Europäische Datenschutzbeauftragte*, Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen — „Gesamtkonzept für den Datenschutz in der Europäischen Union“ (2011/C 181/01), RN 38 <https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_de.pdf> (letzter Aufruf 21.07.20).

chen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.“[32]

Der erste Satz ist im wesentlichen inhaltsgleich mit dem in Erwägungsgrund 26 der DS-RL. Im Gegensatz zum Erwägungsgrund 26 der DS-RL bezieht sich Erwägungsgrund 26 der DSGVO auf die Pseudonymisierung, die seinerzeit in der DS-RL selbst nicht enthalten war.

Die Formulierung "vernünftigerweise" ist in der englischen Textfassung gleich geblieben ("reasonably likely"), allerdings wurde die deutsche Version richtigerweise (wie weiter oben dargelegt) nicht mehr mit "vernünftigerweise" übersetzt. Der dritte Satz des Erwägungsgrund 26 der DSGVO lautet *„[u]m festzustellen, ob eine natürliche Person identifizierbar ist, sollten **alle Mittel** berücksichtigt werden, die **von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt** werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern.“* [Hervorhebungen durch die Verfasserin]. Wie bereits im Erwägungsgrund 26 der DS-RL festgehalten, soll das Wissen Dritter im Sinne einer anderen Person in die Bestimmung der Identifizierbarkeit einbezogen werden.[33] Nach dem Wortlaut kann eine andere Person eine juristische oder natürliche Person sein, die nicht der für die Datenverarbeitung Verantwortliche oder die betroffene Person selbst ist.

Im Gegensatz zur DS-RL wird in Erwägungsgrund 26 der DSGVO näher auf die Mittel eingegangen, die für die Ermessensentscheidung einzubeziehen sind. So heißt es: „*Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten **alle objektiven Faktoren**, wie die **Kosten der***

[32] ErwGr 26 (EU) 2016/679.
[33] *Krügel*, Das personenbezogene Datum nach der DS-GVO, ZD 2017, 455 (456).

Identifizierung *und der* ***dafür erforderliche Zeitaufwand****, herangezogen werden, wobei die* ***zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen*** *zu berücksichtigen sind."* [Hervorhebungen durch die Verfasserin] Wie viel Zeitaufwand und Kosten ist nach allgemeinen Ermessen zur Informationsbeschaffung wahrscheinlich? Was darf eine Datenabfrage kosten und wie viel Zeit dafür aufgewendet werden? Diese Fragen wurden bisher in der Rechtsprechung nicht explizit beantwortet, weshalb diese Merkmale zwar eine Hilfestellung bieten, aber in der Praxis wenig tauglich sind.

Neu ist auch die Einbeziehung von technologischen Entwicklungen. Dies zeigt, dass im Gegensatz zur DS-RL der technologische Fortschritt in den Fokus des Gesetzgebers gerückt ist.[34] Erwägungsgrund 26 bezieht sich auf die Technologien die zum Zeitpunkt der Verarbeitung verfügbar sind und technologische Entwicklungen. Diese Einschränkung auf die zum Zeitpunkt der Verarbeitung verfügbaren Technologien, stellt einen Versuch dar, eine zeitliche Begrenzung zu schaffen, da ansonsten weit in der Zukunft liegende Technologien berücksichtigt werden müssten.[35] Eine Vorschau in die Zukunft, in der alle Aspekte der technologischen Entwicklung bei der Bestimmung des Anwendungsbereichs des Datenschutzrechts berücksichtigt werden, ist realitätsfern. Dennoch können zukünftige verfügbare Technologien und Forschungsergebnisse, die kurzfristig zugänglich sind und nach dem Vernunftprinzip mit aller Wahrscheinlichkeit erwartet werden können, nicht völlig ignoriert werden.[36] Zudem verlangt der Telos des Datenschutzrechts den Missbrauch von Daten und das nicht nur im Hier und Jetzt, sondern auch im Hinblick auf Datenverarbeitungen in der Zukunft zu verhindern, was bedeutet, dass bei der Prognose des Anwendungsbereichs die noch nicht vorherrschenden Umstände berücksichtigt werden müssen. Artikel 1 DSGVO lässt eine zeitliche Begrenzung im Sinne des Datenschutzes nur in der Gegenwart nicht erkennen.[37] Es erfordert allerdings ein erhebliches Fachwissen im technischen Bereich, welche Technologien derzeit und in Zukunft für eine bestimmte Verarbeitung zur Verfügung stehen.[38]

2.4 Vergleich und Schlussfolgerung

[34] *Krügel*, Das personenbezogene Datum nach der DS-GVO, ZD 2017, 455 (456).
[35] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 313 f.
[36] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 313 f.
[37] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 314.
[38] *Krügel*, Das personenbezogene Datum nach der DS-GVO, ZD 2017, 455 (456).

Anders als in der letzten und in Geltung stehenden Fassung der DSGVO wurde ein Versuch einer Definition anonymer Daten im Bericht über den Vorschlag der DSGVO weitaus öfters in den Erwägungsgründen und Artikeln erwähnt.[39] Der Versuch einer Definition von anonymen bzw. anonymisierten Daten in dem Erwägungsgrund, wie auch bereits in der DR-RL, zu formulieren und nicht in den Gesetzestext aufzunehmen, gibt einerseits den Nutzern mehr Spielraum für Interpretationen und schafft andererseits Unsicherheit hinsichtlich der Frage, wann Daten als anonym oder anonymisiert im Sinne der DSGVO gelten. Hätte man eine Definition von anonymisierten Daten in den Normtext aufgenommen, wäre diese festgehaltene Definition rechtsverbindlich. Auch Normen unterliegen der Auslegung durch Anwender und Gerichte. Ob dies mehr Rechtssicherheit schaffen würde, ist zu bezweifeln, denn eine Legaldefinition zu erarbeiten, die alle Aspekte der Verarbeitung zu jeglichem Zweck abdeckt und die in ihrer Gültigkeit mit dem gesellschaftlichen und technischen Wandel mithalten kann, erscheint als schier unlösbare Aufgabe.

3. Perspektive der Bestimmbarkeit

Es gibt immer noch eine anhaltende Debatte darüber, ob der relative oder objektive Ansatz zur Bestimmung des Personenbezugs gewählt werden sollte. Beide Theorien haben den Anknüpfungspunkt in der Perspektive. Der Unterschied liegt darin, "wie" und "von wem" es möglich ist, zusätzliche Informationen zu erhalten, die die verarbeitende Stelle nicht bereits hat. Beiden Auffassungen ist jedenfalls gemeinsam, dass ein Personenbezug gegeben ist, wenn die verarbeitende Stelle diesen selbst vornehmen kann.[40]

3.1 Der relative Ansatz

Personen, die den strengen relativen Ansatz verfolgen, sind jedenfalls der Meinung, dass ein Datensatz für eine verarbeitende Stelle anonym sein kann oder ist, für die andere aber nicht.[41] Diese Theorie des relativen Personenbezugs baut auf der Tatsache auf, dass es nur auf die Perspektive der verarbeitenden Stellen ankommt. Die Tatsache, dass nur Datenverarbeiter ihren vorhandenen Informationsstand kennen und daher realistisch ein-

[39] *Europäisches Parlament*, BERICHT über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) - (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 61, 213, 314, 337, 357, 512, 632 <https://www.europarl.europa.eu/doceo/document/A-7-2013-0402_DE.pdf> (letzter Aufruf 21.07.20).
[40] *Ziebarth*, in Sydow (Hrsg), Europäische Datenschutz-Grundverordnung[2] Rz 33, 34 (2018).
[41] *Ziebarth*, in Sydow (Hrsg), Europäische Datenschutz-Grundverordnung[2] Rz 36 (2018).

schätzen können, ob „[...] *alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden* [...]*"*[42], verhindert nach Ansicht mancher eine Ausweitung des Anwendungsbereichs des Datenschutzrechts.[43] Diesem strengen relativen Ansatz widerspricht jedoch die Tatsache, dass im Erwägungsgrund 26 der DSGVO sowie bereits im Erwägungsgrund 26 der DS-RL die wahrscheinlich verwendeten Mittel einer anderen Person ausdrücklich erwähnt werden und zur Beurteilung herangezogen werden sollten.[44] Interpretiert man den Wortlaut des Erwägungsgrundes 26 der DSGVO, so liegt es auf der Hand, dass der verarbeitenden Stelle nicht nur solche Mittel zugerechnet werden können, deren Verwendung in ihrer Sphäre sind. Vielmehr ergibt sich aus diesem, dass auch die Mittel eines Dritten, im Sinne jeder anderen Person, der verarbeitenden Stelle zugerechnet werden müssen, die diese wahrscheinlich zur Identifizierung einer Person heranzieht.[45] Der Gesetzgeber hat die Definition des Begriffs "Dritter" (Artikel 4 Z 10 DSGVO) eben nicht herangezogen, sondern *"jede andere Person"* in den Erwägungsgrund aufgenommen und damit zum Ausdruck gebracht, dass darunter andere Verantwortliche, Auftragsverarbeiter und betroffene Person ebenfalls fallen können.[46] Diese strenge relative Sichtweise wird kaum noch verfolgt. Diejenigen, die den relativen Ansatz befürworten, beziehen auf die eine oder andere Art das Wissen Dritter, im Sinne jeder anderen Person, in ihre Überlegungen mit ein.[47] Nach dieser Auffassung kommt es auf das zurechenbare Wissen eines Dritten an, allerdings nur nach dem Grundsatz, dass nur solche Mittel berücksichtigt werden, die nach allgemeinem Ermessen von einer anderen Person wahrscheinlich genutzt werden.[48]

3.1.1 Die anonymisierende Wirkung der Pseudonymisierung

Die Pseudonymisierung ist eine Verarbeitung personenbezogener Daten in der Weise, dass Daten nur mit Hilfe zusätzlicher Informationen, einer betroffenen Person zugeordnet

[42] ErwGr 26 VO (EU) 2016/679.
[43] *Haase*, Datenschutzrechtliche Fragen des Personenbezugs (2015) 297; *El Emam*, Guide to the De-Identification of Personal Health Information (2013) 147; *Hornung*, Die digitale Identität (2005) 142 ff.
[44] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 297 f; *Bergauer/Gosch*, Die Pseudonymisierung personenbezogener Daten gemäß der DSGVO - zugleich eine Replik auf Geuer/Wollmann, Verarbeitung von pseudonymen Daten mit besonderem Fokus auf Art 26 und 28 DS-GVO, jusIT 2020 63 (65).
[45] *Arning/Forgó/Krügel,* Datenschutzrechtliche Aspekte der Forschung mit genetischen Daten, DUD (2006) 700 (704).
[46] *Bergauer/Gosch*, Die Pseudonymisierung personenbezogener Daten gemäß der DSGVO - zugleich eine Replik auf Geuer/Wollmann, Verarbeitung von pseudonymen Daten mit besonderem Fokus auf Art 26 und 28 DS-GVO, jusIT 2020 63 (65); *Haase*, Datenschutzrechtliche Fragen des Personenbezugs (2015) 298.
[47] *Haase*, Datenschutzrechtliche Fragen des Personenbezugs (2015) 298.
[48] *Haase*, Datenschutzrechtliche Fragen des Personenbezugs (2015) 304.

werden können.[49] In der DSGVO ist die Pseudonymisierung von Daten eine Datensicherheitsmaßnahme, um *„ein dem Risiko angemessenes Schutzniveau“* bei der Verarbeitung von personenbezogenen Daten durch den Verantwortlichen und Auftragsverarbeiter *„zu gewährleisten“*.[50] Folglich wird die Pseudonymisierung in Artikel 25 Abs. 1 DSGVO als ein Verfahren zur Realisierung des Privacy by Design normiert. Die Definition im Artikel 4 Z 15 DSGVO schreibt vor, dass die Pseudonymisierung *„eine Verarbeitung* [...] *personenbezogener Daten“* ist *„in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifzierten oder identifizierbaren natürlichen Person zugewiesen werden“* kann.[51] Der erste Teil des Satzes definiert bereits die Pseudonymisierung als eine gesonderte Verarbeitung und nicht als eine besondere Form personenbezogener Daten. Auch wenn ein Datum oder ein Datensatz pseudonymisiert worden ist und damit als personenbezogen betrachtet wird, ist die Pseudonymisierung an sich keine eigenständige Datenkategorie.[52] Auch die österreichische Datenschutzbehörde (DSB) stellte in einer ihrer Entscheidungen aus 2018 fest, dass die Pseudonymisierung eine Maßnahme zur Datensicherheit ist.[53] In einer Entscheidung aus dem Jahr 2019 stellte die DSB zudem fest, dass sich durch die Pseudonymisierung der Bezug zu einer Person nicht ändert, da es sich nur um einen Verarbeitungsschritt handelt, es bei der Pseudonymisierung aber genau darum geht, dass eine Rückverfolgbarkeit zu einer Person noch möglich ist.[54] Dieser Ansatz wurde bereits von der Artikel-29-Datenschutzgruppe in ihrer Stellungnahme zu den Anonymisierungstechniken vertreten. Die Pseudonymisierung stellt keinen Anonymisierungsvorgang dar. Sie erschwert lediglich die Verknüpfung eines Datensatzes mit der tatsächlichen Identität einer betroffenen Person.

---

[49] Art 4 Z 5 (EU) 2016/679.
[50] Art 32 VO (EU) 2016/679.
[51] *Finck/Pallas*, They who must not be identified-distinguishing personal from non-personal data under the GDPR, International Data Privacy Law 2020, 11 (21).
[52] *Bergauer/Gosch*, Die Pseudonymisierung personenbezogener Daten gemäß der DSGVO - zugleich eine Replik auf Geuer/Wollmann, Verarbeitung von pseudonymen Daten mit besonderem Fokus auf Art 26 und 28 DS-GVO, jusIT 2020 63 (64); *Gosch*, Pseudonymisierung und Verschlüsselung sensibler Daten, jusIT 2019, 107 (108); *Art-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken WP 216 0829/14/DE, 8 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf> (20.07.20).
[53] DSB 13. 09. 2018, DSB-D123.070/0005-DSB/2018.
[54] DSB 14. 01. 2019, DSB-D123.224/0004-DSB/2018.

Die anonymisierende Wirkung der Pseudonymisierung soll nun darin bestehen, dass bei der Übermittlung eines pseudonymisierten Datensatzes an eine andere Person, diese keine Zuordnung vornehmen kann, da diese den Schlüssel nicht habe und somit für diese Person der Datensatz anonymisiert ist.[55] Dieser generellen Annahme muss entgegengehalten werden, dass die Qualität des Datensatzes nicht in diese Überlegungen einbezogen wird. Die bloße Ersetzung eines identifizierenden Merkmals durch eine Identifikationsnummer im Sinne eines Schlüssels schließt nicht aus, dass jemand eine betroffene Person identifizieren kann, wenn der Datensatz weitere identifizierende Merkmale enthält, sowie deren Kombination, eine Re-Identifizierung ermöglichen.[56] Die anonymisierende Wirkung der Pseudonymisierung kann keine Rechtssicherheit schaffen. Der Erwerb von Zusatzwissen, sei es durch Internetrecherchen, öffentliche Datenbanken, soziale Netzwerke, kann die Sachlage und damit die Möglichkeit der Re-Identifizierung jederzeit ändern. Einhergehend mit der Theorie der anonymisierenden Wirkung der Pseudonymisierung ist nach mancher Ansicht, in diesem Fall, weder ein Vertrag über die gemeinsame Verantwortung noch ein Auftragsverarbeitervertrag abzuschließen.[57] Diese Auffassung widerspricht dem Telos der DSGVO, insbesondere den Artikeln 26 und 28, da es bei diesen Bestimmungen gerade darum geht, Datenverarbeiter stärker in die Verantwortung zu nehmen und sie zu verpflichten sich mit dem Datenschutz auseinanderzusetzen.

Die Artikel-29-Datenschutzgruppe selbst nennt in ihrer Stellungnahme mehr Beispiele für die Herstellung eines pseudonymisierten Datensatzes, als nur die Trennung von personenbezogenen Daten und zusätzlichen identifizierenden Informationen. Ein Beispiel ist die Verschlüsselung eines Datensatzes mit einem geheimen Schlüssel. Beim Verschlüsseln im Sinne eines technischen Verfahrens wird ein lesbarer Text (Klartext) oder auch andere Formen von Informationen, wie z. B. Ton- oder Bildaufnahmen, in eine unlesbare, nicht leicht deutbare, Zeichenfolge (Geheimschrift) transformiert.[58] Ein Datensatz gilt als verschlüsselt, wenn er nur mit einem bestimmten Schlüssel entschlüsselt werden kann. Der Schlüssel verbleibt beim Inhaber des Datensatzes. Der Schlüssel ermöglicht die Ent-

[55] *Haimberger/Geuer,* Anonymisierende Wirkung der Pseudonymisierung, Dako 2018, 57 (59); *Arning/Forgó/Krügel,* Datenschutzrechtliche Aspekte der Forschung mit genetischen Daten, DUD (2006) 700 (702).
[56] *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, 0829/14/DE, 26 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf> (letzter Aufruf 24.01.2021);
[57] *Geuer/Wollmann*, Verarbeitung von pseudonymen Daten mit besonderem Fokus auf Art 26 und 28 DSGVO, jusIT 2020, 18 (23).
[58] *Ernestus*, in Simitis (Hrsg), Kommentar zum Bundesdatenschutzgesetz[8] § 9 Rz 166 (2014).

schlüsselung, aber der Inhalt des Datensatzes selbst wurde nicht verändert.[59] Bei der Verschlüsselung werden personenbezogene Daten derart verarbeitet, dass der Inhalt der Daten (also im Klartext) ohne Hinzufügung zusätzlicher Informationen (in diesem Fall des Schlüssels) nicht mehr einer Person zugeordnet werden kann, sofern der Schlüssel getrennt und ausreichend sicher verwahrt wird.[60] Somit kann die Verschlüsselung eines Datensatzes als eine Pseudonymisierungsmethode angesehen werden, auch wenn diese nicht unter die Definition in Artikel 4 Z 5 DSGVO fällt.[61] Der Unterschied zur definierten Pseudonymisierung in der DSGVO besteht darin, dass selbst bei der Erlangung von zusätzlichem Wissen (mit solchen Mitteln, die nach allgemeinem Ermessen wahrscheinlich verwendet werden) oder wenn der verschlüsselte Datensatz bereits so viele identifizierende Merkmale enthält und deren Kombination eine Re-Identifizierung ermöglicht, diese Informationen den Datenverarbeitern des verschlüsselten Datensatzes nichts im Bezug auf eine Re-Identifizierung nutzen. Das Zusatzwissen besteht ausschließlich in Form des Entschlüsselungsmechanismus. Auch hier kommt es darauf an, ob dieses Zusatzwissen nach den Kriterien des Erwägungsgrundes 26 der DSGVO erlangt werden kann. In jedem Fall ist die Möglichkeit, dieses sehr spezifische Zusatzwissen zu erlangen, erschwert.

Im Safe-Harbor-Abkommen aus 2000 vertrat die Europäische Kommission die Meinung, dass die Übermittlung von verschlüsselten Forschungsdaten in die USA kein Export personenbezogener Daten ist, wenn der Schlüssel nicht mit den Daten offengelegt oder übermittelt wird.[62] Diese Ansicht bedingt die Annahme, dass ein verschlüsselter Datensatz für den Empfänger nicht personenbezogen ist. Im Gegensatz dazu führt der Europäische Datenschutzausschuss (EDSA) in seiner Empfehlung zu Maßnahmen, die bei der Übermittlung von Daten in Drittländer zu ergreifen sind (veröffentlicht im Jahr 2020), aus, dass, wenn „[...] ***personenbezogene[n] Daten*** *vor der Übermittlung* ***verschlüsselt*** *werden, und zwar mit einer Methode, die dem Stand der Technik entspricht und die für den gesamten Zeitraum, für den die Daten zu schützen sind, garantiert,* ***dass ohne Kenntnis des Ent-***

[59] *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, 0829/14/DE, 24 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf> (letzter Aufruf 24.01.2021); siehe auch: *Gosch*, Pseudonymisierung und Verschlüsselung sensibler Daten, jusIT 2019, 107 (108).
[60] *Gosch*, Pseudonymisierung und Verschlüsselung sensibler Daten, jusIT 2019, 107 (108).
[61] *Gosch*, Pseudonymisierung und Verschlüsselung sensibler Daten, jusIT 2019, 107 (108).
[62] ENTSCHEIDUNG DER KOMMISSION vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl 2000/215, 24.

schlüsselungsschlüssels *(End-to- End-Verschlüsselung)* ***keine Entschlüsselung möglich ist,"*** [Hervorhebungen durch die Verfasserin] dies eine effektive zusätzliche Maßnahme zur Ergänzung von Übermittlungsmechanismen sei.[63] Diese Ausführung untermauert die Annahme, dass die Verschlüsselung personenbezogener Daten eine Datensicherheitsmaßnahme im Sinne einer Pseudonymisierung ist und nicht dazu führt, dass diese beim Empfänger zu anonymisierten Daten werden. Dies würde sonst dem zu Folge bedeuten, dass nur der Übertragungsweg schutzwürdig ist, nicht jedoch der Datensatz an sich, was wiederum dem Grundsatz widerspricht, dass das durch die DSGVO gewährleistete Schutzniveau für natürliche Personen bei der Übermittlung ihrer Daten in Drittländer nicht untergraben werden darf.[64]

3.2 Der absolute Ansatz

Die absolute Anonymisierung erfordert einen wesentlich strengeren Ansatz und kann daher als die stärkste Form der Anonymisierung bezeichnet werden. Sie setzt voraus, dass niemand einen Personenbezug herstellen kann und dieser irreversibel ist.[65] Alle denkbaren insbesondere technologischen Bedingungen müssen in die Bewertung einbezogen werden.[66] Da Verantwortliche nicht wissen können, welches Zusatzwissen Dritte haben könnten, müssen diese sicherstellen, dass eine Re-identifikation auch mit Zusatzwissen unmöglich ist.[67]

Diejenigen, die Daten freigeben, können nie mit Sicherheit ausschließen, dass Dritte in der Lage sein könnten, die betroffenen Personen auf Grundlage ihres zusätzlichen Wissens zu identifizieren.[68] Es ist auch wahrscheinlich, dass in der Zukunft neue Datenverarbeitungstechniken entwickelt werden, die alle aktuellen Anonymisierungsprozesse beeinflussen können. Je mehr Datensätze für die Öffentlichkeit freigegeben werden (Stichwort "Open Data"), desto eher ist eine Verknüpfung zwischen Datensätzen wahrscheinlich, die

[63] *EDSA,* Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, 31.
[64] Art 44 VO (EU) 2016/679.
[65] *Ziebarth*, in Sydow (Hrsg), Europäische Datenschutz-Grundverordnung[2] RN 29 (2018).
[66] *Karg*, Anonymität, Pseudonyme und Personenbezug revisited?, DuD 2015, 520 (524).
[67] *Ziebarth*, in Sydow (Hrsg), Europäische Datenschutz-Grundverordnung[2] RN 29 (2018).
[68] *Finck/Pallas*, They who must not be identified-distinguishing personal from non-personal data under the GDPR, International Data Privacy Law 2020, 11 (19).

eine Identifizierbarkeit von Personen ermöglicht.[69] Werden anonymisierte Daten mit der Öffentlichkeit geteilt, ist die Anforderung, eine wirksame Anonymisierung zu gewährleisten, jedenfalls höher, da es praktisch unmöglich ist, die Veröffentlichung zurückzuziehen.[70] Die Anonymisierung kann, um dem absoluten Ansatz gerecht zu werden, nie als einmalige Aufgabe gesehen werden[71], da das zusätzliche Wissen Dritter, der technologische Stand und die technologischen Entwicklungen regelmäßig neu bewertet werden müssen.

3.3 Beispiel: IP-Adressen (IPv4-Adressen)

Die Frage, ob IP-Adressen als personenbezogene Daten zu qualifizieren sind, steht immer wieder im Mittelpunkt rechtlicher Diskussionen.[72] Die Beantwortung dieser Frage ist von maßgeblicher praktischer Bedeutung[73], da sowohl der relative Ansatz als auch der absolute Ansatz in einer Entscheidung des EuGH in Bezug auf IP-Adressen unterschiedlich interpretiert werden.

Statische IP-Adressen nehmen eine Sonderstellung ein, da sie in der Regel eine feste Verbindung zu einem bestimmten Netzwerkanschluss haben und damit eine Bestimmbarkeit der dahinter stehenden Person leichter möglich ist als bei dynamischen IP-Adressen.[74] Es wird ebenfalls die Meinung vertreten, dass eine Unterscheidung von statischen und dynamischen IP-Adressen im datenschutzrechtlichen Diskurs keinen Mehrwert hat, da Empfänger nicht zwischen statischer und dynamischer IP-Adresse unterscheiden können und daher durch den Telos des Datenschutzrechts immer unter die geltenden Datenschutzbestimmungen fällt.[75]

---

[69] *Data Protection Commission,* Guidance on Anonymisation and Pseudonymisation, 7 <https://www.dataprotection.ie/sites/default/files/uploads/2020-09/190614%20Anonymisation%20and%20Pseudonymisation.pdf> (letzter Aufruf 30.01.21).
[70] *Finck/Pallas*, They who must not be identified-distinguishing personal from non-personal data under the GDPR, International Data Privacy Law 2020, 11 (19).
[71] *Art-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken WP 216 0829/14/DE, 4 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf> (letzter Aufruf 30.01.21).
[72] *Heidrich/Wegener*, Datenschutzrechtliche Aspekte bei der Weitergabe von IP-Adressen, DuD 2010, 172 (173); *Venzke*, Die Personenbezogenheit der IP-Adresse Lange diskutiert und immer noch umstritten?, ZD 2011, 114.
[73] *Venzke*, Die Personenbezogenheit der IP-Adresse Lange diskutiert und immer noch umstritten?, ZD 2011, 114.
[74] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 382.
[75] *Voigt*, Datenschutz bei Google, MMR 2009, 377 (380).

Eine IP-Adresse ist eine Adresse, die auf dem Internetprotokoll aufsetzt. Sie wird dem Gerät, das mit dem Netzwerk verbunden ist, zugewiesen und ermöglicht so die Adressierung des Geräts. Sie dient dazu, Informationen vom Absender zum Empfänger zu transportieren. Durch die IP-Adressen wissen die verbundenen Router, wohin die Datenpakete zu übermitteln sind.[76] Ohne die Zuordnung der IP-Adresse des Rechners, wäre bei einem Aufruf einer Internetseite keine Verknüpfung möglich, da Seitenanbieter den Inhalt nicht den zugeordneten Rechner übermitteln könnten.[77]

Dynamische IP-Adressen werden aus einem „Pool" von im Moment nicht benutzten IP-Adressen herausgeholt und einem Rechner zugeordnet. Nach Verwendung werden diese in den Pool zurückgeworfen und wiederverwendet.[78] Nur der Access Provider oder der IP-Adressenverwalter (AS) hat die entsprechende Zuordnungsliste.[79]

Bei der Vergabe von statischen IP-Adressen handelt es sich um eine fixe Zuordnung zu einem Anschlussgerät (z.B. Router).[80] Heutzutage sind IP-Adressen, die grundsätzlich 32 Bit lang sind, ein knappes Gut, weshalb sie nicht mehr allzu oft als statische IP-Adressen vergeben werden. Da auch im privaten Bereich immer mehr DSL-Anschlüsse vergeben werden, kommen auch immer mehr Router zum Einsatz, denen über diesen mehrere Geräte in einem Haushalt zugeordnet werden können und so mit Hilfe des Proxys nach außen hin als eine IP-Adresse erscheinen. Vor allem Firmen und größere Institutionen nutzen Proxys. So können mehrere tausend Rechner mit der gleichen IP-Adresse im Internet auftreten.[81]

3.3.1 Zwischenfazit

Statische IP-Adressen, die vom Provider an natürliche Personen vergeben werden, sind rechtlich gleich zu behandeln wie dynamische IP-Adressen, da in beiden Fällen nur der Access-Provider die Möglichkeit der Zuteilung hat.[82]

---

[76] <https://de.wikipedia.org/wiki/IP-Adresse> (letzter Aufruf 19.12.2020).
[77] *Conrad/Hausen,* § 36 Datenschutz im Internet, in Auer-Reinsdorff/Conrad (Hrsg), Handbuch IT- und Datenschutzrecht (2019) RN 86.
[78] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 376.
[79] *Gerlach*, Personenbezug von IP-Adressen, CR 2013, 478.
[80] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 376.
[81] *Kirchberg-Lennartz/Weber*, Ist die IP-Adresse ein personenbezogenes Datum?, DuD 2010, 479.
[82] *Gerlach*, Personenbezug von IP-Adressen, CR 2013, 478 (481).

Eine IP-Adresse ist weltweit für einen bestimmten Zeitraum einem bestimmten Computer durch den Access-Provider zugeordnet.[83] Wenn eine IP-Adresse für eine Netzverbindung zugewiesen wird, wird ein Vertrag zwischen Zugangsanbietern und Endbenutzern geschlossen. Der Zugangsprovider muss immer zumindest den Namen und die Adresse der Kunden verarbeiten. Somit verarbeitet jedenfalls der Zugangsprovider personenbezogene Daten der Kunden, egal ob die IP-Adresse am Ende für mehrere Personen (ein Haushalt) benutzt wird oder nicht. Der Personenbezug wird bei jenen in Ausnahmefällen verneint, die die IP-Adresse gemeinsam nutzen und somit ohne Zusatzwissen nicht einer bestimmten oder bestimmbaren Person zuordenbar sind. Dieser Gedanke ist jedoch zu kurz gefasst, denn je nach den zusätzlichen Kenntnissen kann ein Personenbezug auch dann hergestellt werden, wenn ein Computer von mehreren Personen genutzt wird. Auch hier wird es darauf ankommen, welches Zusatzwissen nach allgemeinem Ermessen von wem zugeordnet werden kann.[84]

3.3.2 IPv6

Mit der Erschöpfung der IPv4-Adressen werden IPv6-Adressen zunehmend an Bedeutung gewinnen.[85] IPv6-Adressen sind zweiteilig aufgebaut bestehend aus dem Präfix (die Netzwerk Adresse) und der „Interface Identifier“ (Adresse des Endgeräts).[86] IPv6-Adressen sind 128 Bit lang. Es stehen also somit 2^{128} verschiedene IPv6-Adressen zur Verfügung, was bedeutend mehr als der Faktor vier ist.[87] Die Geräte-Adresse oder auch „MAC-Adresse“ genannt („Media-Access-Control-Adresse“) identifiziert jedes Gerät, das über einen entsprechenden Adapter an das Netzwerk angeschlossen ist.[88] Wie bei IPv4-Adressen kann die IP-Adresse nur von Zugangsanbietern zugewiesen werden, die ihrerseits nur die Anschlussbesitzer identifizieren können.[89] Selbst bei dynamischen IPv6-Adressen ändert sich die MAC-Adresse nicht. Sie bleibt statisch, auch wenn eine IPv6-Adresse neu zugewiesen wird. Die IPv6-Adresse stellt somit eine Neuerung gegenüber

[83] *Meyerdieks*, Sind IP-Adressen personenbezogene Daten? MMR 2009, 8 (9).
[84] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 381, 382; *Meyerdierks*, Sind IP-Adressen personenbezogene Daten? MMR 2009, 8 (9).
[85] *Heidrich/Forgó/Moos*, Kapitel 1 Datenschutz im Internet, in Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz (2019), RN 19 f.
[86] *Gerlach*, Personenbezug von IP-Adressen, CR 2013, 478 (482); *Wegener/Heidrich*, Neuer Standard - Neue Herausforderungen: IPv6 und Datenschutz, CR 2011, 479 (480).
[87] *Wegener/Heidrich*, Neuer Standard - Neue Herausforderungen: IPv6 und Datenschutz, CR 2011, 479.
[88] *Wegener/Heidrich*, Neuer Standard - Neue Herausforderungen: IPv6 und Datenschutz, CR 2011, 479 (481).
[89] *Wegener/Heidrich*, Neuer Standard - Neue Herausforderungen: IPv6 und Datenschutz, CR 2011, 479, (480).

der herkömmlichen IPv4-Adresse dar und liefert somit automatisch zusätzliche Informationen.[90] Bei der so genannten "Privacy Extension" ist es möglich, den "Interface Identifier" nicht aus der MAC-Adresse zu ermitteln, da in diesem Fall die Auswahl willkürlich erfolgt. Diese Funktion ist jedoch nicht in allen Betriebssystemen standardmäßig verfügbar.[91]

3.3.3 Zusatzwissen

Personenbezogene Daten sind Informationen, die Auskunft über eine identifizierte oder identifizierbare Person geben. Eine IP-Adresse allein ist eine einzigartige Zahlenkombination, die dazu dient, zwei Punkte (Websitebetreiber und Gerät) technisch miteinander zu verknüpfen. Sie wird prinzipiell einem Endgerät und nicht einer natürlichen Person zugewiesen.[92] Sich an dem Merkmal „Zahlenkombination“ festzuhalten und somit den Personenbezug zu verneinen ist allerdings zu kurzsichtig gedacht. Bei der Verarbeitung von IP-Adressen werden meist zusätzliche Informationen mitgesandt und gespeichert. Beim Aufruf einer Website werden generell die IP-Adresse des Rechners und die Abrufzeit (Datum, Stunde, Minute, Sekunde) für einen bestimmten Zeitraum gespeichert. Diese findet sich insbesondere in den sogenannten "Logfiles", die z.B. beim Zugriff auf eine Website hinterlegt werden.[93] Der Webseitenbetreiber bzw. Serviceprovider ist jedoch nicht verpflichtet, eine IP-Adresse zu speichern. In der Rechtssache La Quadrature du Net u. a bestätigt der Europäische Gerichtshof, dass IP-Adressen zur Verfolgung schwerer Straftaten und schwerwiegender Gefahren für die öffentliche Sicherheit ohne Anlass gespeichert werden dürfen, aber nicht müssen. Dies betrifft jedoch nur die IP-Adressen des jeweiligen Serviceproviders aber nicht die Adressen der aufgesuchten Webseiten.[94]

Informationen können auch von Endbenutzern selbst an die Websitebetreiber übermittelt werden (z.B. E-Mail-Adresse bei Newsletter Anmeldung). Die Übermittlung weiterer Informationen durch die Endnutzer selbst in Kombination mit einer statischen IP-Adresse gibt den Webseitenbetreibern jedoch die Möglichkeit, Informationen "permanent" zu sammeln und erhöht damit die Wahrscheinlichkeit, eine dahinter stehende natürliche Person zu

---

[90] *Wegener/Heidrich*, Neuer Standard - Neue Herausforderungen: IPv6 und Datenschutz, CR 2011, 479 (481).
[91] *Wegener/Heidrich*, Neuer Standard - Neue Herausforderungen: IPv6 und Datenschutz, CR 2011, 479 (481 f).
[92] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 379.
[93] *Heidrich/Wegener*, Datenschutzrechtliche Aspekte bei der Weitergabe von IP-Adressen, DuD 2010, 172; *Meyerdierks*, Sind IP-Adressen personenbezogene Daten? MMR 2009, 8 (9).
[94] EuGH 06.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net u. a) Rz 156 ff; *Thiele*, EuGH: Vorratsdatenspeicherung reloaded, jusIT (2020), 224 (225).

identifizieren.[95] Selbst dynamische IP-Adressen, die nur für einen kurzen Zeitraum vergeben werden, können zusätzliche Informationen zur Identifizierung einer natürlichen Person beitragen.[96] Vergleicht man die Informationsbeschaffungsmöglichkeiten einer staatlichen Behörde mit einem Online-Shop, so kann es für die Betreiber des Online-Shops sogar einfacher sein, die Identität der Käufer festzustellen, da diese in der Regel ihre eigenen Identifizierungsinformationen preisgeben und als Nutzer im Internet auftreten.[97]

3.3.4 Vorabentscheidung EuGH (Rechtssache Breyer)

Herr Breyer hatte auf mehrere Webseiten der deutschen Bundesregierung zugegriffen, die Informationen über Aufrufe in Logfiles speicherten. Zu diesen Informationen gehörte auch die dynamische IP-Adresse.[98] Der Fall Breyer wurde bereits 2016 heftig diskutiert und unter Fachleuten und Wissenschaftlern auch danach noch debattiert.[99] Insbesondere die Auseinandersetzung des EuGH mit der Personenbezogenheit von dynamischen IP-Adressen wurde unterschiedlich interpretiert. Die Tatsache, dass IP-Adressen ein personenbezogenes Datum seien, wurde bereits vom EuGH in der Rechtssache Scarlet Extended[100] erläutert. In diesem Fall stellte der EuGH fest, dass IP-Adressen „*geschützte personenbezogene Daten*" sind, weil sie eine „*genaue Identifizierung der Benutzer ermöglichen*". Die Sachlage in der Rechtssache Breyer ist jedoch eine andere, denn in diesem Fall erfolgte die Speicherung und Identifizierung von IP-Adressen durch den Internetzugangsprovider und nicht wie in der Rechtssache Scarlet Extended durch den Webseitenanbieter.[101]

Die dem EuGH vorgelegte erste Frage lautete: "*Mit seiner ersten Frage möchte das vorlegende Gericht wissen, ob Art. 2 Buchst. a der Richtlinie 95/46 dahin auszulegen ist, dass*

---

[95] *Gerlach*, Personenbezug von IP-Adressen, CR 2013, 478 (481).
[96] *Wegener/Heidrich*, Neuer Standard - Neue Herausforderungen: IPv6 und Datenschutz, CR 2011, 479 (480).
[97] *Wegener/Heidrich*, Neuer Standard - Neue Herausforderungen: IPv6 und Datenschutz, CR 2011, 479 (482).
[98] *Finck/Pallas*, They who must not be identified-distinguishing personal from non-personal data under the GDPR, International Data Privacy Law 2020, 11 (17); siehe auch: EuGH 19.10.2016, C-582/14 (Breyer).
[99] *Eckhardt*, EuGH: Dynamische IP-Adressen und die Grundsatzfrage zum Anwendungsbereich des Datenschutzrechts Der Grundsatz zur Bestimmung des sachlichen Anwendungsbereichs des Datenschutzrechts, ZIR 2017; *Jahnel,* EuGH: Dynamische IP-Adressen sind personenbezogene Daten, jusIT 2016; *Kotschy*, Replik zu den Anmerkungen von Dietmar Jahnel zu den Auswirkungen der Vorabentscheidung des EuGH 19. 10. 2016, C-582/14 (Breyer) auf den Begriff der "personenbezogenen Daten" nach § 4 Z 1 DSG 2000, jusIT 2017.
[100] EuGH 24.11.2011, C-70/10 (Scarlet Extended).
[101] EuGH 24.11.2011, C-70/10 Rz 51.

eine dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn nur ein Dritter - hier der Internetzugangsanbieter dieser Person - über die zu ihrer Identifizierung erforderlichen Zusatzinformationen verfügt.“[102]

Die vorgelegte Frage zielt nur auf das zusätzliche Wissen des Internetzugangsproviders ab. Sie berücksichtigt jedoch nicht den Umstand, dass zusätzliche Informationen (die in Verbindung mit der dynamischen IP-Adresse eine Ermittlung der Nutzer ermöglicht) auch im Besitz des Webseitenbetreibers oder eines Dritten sein könnten und somit ein Personenbezug hergestellt werden kann.[103]

Antwort des EuGH: *„Nach alledem ist auf die erste Frage zu antworten, dass Art. 2 Buchst. a der Richtlinie 95/46 dahin auszulegen ist, dass eine dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen.“*[104]

In diesem Fall bestätigt der EuGH implizit, dass nicht nur das Wissen der Verantwortlichen, sondern auch das der Dritten von Bedeutung ist, auch wenn es sich in diesem Fall um einen ganz bestimmten Dritten (Internetzugangsanbieter) handelte.[105]

Das Gericht bestätigte im Wesentlichen, dass, wenn die zusätzlichen Informationen, die zur Feststellung des Personenbezugs im Zusammenhang mit der IP-Adresse erforderlich sind, bei Anbietern nicht verfügbar sind, dies nicht ausschließt, dass es sich um ein perso-

[102] EuGH 19.10.2016, C-582/14 Rz 31.
[103] SCHLUSSANTRÄGE DES GENERALANWALTS MANUEL CAMPOS SÁNCHEZ-BORDONA vom 12. Mai 2016, Rechtssache C-582/14, Rz 60.
[104] EuGH 19.10.2016, C-582/14 Rz 49.
[105] *Finck/Pallas*, They who must not be identified-distinguishing personal from non-personal data under the GDPR, International Data Privacy Law 2020, 11 (18).

nenbezogenes Datum handelt. Es würde jedoch davon abhängen, welche Mittel von Anbietern vernünftigerweise zur Herstellung eines Personenbezuges eingesetzt werden.[106]

Es ist zu beachten, dass im Vorabentscheidungsverfahren die Verfahrenssprache immer jene Sprache ist, in welcher das nationale Gerichtsverfahren geführt wird.[107] Im vorliegenden Fall war das vorlegende Gericht ein Deutsches, so dass insbesondere die Schriftsätze, mündliche Vorbringen der Parteien, einschließlich der vorgelegten oder beigefügten Schriftstücke und Dokumente, in deutscher Sprache vorzulegen waren.[108] Nachdem die DS-RL in der deutschen Fassung den Begriff "vernünftigerweise" beinhaltet, fand dieser auch Eingang in die Entscheidung des EuGH und in die Schlussanträge des Generalanwalts.

Der Generalanwalt stellte in den Schlussanträgen fest, dass die vernünftigerweise verwendeten Mittel diejenigen sind, die eingesetzt werden, um bei jenem Dritten (mit der Betonung "in diesem Fall der Internetdienstanbieter"), an den man sich „*ebenfalls vernünftigerweise*" wenden würde, dann nicht als „*vernünftigerweise*" gelten, wenn die Einholung der Zusatzinformationen bei diesem bestimmten Dritten ein hohes Maß an personellen und finanziellen Ressourcen erfordern würde oder wenn es nicht durchführbar oder gesetzlich verboten wäre. Mit der Annahme des Generalanwalts postuliert er, dass eine Person „*vernünftigerweise*" nicht rechtswidrig handeln wird. Dabei fehlt es an jedweder Lebenserfahrung, dass "vernünftig" handelnde Personen niemals rechtswidrige Handlungen begehen. Wie in seiner Ausführung *„Das ist nicht der Fall, wenn der Kontakt mit diesen Dritten faktisch einen sehr hohen personellen und wirtschaftlichen Aufwand erfordern würde **oder** wenn er praktisch nicht durchführbar **oder** gesetzlich verboten wäre."*[109] [Hervorhebungen durch die Verfasserin] dargelegt, hängt es von der faktischen Möglichkeit unter Berücksichtigung der verfügbaren Ressourcen ab, nicht aber von der Tatsache, dass eine vernünftig handelnde Person niemals rechtswidrig handeln würde.[110] Der Gerichtshof wiederholt in seinem Urteil im Wesentlichen die Ansicht des Generalanwalts, dass *„vernünftigerweise verwendete Mittel"* nicht diejenigen umfassen, die gesetzlich verboten oder

[106] EuGH 19.10.2016, C-582/14 Rz 44, 45.
[107] Art 37 Abs 3 VerfO.
[108] Art 38 Abs 1 VerfO.
[109] SCHLUSSANTRÄGE DES GENERALANWALTS MANUEL CAMPOS SÁNCHEZ-BORDONA vom 12. Mai 2016, Rechtssache C-582/14, Rz 68.
[110] *Kotschy*, Replik zu den Anmerkungen von Dietmar Jahnel zu den Auswirkungen der Vorabentscheidung des EuGH 19. 10. 2016, C-582/14 (Breyer) auf den Begriff der "personenbezogenen Daten" nach § 4 Z 1 DSG 2000, jusIT 2017, 27 (29).

in der Praxis nicht durchführbar sind, wenn „*sie beispielsweise einen unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft erfordern würden, so dass das Risiko der Identifizierung de facto vernachlässigbar erscheint*". Der EuGH zählt zwei verschiedene Bedeutungen des Begriffs "vernünftigerweise" auf, nämlich zum einen, wenn ein gesetzliches Verbot besteht, ohne zu erwähnen, in welcher Form dieses gesetzliche Verbot bestehen muss und zum anderen die praktische Unmöglichkeit, einschließlich zeitlicher, personeller und finanzieller Ressourcen.[111] Dabei ist zu bedenken, dass eine Beschaffung von Zusatzinformationen auf illegalem Wege nicht als völlig unwahrscheinlich und damit praktisch nicht durchführbar abgetan werden kann.[112]

Das Urteil lässt Tendenzen zu beiden Theorien (relativer und absoluter Ansatz) zu. Auf der einen Seite wird das Wissen eines Dritten berücksichtigt, auf der anderen Seite wird es durch jene Mittel begrenzt, die vernünftigerweise zu erwarten sind, wobei objektive Faktoren miteinbezogen werden sollen. Keine der beiden Theorien wurde eindeutig verworfen.[113] Wann und für wen personenbezogene Daten als anonymisiert gelten, ist und bleibt eine Einzelfallentscheidung, bei der alle objektiven Faktoren berücksichtigt werden müssen. IP-Adressen waren und sind jedenfalls personenbezogen.

4. Die Verarbeitung personenbezogener Daten in der Forschung

Es liegt in der Natur der Sache, dass die medizinische Forschung auf die Verarbeitung von medizinischen Daten, insbesondere von Gesundheitsdaten sowie genetischen Daten, angewiesen ist und der medizinische Fortschritt ohne die gewonnenen empirischen Erkenntnisse nur begrenzt möglich ist.[114] Die Annahme, dass die wissenschaftliche Forschung mit anonymisierten Daten das Auslangen findet und kein Interesse an dem dahinterstehenden Individuum besteht, ist weitverbreitet. Abhängig von der Forschungsfrage und der angewendeten Untersuchungsmethode kann ein Personenbezug notwendig sein. Sollen in einer Studie Daten zu einer Person in Bezug gebracht werden, reichen anonymisierte Daten nicht aus (data matching oder record linking).[115] Querschnitts- und Langzeitstudien haben

[111] EuGH 19.10.2016, C-582/14 Rz 46.
[112] *Kotschy*, Replik zu den Anmerkungen von Dietmar Jahnel zu den Auswirkungen der Vorabentscheidung des EuGH 19. 10. 2016, C-582/14 (Breyer) auf den Begriff der "personenbezogenen Daten" nach § 4 Z 1 DSG 2000, jusIT 2017, 27 (29).
[113] *Ziebarth*, in Sydow (Hrsg), Europäische Datenschutz-Grundverordnung[2] RN 37 (2018).
[114] *Sorger,* Verwendung von Gesundheitsdaten im Lichte der §§ 46, in Jahnel (Hrsg), Jahrbuch Datenschutzrecht (2010) 194.
[115] *Pöttgen,* Medizinische Forschung und Datenschutz (2008) 22.

zum Ziel Daten zu einer Person zu erheben und zu verknüpfen. Querschnittsstudien vernetzen gesammelte Daten, die jeweils zu einem bestimmten Zeitpunkt erhoben wurden. In einer Längsschnittstudie werden Personen über einen längeren Zeitraum beobachtet und die entsprechenden Daten der untersuchten Person zugeordnet.[116] Die wissenschaftliche Forschung hat zwar meist zum Ziel einen nicht personenbezogenen Erkenntnisstand zu erreichen, der Weg dahin ist jedoch keinesfalls vom Datenschutz befreit.[117]

Obwohl die DSGVO in allen Mitgliedsstaaten unmittelbar anwendbar ist, sind bei der Verarbeitung personenbezogener Daten auf nationaler Ebene auch die einschlägigen Materiengesetze zu beachten. Neben dem österreichischen Datenschutzgesetz (DSG), welches Ergänzungen zur DSGVO enthält, sind die relevanten materienspezifischen Regelungen, die wiederum dem DSG vorgehen, ebenfalls heranzuziehen.[118] Die Auslegung der Anonymisierung wirft nicht nur auf EU-Ebene Fragen auf, auch in einzelnen österreichischen Gesetzen gibt es Wortfolgen, die eine Definition einer Anonymisierung andeuten, weshalb im Folgenden ausgewählte Bestimmungen erläutert werden.

5. Anonymisierung im § 7 DSG - Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke

Im Jahr 2017 beschloss der österreichische Gesetzgeber das Datenschutz-Anpassungsgesetz 2018, mit welchem das Datenschutzgesetz 2000 (DSG 2000) geändert wurde, zu erlassen. Damit sollten die in der DSGVO enthaltenen Öffnungsklauseln und die RL (EU) 2016/680[119] in nationales Recht umgesetzt werden. Die Bestimmung über die Verarbeitung von Daten für wissenschaftliche Forschungszwecke wurde im DSG 2000 in § 46 normiert.[120]

5.1 Indirekt personenbezogene Daten

[116] *Pöttgen,* Medizinische Forschung und Datenschutz (2008) 23.
[117] *Pöttgen*, Medizinische Forschung und Datenschutz (2008) 26.
[118] ErlRV 1164 BlgNR XXV. GP, 1.
[119] 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 2016/119, 89.
[120] § 46 DSG 2000.

Das DSG 2000 kannte den Begriff der “indirekt personenbezogenen Daten“. Gemäß § 4 DSG 2000 waren indirekt personenbezogene Daten solche, wenn für einen *“Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12)* [...] *der Personenbezug der Daten derart ist, daß dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;“.*[121] Diese indirekt personenbezogenen Daten, galten als personenbezogen. Die Verarbeitung solcher indirekt personenbezogene Daten, brachte den Verarbeitenden lediglich gewisse Erleichterungen bei der Verwendung eben dieser Daten.[122]

Mit der Novellierung des DSG 2000 wurde der Inhalt des § 46 DSG 2000 größtenteils in den § 7 DSG übernommen.[123] Der Begriff "indirekt personenbezogene Daten", der in § 46 Abs.1 Z 3[124] enthalten war, ist der DSGVO fremd und wurde daher nicht gänzlich in den § 7 DSG übernommen. Die Formulierung im Zusammenhang mit den rechtlich zulässigen Mitten wurde allerdings in leicht abgewandelter Form *(„des Betroffenen“* wurde zu *„der betroffenen Person“*) in § 7 Abs. 3 Z 1 DSG und weiteren österreichischen Paragraphen aufgenommen. Durch die Übernahme der Wortfolge *"die Identität der betroffenen Person mit rechtlich zulässigen Mitteln nicht bestimmen kann"*, in Bestimmungen die sich auf die Verarbeitung personenbezogener Daten beziehen, wird der Anwender verleitet, diese Bestimmungen im Lichte der vom EUGH geprägten *„rechtlichen Mittel"* [125] im Zusammenhang mit der Bestimmbarkeit des Personenbezugs, auszulegen.

5.2 § 7 Abs. 1 Z 3 DSG

*„Für im öffentlichen Interesse liegende Archivzwecke, **wissenschaftliche** oder historische **Forschungszwecke** oder statistische Zwecke, die **keine personenbezogenen Ergebnisse zum Ziel** haben, darf der **Verantwortliche** alle personenbezogenen Daten verarbeiten, die [...] **für ihn pseudonymisierte personenbezogene Daten** sind **und** der **Verant-***

[121] § 4 Z 1 DSG 2000.
[122] *Bergauer*, Indirekt personenbezogene Daten - datenschutzrechtliche Kuriosa, in Jahnel (Hrsg), Jahrbuch Datenschutzrecht (2011), 55 (56).
[123] *Medizinische Universität Wien*, Stellungnahme 3/SN-322/ME 25. GP 3.
[124] § 46 Abs 1 Z 3 DSG 2000 „Für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Auftraggeber der Untersuchung alle Daten verwenden, die [...] für den Auftraggeber nur indirekt personenbezogen sind.“
[125] EuGH 19.10.2016, C-582/14 (Breyer) Rz 49.

***wortliche die Identität der betroffenen Person mit rechtlich zulässigen Mitteln nicht bestimmen** kann.“*[126] [Hervorhebungen durch die Verfasserin]

Es ist erlaubt, gemäß § 7 Abs. 1 Z 3 DSG, personenbezogene Daten für wissenschaftliche Forschungszwecke zu verarbeiten, wenn das Ergebnis keinen Personenbezug („anonym“) hat, der Verantwortliche pseudonymisierte Daten verarbeitet und derselbe Verantwortliche die Identität des Betroffenen nicht mit rechtlich zulässigen Mitteln ermitteln kann.[127] "Kann" suggeriert, dass es nicht davon abhängt, ob er "darf", sondern nur von der realistischen Möglichkeit abhängt und zwar ohne dabei unzulässig rechtliche Mittel einzusetzen.[128] Für diese Variante spricht, dass mit der DSG-Novelle zu § 46 DSG 2000 die inkonsequente Terminologie entfernt und geklärt werden sollte, dass der „Auftraggeber", d.h. derjenige, der die wissenschaftliche Forschung durchführt, gemeint ist.[129] „*Nicht mit rechtlich zulässigen Mitteln*" könnte umgekehrt als Definition einer Anonymisierung interpretiert werden, da sie in Z 3 der Pseudonymisierung gegenübergestellt wird. Andererseits kann diese Wortwahl als Tatbestandsmerkmal gesehen werden, unter welchen Umständen es erlaubt ist Daten für wissenschaftliche Zwecke zu verarbeiten, ohne dass sie als Definition der Anonymisierung anzusehen ist. Die Verwirrung stammt wohl aus der Mischung der indirekt personenbezogenen Daten mit der neuen Definition einer Pseudonymisierung in der DSGVO, die eben keine Anonymisierung ist.[130]

Diese Mischung in der Bestimmung kann aufgrund des jetzigen Gesetzeswortlautes in zwei Richtungen interpretiert werden.

Einerseits könnte gemeint sein, dass es sich nicht um einen weiteren Verantwortlichen handeln soll, sondern um denselben - aufgrund eines Redaktionsfehlers und der Übernahme einer Definition aus einem alten Gesetz, welches nicht mehr kompatibel mit der Definition in der DSGVO ist. Andererseits könnte ein Dritter gemeint sein.[131] Wenn dies der Fall wäre, muss für den Dritten derselbe Datensatz anonym sein der für den Verantwortlichen pseudonymisiert ist, um den Voraussetzungen des § 7 Abs. 1 Z 3 zweiter Satz

[126] § 7 Abs 1 Z 3 DSG.
[127] § 7 Abs 1 Z 3 DSG.
[128] DSK 18.11.2009, K121.526/0028-DSK/2009.
[129] ErlRV 472 BlgNR XXIV. GP, 15.
[130] Stellungnahme der Datenschutzbehörde (17/SN-322/ME).
[131] *Gabauer,* Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken (2019) 107.

zu genügen, da dieser nicht einmal mit rechtlichen zulässigen Mitteln einen Personenbezug herstellen kann. Es ist nicht anzunehmen, dass dies tatsächlich beabsichtigt war, da dies einen möglichen Widerspruch zu den Artikeln 26 und 28 DSGVO erzeugt.

6. Gesundheitstelematikgesetz 2012 (GTelG 2012)

Der technische Fortschritt hat auch Eingang in die Patientendokumentation sowie in die automatisierungsgestützte Übertragung von Daten gefunden, die einen gewissen Sicherheitsstandard erfordert.[132] Der österreichische Gesetzgeber hat die Notwendigkeit einer bundesweit einheitlichen Regelung erkannt und das GTelG 2012 verabschiedet.[133] Das GTelG 2012 regelt die Verarbeitung personenbezogener Gesundheitsdaten und genetischer Daten (Artikel 4 Z 15 und Z 13 DSGVO) durch die im GTelG 2012 definierten Anbieter von Gesundheitsdienstleistungen.[134] Eines der Ziele war es unter anderem, die Bereiche Datenschutz und Patientenrechte zu stärken und Patienten die Möglichkeit zu geben die Verwendung ihrer Daten durch Protokolleinsicht zu überwachen und ihre medizinische Behandlung durch Erleichterung der Kommunikation über ELGA zu optimieren.[135]

6.1 ELGA

Der Terminus „ELGA“ steht für elektronischer Gesundheitsakt. Es ist nichts anderes als ein elektronisches Informationssystem, mit dem „ELGA-Gesundheitsdaten“[136] zwischen den Gesundheitsdienstleistern ausgetauscht bzw. von diesen abgerufen werden können.[137] „ELGA-Gesundheitsdaten“ ist ein spezieller Terminus, der ein Datenkonzept erklärt, das aus Gesundheitsdaten und genetischen Daten besteht. Darunter fallen jene personenbezogenen Daten, „*die zur weiteren Behandlung, Betreuung oder Sicherung der Versorgungskontinuität von ELGA-Teilnehmer/inne/n wesentlich sein könnten“.* Dazu gehören insbesondere Entlassungsbriefe von Krankenanstalten, Laborbefunde, die wiederum auch genetische Daten enthalten können, Bilddaten (z.B. radiologische Befunde), Be-

[132] *Aigner*, Datenschutz - Patientenschutz aus gesundheitspolitischer Sicht, RdM 2012, 84 (88).
[133] ErlRV 232 BlgNR XXVII. GP, 1.
[134] Bundesgesetz betreffend Datensicherheitsmaßnahmen bei der Verarbeitung elektronischer Gesundheitsdaten und genetischer Daten (Gesundheitstelematikgesetz 2012 – GTelG 2012), BGBl I 111/2012 idF 115/2020.
[135] ErlRV 232 BlgNR XXVII. GP, 1.
[136] Siehe § 2 Z 9 GTelG 2012.
[137] *Aigner/Leisch*, ELGA - Die Elektronische Gesundheitsakte, RdM 2013, 23.

funde und Daten aus dem Implantatregister (definiert im § 73a MPG). Diese Daten dürfen gemäß dem GTelG 2012 in ELGA verarbeitet werden.[138]

6.1.1 Elektronische Verweise (§ 20 Abs. 5 GTelG 2012)

Durch die dezentrale Speicherung der ELGA-Gesundheitsdaten sind Verweisregister notwendig, um ihren Ablageort zu kennen. Sie stellen gewissermaßen das Inhaltsverzeichnis der ELGA dar.[139] Diese Verweisregister sind Register, die innerhalb der ELGA verwendet werden, um elektronische Verweise auf ELGA-Gesundheitsdaten aufzunehmen.[140] § 20 Abs. 5 GTelG 2012 schreibt vor, dass elektronische Verweise automatisch zu erstellen sind und Daten, die sich auf ELGA-Teilnehmer/innen[141], Daten, die sich auf den ELGA-Gesundheitsdiensteanbieter[142] und Daten, die sich auf die ELGA-Gesundheitsdaten[143] beziehen, enthalten müssen.

6.1.2 Die Verarbeitung personenbezogener Daten zur Optimierung und Evaluierung von ELGA (§ 20 Abs. 6 GTelG 2012)

Daten, die im § 20 Abs. 5 GTelG 2012 taxativ aufgelistet sind, dürfen von ELGA-Systempartnern zur Optimierung und Evaluierung von ELGA verarbeitet werden. Zu diesen Zwecken dürfen auch personenbezogene Daten von ELGA-Teilnehmer/innen verarbeitet werden. Da sich der Wortlaut im § 20 Abs. 6 Z 1 GTelG 2012 auf die personenbezogenen Daten der ELGA-Teilnehmer/innen bezieht, ist davon auszugehen, dass zum einen die in § 20 Abs. 5 Z 1 GTelG 2012 und zum anderen die in § 20 Abs. 5 Z 3 GTelG 2012 definierten Daten gemeint sind. Personenbezogene Daten von ELGA-Teilnehmer/innen sind auch solche Daten, die sich auf ELGA-Gesundheitsdaten beziehen, wie sie im Gesetz normiert sind: „[...] *a) den Speicherort der ELGA-Gesundheitsdaten, b)*

---

[138] § 2 Z 9 GTelG 2012.
[139] *Milisits/Pfandlsteiner*, Wie funktioniert ELGA für ELGA-GDA?, in Aigner/Kletečka/Kletečka-Pulker/Memmer (Hrsg), Handbuch Medizinrecht (Stand 1.3.2020, rdb.at).
[140] § 2 Z 13 GTelG 2012.
[141] § 20 Abs 5 Z 1 GTelG 2012 „1. Daten, die sich auf den/die ELGA-Teilnehmer/in beziehen: a) das bPK-GH des ELGA-Teilnehmers/der ELGA-Teilnehmerin oder b) lokale Patient/inn/en-Kennungen,".
[142] § 20 Abs 5 Z 2 GTelG 2012 „a) die eindeutige Kennung des ELGA-Gesundheitsdiensteanbieters, der für die Aufnahme der ELGA-Gesundheitsdaten verantwortlich ist, b) die natürliche Person, die die ELGA-Gesundheitsdaten in ELGA gespeichert hat,"
[143] § 20 Abs 5 Z 3 GTelG 2012 „a) den Speicherort der ELGA-Gesundheitsdaten, b) die eindeutige Kennung der ELGA-Gesundheitsdaten, c) Datum und Zeitpunkt der Erstellung der ELGA-Gesundheitsdaten, d) den Hinweis auf allenfalls frühere Versionen dieser ELGA-Gesundheitsdaten, e) sofern vorhanden, einen strukturierten Hinweis auf die medizinische Bezeichnung der ELGA-Gesundheitsdaten sowie f) Datum und Zeitpunkt, an dem der elektronische Verweis auf ELGA-Gesundheitsdaten in ein Verweisregister aufgenommen wurde."

die eindeutige Kennung der ELGA-Gesundheitsdaten, c) Datum und Zeitpunkt der Erstellung der ELGA-Gesundheitsdaten, d) den Hinweis auf allenfalls frühere Versionen dieser ELGA-Gesundheitsdaten, e) sofern vorhanden, einen strukturierten Hinweis auf die medizinische Bezeichnung der ELGA-Gesundheitsdaten sowie f) Datum und Zeitpunkt, an dem der elektronische Verweis auf ELGA-Gesundheitsdaten in ein Verweisregister aufgenommen wurde".[144]

Personenbezogene Daten von ELGA-Teilnehmer/innen dürfen nur dann verarbeitet werden, wenn Personenidentifikationsdaten (die nicht gesetzlich definiert sind) „[...] *durch ein **nicht rückführbar verschlüsseltes eindeutiges Personenkennzeichen*** [...]" ersetzt werden, „[...] *wobei die **Identität der betroffenen Person** (Art. 4 Z 1 DSGVO) **mit rechtlich zulässigen Mitteln nicht bestimmt** werden kann* [...]."[145] [Hervorhebungen durch die Verfasserin] Personenkennzeichen bzw. bereichsspezifische Personenkennzeichen (bPK) sind Mittel zur eindeutigen Identifizierung von überwiegend natürlichen Personen im österreichischen E-Government-System. Diese werden mit einem kryptographischen Verfahren durch die Stammzahl[146] einer natürlichen Person und einem bestimmten Bereich der staatlichen Verwaltung erstellt.[147] Ein Personenkennzeichen bewirkt, dass die mit ihm verknüpften Daten einen eindeutigen Personenbezug aufweisen. Gleichzeitig ist es möglich, eine besonders einfache und qualitativ hochwertige Verknüpfbarkeit der Daten zu schaffen, vor allem wenn diese mit einem Personenkennzeichen des gleichen Bereichs verbunden sind.[148] In jedem Fall kann davon ausgegangen werden, dass zur Legitimation der Verarbeitung nicht nur der Name, wie im Forschungsorganisationsgesetz (FOG) (vgl. § 2d Abs. 2 Z 1 lit. a FOG) vorgesehen, durch ein Personenkennzeichen ersetzt werden muss, sondern auch andere typische Identifikationsdaten wie Wohnadresse, Geburtsdatum, Geschlecht etc. Dies ergibt sich aus dem angegebenen Plural (Personenidentifikationsdaten).

[144] § 20 Abs 5 Z 3 GTelG 2012.
[145] § 20 Abs 6 GTelG 2012.
[146] <https://www.oesterreich.gv.at/lexicon/S/Seite.990212.html> (letzter Aufruf 09.11.20) *„Im österreichischen E-Government erfolgt die eindeutige Identifikation von natürlichen Personen durch eine geheime Stammzahl, die nur auf der Bürgerkarte gespeichert werden darf, und davon abgeleiteten bereichsspezifischen Personenkennzeichen.";* § 6 E-GovG.
[147] <https://www.bmdw.gv.at/Ministerium/DasBMDW/Stammzahlenregisterbehoerde/Bereichsspezifische_Personenkennzeichen/Beschreibung-von-bereichsspezifischen-Personenkennzeichen.html> (letzter Aufruf 09.11.20); § 9 Abs 1 E-GovG.
[148] Stellungnahme der Datenschutzbehörde (1/SN-10/ME).

Das Exportformat von personenbezogenen Daten der ELGA-Teilnehmer/inne/n, darf beim Export bereits nur mehr ein Pseudonym beinhalten und soll zusätzlich mit einem Einmalschlüssel verschlüsselt werden, so dass die jeweiligen Betreiber der Verweisregister nicht mehr auf das Pseudonym der ELGA-Teilnehmer/innen schließen können.[149] Die zweite Voraussetzung für die Legitimation der Datenverarbeitung zur Optimierung und Evaluation von ELGA ist, dass die Identität (wörtlich: „*wobei die Identität*“) der betroffenen Personen nicht mit rechtlich zulässigen Mitteln bestimmt werden kann. Durch die Formulierung „*wobei die Identität*" impliziert, dass sich die Perspektive nicht auf die Datenverarbeiter oder eine bestimmte Person bezieht, sondern niemand den Personenbezug mit rechtlich zulässigen Mitteln herstellen kann.[150] Dies legt nahe, dass eine Anonymisierung vorausgesetzt wird. Die Ausführungen in den dazugehörigen Erläuterungen selbst sprechen allerdings von einer Pseudonymisierung (*„Die verpflichtende Pseudonymisierung gilt hingegen nicht für die Verarbeitung personenbezogener Daten von ELGA-Gesundheitsdiensteanbietern, da diese für die Evaluierung erforderlich sind.“).*[151] Dies setzt voraus, dass im Falle einer doppelten Verschlüsselung mit einem Personenkennzeichen und wenn niemand mit rechtlich zulässigen Mitteln einen Personenbezug herstellen kann, immer noch von einer Pseudonymisierung und nicht von einer Anonymisierung ausgegangen wird. Dem ist grundsätzlich zuzustimmen, da es zu kurz gegriffen ist, die Mittel der Möglichkeit zur Herstellung eines Personenbezugs nur mit rechtlich zulässigen Mitteln zu messen, da dies nur eine Möglichkeit ist, die Herstellbarkeit eines Personenbezugs zu prüfen. Auch hier wird ein Teil der Definition der indirekt personenbezogenen Daten mit der Definition der Pseudonymisierung vermischt, was die richtige Ausführung und Auslegung der Gesetzesbestimmung erschwert.

6.1.3 Das Protokollierungssystem (§ 22 GTelG 2012)

Jeder Verarbeitungsschritt wird durch das Protokollierungssystem in ELGA dokumentiert. Das bedeutet, dass jeder Zugriff von ELGA-Teilnehmer/innen, ELGA-GDA[152] sowie Mitar-

[149] ErlRV 232 BlgNR XXVII. GP, 4 f.
[150] § 20 Abs 6 Z 1 GTelG 2012.
[151] ErlRV 232 BlgNR XXVII. GP, 5.
[152] § 2 Z 2 GTelG 2012 „Verantwortlicher oder Auftragsverarbeiter (Art. 4 Z 7 und 8 DSGVO), die regelmäßig in einer Rolle nach der gemäß § 28 Abs. 1 Z 1 erlassenen Verordnung Gesundheitsdaten oder genetische Daten in elektronischer Form zu folgenden Zwecken verarbeiten: a) medizinische Behandlung oder Versorgung oder b) pflegerische Betreuung oder c) Verrechnung von Gesundheitsdienstleistungen oder d) Versicherung von Gesundheitsrisiken oder e)Wahrnehmung von Patient/inn/en/rechten.“

beitern der ELGA-Schlichtungsstelle, sowie die Art der Bearbeitung protokolliert werden. Damit ist eine lückenlose Verfolgung der Bearbeitungsschritte in ELGA gewährleistet.[153] Grundsätzlich ist das Protokollierungssystem zu befürworten, da es insbesondere die ELGA-Teilnehmer/innen vor dem Missbrauch ihrer Daten schützten soll und die Durchsetzung ihrer Rechte im Falle eines solchen Missbrauchs ermöglicht.[154]

Jede Verarbeitung von ELGA-Gesundheitsdaten ist zu protokollieren mit *„1. Datum und Zeit der Verarbeitung, 2. der eindeutigen Protokoll-Transaktionsnummer, 3. Art des Verarbeitungsvorgangs, 4. der eindeutigen elektronischen Identität des ELGA-Gesundheitsdiensteanbieters oder der ELGA-Ombudsstelle, der/die den Vorgang ausgelöst hat/haben, 5. dem Namen der natürlichen Person, die die ELGA-Gesundheitsdaten tatsächlich verarbeitet hat, 6.der eindeutigen Kennung der verarbeiteten ELGA-Gesundheitsdaten, 7.den Abfragekriterien sowie 8. den Fehlermeldungen bei sonstigen Abfragen, wenn sie zu Fehlermeldungen führen.“*[155] Diese müssen nach dem Zugang 3 Jahre lang in lesbarer Form aufbewahrt werden.[156] Diese Daten dürfen nicht personenbezogen verarbeitet werden, es sei denn, die erforderlichen Bedingungen sind erfüllt.[157] Eine dieser Bedingungen ist, dass zur Optimierung und Evaluierung von ELGA die in Absatz 2 abschließend aufgezählten Daten in pseudonymisierter Form verarbeitet werden, „*wobei die Identität der betroffenen Person (Art. 4 Z 1 DSGVO) mit rechtlich zulässigen Mitteln nicht bestimmt werden kann.“*[158]

In den Gesetzeserläuterungen heißt es dazu: *„**Pseudonymisierte Daten** iSd DSGVO sind **nicht deckungsgleich mit nur indirekt personenbezogenen Daten iSd DSG 2000**. Eine **Pseudonymisierung liegt nur dann vor, wenn der die Daten Verarbeitende (gar) keine Möglichkeit hat, die Zuordnung zwischen Pseudonym und Personenkennung herzustellen**.* [...]*“* [Hervorhebungen durch die Verfasserin]

[153] *Milisits/Pfandlsteiner*, Das Protokollierungssystem (§ 22 GTelG 2012), in Aigner/Kletečka/Kletečka-Pulker/Memmer (Hrsg), Handbuch Medizinrecht (Stand 1.3.2020, rdb.at).
[154] ErlRV 1936 BlgNR XXIV. GP, 33 f.
[155] § 22 Abs 2 GTelG 2012.
[156] § 22 Abs 3 GTelG 2012.
[157] § 22 Abs 5 GTelG 2012 „1. zur gerichtlichen oder außergerichtlichen Durchsetzung sowie Abwehr geltend gemachter rechtlicher Ansprüche oder 2. zur Sicherstellung einer Verarbeitung gemäß der Rollen (§ 5) oder 3. zur Information über die Aktualisierung von ELGA-Gesundheitsdaten oder 4. im Falle technischer Notwendigkeit [...].“
[158] § 22 Abs 5 Z 5 GTelG 2012.

Der erste Satz muss im Grundsatz gebilligt werden. Pseudonymisierte Daten sind nicht kongruent mit dem Konzept der indirekt personenbezogen Daten, wie es im früheren DSG 2000 normiert war. Indirekt personenbezogene Daten sind Daten, bei denen die tatsächlichen Verwender den Personenbezug nicht mit rechtlich zulässigen Mitteln herstellen können. Für diese waren diese Daten indirekt personenbezogen.[159]

Dem zweiten Satz kann nicht zugestimmt werden. Bei der Pseudonymisierung werden Daten in einer Weise verfremdet, dass ohne die Hinzufügung zusätzlicher Informationen, die gesondert aufbewahrt werden müssen, kein direkter Personenbezug hergestellt werden kann, ohne dass die voneinander getrennten Informationen wieder zusammengeführt werden. Dies kann entweder durch einen Zuordnungsschlüssel oder durch Hinzufügen weiterer Informationen erfolgen, die zu einer eindeutigen Identifizierung einer Person führen.[160] Bei der Pseudonymisierung wird nicht darauf abgestellt, wer eine Zuordnung vornehmen kann. Erneut ist auch hier die Unschärfe in der Unterscheidung der Pseudonymisierung, indirekt personenbezogener Daten und der Anonymisierung zu finden.

6.2 Statistische Auswertungen (§ 24g GTelG 2012)

Mit der Novellierung des Gesetzes im Jahr 2020 (BGBl. I Nr. 115/2020) wurden Regelungen zu einem elektronischen Impfpass in das GTelG 2012 aufgenommen. Damit soll die Bereitschaft der Durchführung von Kinder- und Jugendschutzimpfungen mit Hilfe eines elektronischen Impfdatensatzes zu einer ambulanten Versorgung führen, dadurch andere Stationen entlastet und die Verteilung der Ressourcen optimiert werden. Als Mittel zur Erreichung dieses Ziels soll eine zentrale und lückenlose Datenerfassung mit Hilfe eines elektronischen Impfausweises dienen.[161] Statistische Auswertungen sollen helfen, Impfraten zu ermitteln, bzw. zu analysieren, ob die Impfintervalle gemäß den Empfehlungen eingehalten werden oder ob definierte Gruppen geimpft wurden.[162] Um dem Prinzip der Datenminimierung (Artikel 5 Abs. 1 lit. c DSGVO) und der Sicherheitsanforderung (Artikel 32 DSGVO) der DSGVO gerecht zu werden, sind Daten für die statistische Auswertung, die im zentralen Impfregister gespeichert[163] werden „[...] *derart zu pseudonymisieren, dass*

[159] *Dohr/Pollirer/Weiss/Knyrim*, DSG Datenschutzrecht[2] § 4 62 (2017).
[160] Art 4 Z 4 VO (EU) 2016/679; *Hödl* in Knyrim (Hrsg), DatKomm Art 4 DSGVO RN 57 (Stand 1.12.2018).
[161] ErlRV 232 BlgNR XXVII. GP 1.
[162] ErlRV 232 BlgNR XXVII. GP 11.
[163] § 24c Abs 2 Z 2 lit a bis d GTelG 2012 „[...] *Angaben a) zum Impfstoff (Klassifikation, Handelsname, Hersteller, Zulassungsnummer, Chargennummer, Verfallsdatum, Serialisierungsnummer, Pharmazentralnum-*

*Verarbeitende **keine legale Möglichkeit** haben, die **Zuordnung zwischen Pseudonym und betroffener Person** herzustellen.“*[164] [Hervorhebung durch die Verfasserin] Alle Identifikationsdaten (mit Ausnahme von Geschlecht, Geburtsjahr und -monat sowie des Gemeindecodes) müssen durch einen nicht zurückverfolgbares, verschlüsseltes eindeutiges Personenkennzeichen (bPK-GH) ersetzt werden. Der Gemeindecode (GCD) ist grundsätzlich identisch mit der Gemeindekennzahl (GKZ). Für Wien weist der GCD jedoch auch die Wiener Bezirke aus.[165] Der Zusammenhang zwischen der Pseudonymisierung und den gesetzlich zulässigen Mitteln zur Herstellung des Personenbezugs wird in den zugehörigen Gesetzeserläuterungen nicht behandelt. Wieder wird nicht auf eine bestimmte Sichtweise abgestellt, wer die Identität mit rechtlich zulässigen Mitteln nicht bestimmen kann bzw. können soll, um den Anforderungen des § 24g Abs. 1 GTelG 2012 zu entsprechen.

§ 24 Abs. 2 GTelG 2012 räumt die Möglichkeit ein, die Daten des zentralen Impfregisters aus Gründen eines erheblichen öffentlichen Interesses nach Art 9 Abs. 2 lit. g - j DSGVO mit Daten aus anderen Registern zu verknüpfen, um die Durchimpfungsrate der Bevölkerung zu optimieren, die Verfügbarkeit digital gespeicherter Impfinformationen zur Steuerung des Gesundheitswesens zu nutzen und die Belastung aller Bürger, Leistungserbringer im Gesundheitswesen und des Gesundheitswesens insgesamt zu verringern.[166] Dabei müssen diese Identifikationsdaten in diesen Registern auch durch ein nicht zurückzuverfolgendes verschlüsseltes Personenkennzeichen ersetzt werden. Im Gegensatz zu § 20 Abs. 6 GTelG 2012 wird hier explizit im Gesetzestext darauf hingewiesen, dass Geschlecht, Geburtsjahr und -monat sowie Gemeindecode von der Ersetzung durch das bereichsspezifische Personenkennzeichen ausgenommen sind.[167] Dies soll nach den rechtlichen Ausführungen zu einer doppelten Pseudonymisierung führen, die einer Anonymisierung nahe kommt.[168] Ob die doppelte Pseudonymisierung einer Anonymisierung nahe kommen kann oder tatsächlich eine ist, ist und bleibt eine Einzelfallentscheidung. Je nach

---

mer und Anatomisch-Therapeutisch-Chemische Zuordnung), b) zur verabreichten Impfung (Datum der Verabreichung, Dosierung und Dosis, angewandtes Impfschema, Impfempfehlung und Zuordnung zu Impfprogrammen), c) zur Bürgerin/zum Bürger (Name, Geburtsdatum, Geschlecht, Wohnadresse, Angaben zur Erreichbarkeit, Angaben zu einer allfälligen Vertretung, Sozialversicherungsnummer, bereichsspezifisches Personenkennzeichen Gesundheit, Gemeindecode, Titerbestimmung, impfrelevante Vorerkrankungen und besondere Impfindikationen) sowie d) zum impfenden bzw. speichernden Gesundheitsdiensteanbieter (Name, Rolle, Berufsadresse und Datum der Speicherung).“

[164] ErlRV 232 BlgNR XXVII. GP. 37.

[165] ErlRV 232 BlgNR XXVII. GP. 37.

[166] § 24g Abs 2 iVm § 24b GTelG 2012.

[167] § 24g Abs 1 GTelG.

[168] ErlRV 232 BlgNR XXVII. GP. 38.

Qualität und Quantität der Daten ist eine tatsächliche Rückverfolgbarkeit auf eine betroffene Person möglich. Das Erfordernis einer Einzelfallbetrachtung bei der Ermittlung des Personenbezugs reduziert das rechtliche verbleibende Risiko einer Re-Identifizierung. Sie beseitigt aber nicht das faktische Risiko, das nach wie vor existiert.[169]

7. Genetische Daten

Die „Genetik" ist eine „*Wissenschaft, die sich mit den Gesetzmäßigkeiten der Vererbung von Merkmalen und mit den grundlegenden Phänomenen der Vererbung im Bereich der Moleküle befasst.*"[170] Beim Menschen ist die DNA in 23 Chromosomenpaaren organisiert. Sie ist der Träger des genetischen Codes. Bei etwa drei Milliarden Bausteinen in der DNA sind etwa 99,9 % identisch. Dennoch ist das genetische Material jedes Einzelnen unverwechselbar: Es unterscheidet sich an etwa 3 Millionen Stellen von jedem Anderen. Nur eineiige Zwillinge und Mehrlinge sind in diesem Fall eine Besonderheit. In diesem Fall ist die DNA-Sequenz, d.h. die Anordnung ihrer Bestandteile, identisch.[171]

Die genetische Identität ist ein einmaliger Code. Dieser Code ergibt sich aus der einzigartigen Kombination der genetischen Information. Zwar ist die genetische Information einzigartig, was es ermöglicht, ein Individuum von anderen Individuen zu unterscheiden, doch dieselbe genetische Information offenbart auch Informationen über die Blutsverwandten (biologische Familie) dieser Person einschließlich derer in nachfolgenden und früheren Generationen. Darüber hinaus können genetische Daten eine Gruppe von Individuen (z.B. Abstammungsgemeinschaften) charakterisieren; genetische Daten können Herkunft und familiäre Bindungen offenbaren. Angesichts der Entwicklungen in der wissenschaftlichen Forschung könnten genetische Daten in Zukunft möglicherweise mehr Informationen als derzeit möglich liefern und von einer zunehmenden Zahl gewinnorientierter Unternehmen für deren Zwecke genutzt werden.[172]

---

[169] *Karg*, Anonymität, Pseudonyme und Personenbezug revisited?, DuD 2015, 520 (525).
[170] <https://www.duden.de/rechtschreibung/Genetik> (letzter Aufruf 28.09.20).
[171] *Kollek*, Der naturwissenschaftliche Blickwinkel, in Sokol (Hrsg), Der gläserne Mensch – DNA-Analysen, eine Herausforderung an den Datenschutz (2003), 15.
[172] *ARTICLE 29 Data Protection Working Party*, Working Document on Genetic Data, WP 91 12178/03/EN, 4, 5, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf> (letzter Aufruf 30.09.20).

Genetische Daten können aus einer Reihe von menschlichen Substanzen mit wissenschaftlichen Methoden bestimmt werden. Dazu gehören insbesondere Blut, Speichel, Haut, Fingernägel, Haare, aber auch andere Gewebeproben und Körperflüssigkeiten, die bereits in kleinster Dosierung vorhanden sind.[173] Diese Proben sind auch ohne das Wissen der Probenspender ohne großen Aufwand beschaffbar.[174] Genetische Daten haben eine weitreichende Bedeutung, weil sie Aussagen über die Wahrscheinlichkeit des Auftretens zukünftiger Krankheiten und Veranlagungen einer oder mehrerer Personen (Verwandte) gleichzeitig machen können. Die Daten werden daher nicht retrospektiv, sondern mit Wirkung auf die Zukunft analysiert.[175] Jeder Mensch hat für immer eine "genetische Identität".[176] Altes Untersuchungsmaterial kann auch nach sehr langer Zeit mit neuem Material verglichen werden. Je größer die DNA-Stücke sind und je mehr genetisches Material getestet wird, desto wahrscheinlicher ist es zudem, dass ein Genom individualisiert werden kann und so die einzigartigen Merkmale eines Genoms zum Vorschein kommen.[177]

7.1 Biologische Probe als Informationsmedium

Informationsmedien sind im Prinzip keine Form von Daten, Angaben oder Informationen. Sie ermöglichen lediglich das Speichern, Abrufen oder das Übertragen von Informationen.[178] Proben halten Informationen. Bei der Analyse von Proben können diese Informationen in Form von Daten extrahiert werden.[179] Wenn eine Probe mit einem Code in der Form eines Etiketts versehen wird, gibt das Etikett die Information preis, dass sie von einer bestimmten oder bestimmbaren Person stammt.[180] Wenn die Probe an einem speziellen Ort, in einem Krankenhaus, Labor oder einer Arztpraxis aufbewahrt wird, könnte diese Informationen verwendet werden, um festzustellen, wo diese Person war und wo die Probe entnommen wurde.

---

[173] *Vossekuhl*, Der Schutz genetischer Daten (2013) 4; *Hofmann/Hödl*, Schwerpunkt: Open Source Biologie und Datenschutz, DuD (2013), 227 (230); *Peissl*, Datenschutz im medizinischen Bereich in Stelzer (Hrsg), Biomedizin - Herausforderung für den Datenschutz (2005) 11.
[174] *Wellbrock*, Datenschutzrechtliche Aspekte des Aufbaus von Biobanken für Forschungszwecke, MedR 2003, 77 (78); *Weichert*, Genetische Genealogie und Datenschutz, DuD (2019), 149 (150).
[175] *Peissl*, Datenschutz im medizinischen Bereich in Stelzer (Hrsg), Biomedizin - Herausforderung für den Datenschutz (2005) 11 f.
[176] *Vossekuhl*, Der Schutz genetischer Daten (2013), 97.
[177] *Menzel*, Die rechtliche Sicht, in Sokol (Hrsg), Der gläserne Mensch – DNA-Analysen, eine Herausforderung an den Datenschutz (2003) 6.
[178] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 120.
[179] *Vossekuhl*, Der Schutz genetischer Daten (2013) 5.
[180] *Herbst,* Rechtliche und ethische Probleme des Umgangs mit Proben und Daten bei großen Biobanken, DuD (2016), 371 (372).

Biologische Proben werden zur Erlangung von Gesundheitsdaten oder genetischen Daten verwendet. Die Probe selbst ist eine Substanz, eine körperliche Sache und kein Datum, weshalb sie an sich nicht unter das Datenschutzrecht fällt.[181] Erst der Vorgang, die darin enthaltenen Informationen in Form von Daten lesbar zu machen, macht das Analyseergebnis zu einem Datum und nicht die Probe selbst.[182] Gegen die Einstufung einer körperlichen Substanz als Informationsmedium im Sinne eines Speichers spricht, dass sie nicht zum Import von Daten in eine Substanz oder als natürlicher Speicher von Informationen verwendet wird, da diese bereits naturgemäß vorhanden sind und waren. Die durch die wissenschaftliche Forschung entwickelte Möglichkeit, Informationen in Form von Daten aus menschlichem Material zu gewinnen, macht den Menschen nicht zu einem wandelnden Datenspeichermedium, der als datenverarbeitendes Speichermedium infolgedessen unter das Datenschutzrecht fallen würde.[183]

7.1.1 Biobanken als Datensammlung

Biobanken stellen eine besondere Form der Nutzung menschlichen Materials dar. Sie werden zur Verwahrung von Humansubstanz (Blut, Gewebe, Zellen, Körperflüssigkeiten, DNA etc.) und typischerweise anderen Daten verwendet, die mit einer Person gekoppelt oder ihr zugeordnet werden können, aus dem Material selbst stammen oder mit Methoden der Biochemie, Immunologie, Molekularbiologie oder Genanalyse für medizinische und/oder wissenschaftliche Zwecke analysiert werden. Auf Grundlage dieser systematischen Probenentnahme und Analyse sollen personalisierte therapeutische Maßnahmen entwickelt und die Ursachen und der Verlauf von Krankheiten erforscht werden.[184] Durch Biobanken können verfügbare Proben und Daten für eine Vielzahl verschiedener Forschungsfragen in verschiedenen medizinischen Bereichen, genutzt werden.[185] Eine Bio-

[181] ErwGr 35 VO (EU) 2016/679 *„.[...] Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben,* ***abgeleitet wurden****,[...]“* (Hervorhebungen durch die Verfasserin); *Haidinger,* Was sind personenbezogene Daten?, Dako 2014, 17; *Art-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff »personenbezogene Daten« WP 136 01248/07/DE, 10 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_de.pdf> (letzter Aufruf 30.09.20); *Herbst,* Rechtliche und ethische Probleme des Umgangs mit Proben und Daten bei großen Biobanken, DuD (2016), 371 ff.
[182] *Von Freier,* Getrennte Körperteile in der Forschung zwischen leiblicher Selbstverfügung und Gemeinbesitz, MedR (2005), 321 (324); *Vossekuhl*, Der Schutz genetischer Daten (2013), 5.
[183] *Breyer*, Der datenschutzrechtliche Schutz von Körpersubstanzen, die Patienten zu Analysezwecken entnommen wurden, MedR (2004), 660; *Vossekuhl*, Der Schutz genetischer Daten (2013), 5.
[184] *Grimm,* Biobanken, in Aigner/Kletečka/Kletečka-Pulker/Memmer (Hrsg), Handbuch Medizinrecht (Stand 1.3.2020, rdb.at).
[185] *Pöttgen,* Medizinische Forschung und Datenschutz (2008) 212.

bank kann als eine BigData-Anwendung[186] gesehen werden, da sie nicht nur aus den Proben allein besteht, sondern auch aus den zugehörigen Daten in strukturierter, analysierbarer Form.[187] Humanbiobanken sind heutzutage keine Seltenheit mehr.[188] Die Humangenomforschung hat durch den technologischen Fortschritt und die dadurch möglich gewordenen detaillierten Einblicke in das menschliche Erbgut eine neue Qualität erreicht.[189] Menschliches Material und genetische Daten werden in enormer Zahl zu Forschungszwecken gespeichert, genutzt und verarbeitet. Und die Tendenz ist steigend.[190] Früher beschränkte sich die Technologie auf die Analyse einzelner Gene, doch heute ist es möglich, ganze Genome zu analysieren. Viele Unternehmen bieten inzwischen Gentests an, um das Erbgut auf spezielle Krankheiten wie bestimmte Krebsarten, Asthma oder Diabetes zu untersuchen.[191] Darüber hinaus wird es heutzutage als Lifestlyle-Produkt (z.B. "myDNA Slim"[192]) vermarktet. Nach der Laboranalyse wird den Kunden ein maßgeschneiderter Ernährungsplan zugestellt, den sie für den bereits reduzierten Preis von 189 Euro[193] und ihrer DNA erhalten können.

Nicht nur die akademische wissenschaftliche Forschung ist an der Nutzung von Biobanken interessiert, auch das Interesse kommerzieller pharmazeutischer Forschung an Aufbau und Nutzung von Biobanken ist gegeben.[194] Mit der Novellierung des FOG wurde eine Rechtsgrundlage für Biobanken und für die Verarbeitung im Sinne von Datensammlungen geschaffen, wenn diese insbesondere aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist wie im Bereich der öffentlichen Gesundheit, der medizinischen Diagnostik sowie zu wissenschaftlichen Forschungszwecken und in einem angemessenen Verhältnis zum verfolgten Ziel steht, das Wesen des Rechts auf Datenschutz gewahrt wird und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorgesehen werden.[195] Wissenschaftliche Einrichtungen,

[186] *Haimberger*, Aktuelle datenschutzrechtliche Herausforderungen in der medizinischen und pharmazeutischen Forschung, (2020), 64.
[187] <https://biobank.medunigraz.at/spenderinnen/> (letzter Aufruf 06.10.2020).
[188] <https://directory.bbmri-eric.eu/menu/main/contact> (letzter Aufruf 06.10.2020).
[189] *Mathieu/Löhnhardt/Grütz/Weil/Drepper/Krawczak*, Ethische und rechtliche Implikationen der Speicherung humaner Genomdaten, Medizinische Genetik (2003), 278.
[190] *Vossekuhl*, Der Schutz genetischer Daten (2013) 108.
[191] *Hofmann/Hödl*, Schwerpunkt: Open Source Biologie und Datenschutz, DuD (2013), 227 (230).
[192] <https://shop.lykon.de/products/mydna-slim?variant=31460524720185> (letzter Aufruf 07.10.20).
[193] Informationsstand von Jänner 2021
[194] *Nationaler Ethikrat*, Biobanken für die Forschung Stellungnahme, 10 <https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/Archiv/NER_Stellungnahme_Biobanken.pdf> (letzter Aufruf 08.10.2020).
[195] Art 9 Abs 2 lit g, i und j VO (EU) 2016/679 iVm § 2d Abs 2 FOG.

wie z.B. Personengemeinschaften sowie juristische Personen, die Zwecke im Sinne von Art 89 Abs. 1 DSGVO verfolgen, d.h. vor allem in der Forschung und experimentellen Entwicklung[196] tätig sind, unabhängig davon, ob sie akademische oder privatwirtschaftliche Einrichtungen sind, sind berechtigt, jegliche personenbezogenen Daten zu verarbeiten, insbesondere im Rahmen von Big Data, personalisierter Medizin, biomedizinischer Forschung und Biobanken. Damit schafft das neu verabschiedete FOG eine weitreichende gesetzliche Grundlage für die Verarbeitung von personenbezogenen Daten und humanen Materialien für wirtschaftlich agierende Unternehmen und stellt somit keine Privilegierung für rein wissenschaftlich tätige Institutionen mehr dar.[197] Somit ist es jedermann gestattet, personenbezogene Daten, Humanmaterial und daraus gewonnene Daten zu sammeln, zu speichern und zu verteilen, der einen Forschungszweck rechtfertigen kann. Wenn man bedenkt, dass die Verbreitung genetischer Daten in verschiedenen Bereichen, wie z.B. Versicherungs- oder Arbeitsverhältnissen, erhebliche Folgen haben oder zu einer grundsätzlichen Stigmatisierung führen könnte, stellt sich die Frage, ob dies mit dem Recht auf Datenschutz und der Wissenschaftsfreiheit vereinbar ist.[198]

7.2. Gentechnikgesetz (GTG)

Zweck dieses Gesetzes ist der Schutz der Gesundheit der Menschen und ihrer Nachkommen in der Forschung, Entwicklung und Nutzung der Gentechnik.[199] Eine genetische Analyse gemäß dem GTG ist als „*Laboranalyse* [...]“ definiert, „[...] *die zu Aussagen über konkrete Eigenschaften hinsichtlich Anzahl, Struktur oder Sequenz von Chromosomen, Genen oder DNA – Abschnitten oder von Produkten der DNA und deren konkrete chemische Modifikationen führt, und die damit nach dem Stand von Wissenschaft und Technik Aussagen über einen Überträgerstatus, ein Krankheitsrisiko, eine vorliegende Krankheit oder einen Krankheits- oder Therapieverlauf an einem Menschen ermöglicht.*“[200]

[196] § 2b Z 10 FOG „Tätigkeiten der Forschung und experimentellen Entwicklung“: Aktivitäten, die a) neuartig, b) schöpferisch, c) ungewiss in Bezug auf das Endergebnis, d) systematisch und e) übertrag- oder reproduzierbar sind“.
[197] §§ 2b Z 14 und § 2d Abs 2 FOG.
[198] *Pöttgen,* Medizinische Forschung und Datenschutz (2008) 213; *Wellbrock*, Datenschutzrechtliche Aspekte des Aufbaus von Biobanken für Forschungszwecke, MedR 2003, 77 (78).
[199] Bundesgesetz, mit dem Arbeiten mit gentechnisch veränderten Organismen, das Freisetzen und Inverkehrbringen von gentechnisch veränderten Organismen und die Anwendung von Genanalyse und Gentherapie am Menschen geregelt werden (Gentechnikgesetz – GTG), BGBl 510/1994 idF 59/2018
[200] § 4 Z 23 GTG.

§ 66 GTG schreibt vor*, „dass Genetische Analysen am Menschen für wissenschaftliche Zwecke und zur Ausbildung* [...] *nur an* ***de-identifizierten Proben*** *durchgeführt werden“* dürfen. *„**Nicht-genetische medizinische Daten, die mit genetischen Daten derselben Person verknüpft** werden sollen, müssen dabei ebenfalls **de-identifiziert** werden. Die Zuordnung dieser Daten zum jeweiligen Probenspender darf nur in den Einrichtungen erfolgen, die über eine gültige Einwilligung (Art. 4 Nr. 11 DSGVO) der betroffenen Person für diese Zuordnung verfügen. (2) Ergebnisse aus genetische Analysen gemäß Abs. 1 dürfen nur dann vernetzt oder veröffentlicht werden, wenn durch geeignete Maßnahmen sichergestellt ist, daß - abgesehen von Abs. 1 -* ***der Probenspender nicht bestimmbar ist.“***[201] [Hervorhebungen durch die Verfasserin] Die Spezifikation eines Attributs, das nur eine Person hat, macht diese identifizierbar. Der genetische Code macht unter diesem Blickwinkel bereits eine Person identifizierbar, unabhängig davon, ob Name, Anschrift oder andere identifizierende Daten mit ihr verknüpft sind. Aus einer anderen Perspektive können genetische Daten nur dann als personenbezogen betrachtet werden, wenn sie mit anderen identifizierenden Informationen in Verbindung gebracht werden können.[202] Auch unter dem Aspekt des in Österreich verbreiteten Ausdrucks "mit rechtlich zulässigen Mitteln", den das DSG 2000 im Zusammenhang mit den indirekt personenbezogenen Daten kannte, die dadurch definiert waren, dass ihr Personenbezug mit legalen Mitteln nicht wiederhergestellt werden konnte und infolgedessen das Datenschutzrecht nur eingeschränkt auf sie anwendbar war, ist eine Identifizierbarkeit durch genetische Daten ohne Verknüpfung mit weiteren Daten heute grundsätzlich möglich, dies insbesondere mit rechtlich zulässigen Mitteln.[203]

In den Erläuterungen zu § 66 GTG heißt es, dass aufgrund der eingegangenen Stellungnahmen der Begriff "anonymisieren" durch "de-identifizieren" ersetzt wurde. Dadurch werden identifizierende Informationen wie Name und Geburtsdatum entfernt.[204] Um § 66 Abs. 1 GTG zu entsprechen, müssen auch nicht-genetische, aber medizinische Daten de-identifiziert werden, wenn sie mit den genetischen Daten verknüpft werden sollen. Weshalb der Begriff des Anonymisierens nicht mit Vorgabe der Pseudonymisierung ersetzt wurde, ist aus den Erläuterungen nicht ersichtlich. Im Grunde werden Daten in einer Weise verarbeitet, die ohne Hinzuziehung der gestrippten Informationen, wie Name und Ge-

[201] § 66 Abs 1 und 2 GTG.
[202] *Hofmann/Hödl*, Schwerpunkt: Open Source Biologie und Datenschutz, DuD (2013), 227 (232 f).
[203] *Hofmann/Hödl*, Schwerpunkt: Open Source Biologie und Datenschutz, DuD (2013), 227 (233).
[204] ErlRV 108 BlgNR XXVI. GP, 77.

burtsdatum, nicht mehr dieser spezifischen Person zugeordnet werden können. Entweder wollte der Gesetzgeber eben nicht die Pseudonymisierung vorgeben, da er davon ausgeht, dass bei genetischen Analysen für die Forschung und Ausbildung die identifizierenden nicht-medizinischen Daten erst gar nicht zur Zuordnung aufbewahrt werden weshalb der zweite Halbsatz nicht erfüllt wird oder dieser hat schlicht und einfach die Pseudonymisierung nicht in Betracht gezogen oder er wollte eine eigene Zwischenstufe der Pseudonymisierung schaffen, ohne diese aber abschließend im Normtext zu definieren. Auf diese Weise bleibt das allgemeine Datenschutzrecht anwendbar, und es wird keine Möglichkeit geschaffen, genetische Daten zur Verwendung in Forschung und Entwicklung in der Gentechnik unter Missachtung des europäischen Datenschutzrechts zu verarbeiten.

Im Grunde genommen ist die De-Identifikation auch nichts anderes als eine Datensicherheitsmaßnahme, indem identifizierende Informationen entfernt werden, die ohne zusätzliche Informationen an sich keine eindeutige Identifizierung einer Person ermöglichen. Was ist aber heute noch eine direkt identifizierende Information? Der Vor- und Nachname reicht inzwischen nicht mehr aus, um eine Person unter rund 7,77 Milliarden[205] Menschen auf der Welt eindeutig zu identifizieren. Eine Identifikation einer Person ist um so eher möglich, je eindeutiger die Information ist oder je untrennbarer sie von dieser Person ist.[206]

7.2.1 Einzigartigkeit

Die Einzigartigkeit von Informationen hängt von der Genauigkeit und dem Zeitpunkt der Erfassung ab. Wenn eine Blutprobe entnommen und bestimmte Werte analysiert werden, handelt es sich um eine Momentaufnahme, die sich von einem früheren oder späteren Zeitpunkt unterscheiden kann.[207] Auch die Erfassung von Informationen wie Haarfarbe braun, Größe 164 cm, keine Tätowierungen, Führerschein vorhanden, sind variable Informationen. Eine Haarfarbe kann gewechselt werden, mit zunehmendem Alter verringert sich die Größe, eine Tätowierung kann gestochen und der Führerschein abgenommen werden.

[205] <https://de.statista.com/themen/75/weltbevoelkerung/> (letzter Aufruf 15.10.20).
[206] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 277.
[207] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 283.

Zur Identifizierung genetischer Daten nennen Arning, Forgó und Krügel ein Beispiel: „*Man stelle sich vor, dass eine für die Identifizierung einer Person ausreichend große Gensequenz ohne jeden weiteren Personenbezug im Rahmen einer Studie über das HIV-Virus im Internet veröffentlicht wird. Ist die genetische Information dieser Person in anderem Zusammenhang bereits als Referenzdatensatz gespeichert,* [...] *wäre für alle Personen, die Zugriff auf diese Datenbanken haben, nunmehr eine Identifizierung der betroffenen Person und seiner HIV-Erkrankung* […] *möglich."*[208] Werden genetische Daten mit zusätzlichen Informationen verknüpft, so hat dies zur Folge, dass jede zusätzliche Information, die allein zu den nicht-genetischen Informationen hinzugefügt wird, zu einer Anreicherung von Informationen führt, die ihrerseits wiederum eine Identifizierbarkeit ermöglichen könnte. In jedem Fall macht die jeweilige Verknüpfbarkeit der Information mit der einzigartigen genetischen Information diese Person identifizierbar. Ohne diese zusätzliche Information ist allein der genetische Code, der zwar eindeutig ist, aber ohne verknüpfbare Information kein Mittel, um eine bestimmte Person zu finden. Genetische Daten sind zugleich Schlüssel "der genetische Code" und personenbezogenes Datum. Der genetische Code ist der Schlüssel den es zu entschlüsseln gilt, um die darin enthaltenen Informationen lesbar zu machen. Der Schlüssel als das zu verwendende Identifikationsmittel ist wertlos ohne den Raum hinter dem Schloss als Referenzdatenbank oder zusätzliche Informationen. Solange diese Komponenten nicht verfügbar sind, ist der genetische Code zwar einzigartig aber die dahinter stehende natürliche Person nicht bestimmbar.[209] Aufgrund der wachsenden Zahl von Vergleichsproben (DNA-Proben) in den diversen Biobanken von Forschungsinstitutionen oder Unternehmen, die genetische Analysen anbieten, wird es durch die Zunahme von genaueren, kürzeren und billigeren Methoden immer wahrscheinlicher, die Proben zuordnen zu können. Je mehr Proben gesammelt und gelagert werden und je mehr zusätzliches Wissen verbreitet und vernetzt wird, desto mehr Möglichkeiten gibt es, eine Zuordnung vorzunehmen.[210] Diese Annahmen zur Weiterentwicklung der humangenetischen Forschung sind zu bestätigen und wurden bereits vor längerer Zeit getroffen. Es ist davon auszugehen ist, dass die Humangenetik, die Auswei-

[208] *Arning/Forgó/Krügel,* Datenschutzrechtliche Aspekte der Forschung mit genetischen Daten, DUD (2006) 700 (701).
[209] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 281 f.
[210] *Wellbrock*, Datenschutzrechtliche Aspekte des Aufbaus von Biobanken für Forschungszwecke, MedR 2003, 77 (79).

tung von Biobanken, die Entwicklung von billigeren, schnelleren und einfacheren Methoden zur genetischen Analyse weit fortgeschritten sind (siehe DNA-Chips).[211]

Exkurs: Die Einwilligung (Artikel 4 Z 11 DSGVO) und der „broad consent" (§ 2d Abs. 3 FOG)

§ 66 GTG Abs. 1 dritter Satz selbst sieht vor, dass die Einwilligung nach Artikel 4 Z 11 DSGVO von den Probenspendern einzuholen ist, wenn deren de-identifizierte genetischen und de-identifizierte medizinischen Daten von der Einrichtung, in der diese genetische Analyse durchgeführt wurde, zusammengeführt werden sollen.[212] Der Artikel 4 Z 11 DSGVO definiert die Einwilligung als eine „[...] *freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;"*[213] Der § 66 Abs. 3 GTG selbst verweist wiederum auf § 2d Abs. 3 FOG, welcher den sogenannten „broad consent" regelt. Aus den Erläuterungen zum § 2d Abs. 3 FOG geht hervor, wobei die Betitelung "consent" was ins Deutsche übersetzt "Einwilligung" heißt misslungen ist, dass es sich um keine Einwilligung wie in der DSGVO im Artikel 4 Z 11 definiert, handelt, sondern nur um eine Nachempfindung derer, welche wiederum als „geeignete Garantie" im Sinne des Artikel 89 DSGVO in Verbindung mit Artikel 9 Abs. 2 lit j DSGVO zu sehen ist. Mit einem „broad consent", wie er im FOG normiert ist, kann die Einwilligung in die Verarbeitung besonderer Datenkategorien (z.B. Gesundheitsdaten und genetische Daten) für Forschungsgebiete oder Teile von Forschungsprojekten erteilt werden. In den zugehörigen Erläuterungen wird auf den Erwägungsgrund 33 der DSGVO und auf ein Arbeitspapier („Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)") aus 2007 der damaligen Artikel-29-Datenschutzgruppe, verwiesen.[214] Im Kapitel III. „Überlegungen zu einem geeigneten Rechtsrahmen für EPA-Systeme", Punkt 1 „Wahrung des Selbstbestimmungsrechts" weist diese darauf hin, dass selbst wenn elektronische Patientenakten-Systeme nicht auf der Einwilligung allein als ausschließliche Rechtsgrundlage bestehen können, die Selbstbe-

[211] *Kollek*, Der naturwissenschaftliche Blickwinkel, in Sokol (Hrsg), Der gläserne Mensch – DNA-Analysen, eine Herausforderung an den Datenschutz (2003) 27 f; *Stahl,* Analyse der Genregulation DNAChiptechnologie, Chem. Unserer Zeit (2005), 188.
[212] § 66 Abs 1 GTG.
[213] Art 4 Z 11 VO (EU) 2016/679.
[214] ErlRV 68 BlgNR XXVI. GP, 35.

stimmung der Patienten über den Beginn, Umfang und Zweck der Nutzung ihrer Daten als Schutzmechanismus eine wichtige Rolle spielen sollte.[215] Die Artikel-29-Datenschutzgruppe beschreibt eine Möglichkeit, eine „Zustimmung als geeignete Garantie“ zu betrachten, die nicht den Anforderungen der Einwilligung des damaligen Artikels 8 Absatz 2 der DS-RL[216] entsprechen muss. Diese Zustimmung als geeignete Garantie kann sich als opt-out in Form einer ausdrücklichen Ablehnung manifestieren. Die Wahl des Wortes "Zustimmung" anstelle von "Einwilligung" ist auch ein Hinweis darauf, dass hier die Unterscheidung betont wird, dass " Einwilligung" ein opt-in in Form der Abgabe einer gültigen Einwilligungserklärung und opt-out die ausdrückliche Möglichkeit zum Widerspruch ist. Der im FOG deklarierte „broad consent“ sieht jedoch eine vorherige ausdrückliche Einwilligung und nicht ein opt-out vor. Darüber hinaus unterscheidet die Artikel-29-Datenschutzgruppe in ihrem Arbeitspapier zu EPA zwischen verschiedenen Arten von Gesundheitsdaten, die je nach Schwere der Folgen (z.B. Daten zum Schwangerschaftsabbruch, psychiatrische Daten etc.) zu unterscheiden sind, so dass für die Ausübung des Selbstbestimmungsrechts in Bezug auf die Verarbeitungsmöglichkeiten unterschiedliche Maßstäbe angelegt werden sollen.[217] Eine solche Unterscheidung hat der Gesetzgeber im FOG nicht vorgesehen. Da jedoch der Verweis auf das Arbeitspapier der Artikel-29-Datenschutzgruppe betreffend "opt-in" und "opt-out" bereits fehlerhaft ist, ist das Versäumnis diese Unterscheidung zu treffen, nur eine Unstimmigkeit von vielen.

Der Unionsgesetzgeber hat die Möglichkeit eines „broad consent“ vorgesehen, allerdings nicht im Gesetzestext selbst, sondern in den Erwägungsgründen. Darin ist jedoch nicht von eindeutigen Fällen die Rede, sondern es wird festgestellt, dass oftmals der Zweck der Forschung zu Beginn eines Forschungsprojektes noch nicht feststeht und dass es den Betroffenen "erlaubt" ist, ihre Einwilligung für bestimmte Bereiche der wissenschaftlichen Forschung zu erteilen, wenn entsprechende wissenschaftliche und ethische Normen ein-

[215] *Art 29-Datenschutzgruppe*, Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), WP 131, 00323/07/DE, 14 <http://bmg.gv.at/cms/home/attachments/9/5/8/CH1045/CMS1201688092738/wp131.pdf>. (letzter Aufruf 01.10.20).
[216] Art 8 Abs 2 lit a RL 95/46/EG „[...] Die betroffene Person hat ausdrücklich in die Verarbeitung der genannten Daten eingewilligt, es sei denn, nach den Rechtsvorschriften des Mitgliedstaats kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden; [...]“.
[217] *Art-29-Datenschutzgruppe*, Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), WP 131, 00323/07/DE, 15 <http://bmg.gv.at/cms/home/attachments/9/5/8/CH1045/CMS1201688092738/wp131.pdf>. (letzter Aufruf 01.10.20).

gehalten werden. Die Formulierung lässt eher eine Ausnahme als die Regel vermuten.[218] Diese Meinung wird auch von der Artikel-29-Datenschutzgruppe in deren Arbeitspapier „Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/67“ vertreten: *„Für Fälle, in denen die **Zwecke für die Datenverarbeitung** im Rahmen **eines wissenschaftlichen Forschungsprojektes am Anfang nicht angegeben** werden können, ermöglicht Erwägungsgrund 33 **ausnahmsweise**, dass der Zweck **allgemeiner beschrieben** werden kann.“*[219] [Hervorhebungen durch die Verfasserin] Insbesondere bei der Verarbeitung besonderer Kategorien von Daten sind an die erwähnte Möglichkeit der Einwilligung zu bestimmten Bereichen der wissenschaftlichen Forschung, wie sie in Erwägungsgrund 33 beschrieben ist, strengere Maßstäbe anzulegen. Verantwortliche der Datenverarbeitung müssen daher andere Wege finden, um dem Grundsatz der informierten Einwilligung zu genügen. Das Einholen der Einwilligung in verschiedenen Stadien oder nach jedem Zwischenergebnis wäre eine Möglichkeit, die anfängliche Zweckunschärfe auszugleichen. Natürlich würde dies zu einer gewissen Unsicherheit hinsichtlich der Bestandsfestigkeit eines Forschungsprojekts führen; andererseits ist das Widerrufsrecht jeder Einwilligung immanent, unabhängig davon, ob sie in informierter Weise und in Kenntnis der Sachlage oder auf einen bestimmten Forschungsbereich begrenzt, erfolgt, was bedeutet, dass eine betroffene Person in jeder Phase des Forschungsprojekts ihr Widerrufsrecht ausüben und sich mit ihren Daten aus dem Forschungsprojekt herausnehmen kann. Dasselbe gilt für die Möglichkeit, die betroffenen Personen laufend zu informieren, um die erste Einwilligung mit einem unbestimmten Forschungszweck zu legitimieren.[220] Die von den Grundrechten der Europäischen Union garantierte Wissenschaftsfreiheit steht seit jeher im Konflikt mit dem Datenschutz als höchstpersönliches Recht, in dem die Einwilligung zur Datenverarbeitung der eigenen personenbezogenen Daten der Inbegriff dieses Rechts ist. Dass die Einwilligung in die Datenverarbeitung zu wissenschaftlichen Forschungszwecken nicht die unproblematischste Rechtsgrundlage ist, insbesondere bei klinischen Prüfungen, wurde auch vom Europäischen Datenschutzausschuss in einer Stellungnahme ausgearbeitet.[221] Insbesondere das Problem der Freiwilligkeit der Einwilligung, wird in der besag-

[218] ErwGr 33 VO (EU) 2016/679.
[219] *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 17/DE, 34 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.> (letzter Aufruf 10.10.2020).
[220] *Artikel-29-Datenschutzgruppe*, WP 259 rev.01, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 17/DE, 34 f. <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.> (letzter Aufruf 10.10.2020).
[221] Siehe *EDSA*, Stellungnahme 3/2019 zu den Fragen und Antworten zum Zusammenspiel der Verordnung über klinische Prüfungen und der Datenschutz-Grundverordnung (DSGVO).

ten Stellungnahme hervorgehoben, wenn Studienteilnehmerinnen einen schlechten Gesundheitszustand haben, zu einer ökonomisch oder gesellschaftlich schwächeren Bevölkerungsgruppe zählen oder sich in einer anderen Abhängigkeit befinden.[222]

Im Absatz 1 des § 66 GTG geht es nach dem Wortlaut um die Einwilligung zur Zuordnung, während die Änderung in Absatz 1 nach den Erläuterungen des Gesetzes keine inhaltliche Änderung darstellen soll. Im damaligen § 66 Abs. 1 GTG hieß es: „*Genanalysen am Menschen für wissenschaftliche Zwecke und zur Ausbildung dürfen* ***nur mit ausdrücklicher und schriftlicher Zustimmung des Probenspenders*** *oder an anonymisierten Proben durchgeführt werden* [...]*“.*[223] [Hervorhebungen durch die Verfasserin] Nach dem derzeitigen Wortlaut dieser Bestimmung ist für die genetische Analyse keine ausdrückliche schriftliche Einwilligung der Probenspender erforderlich, da die Einwilligung nur dann zur Anwendung kommt, wenn die bereits bei der genetischen Analyse erhobenen Daten mit den anderen medizinischen Daten verknüpft werden. Aufgrund der historischen Auslegung und des Willens des Gesetzgebers, der in den Erläuterungen festgehalten ist, ist diese Rechtsnorm auf eine sprachliche Ungenauigkeit zurückzuführen. Sinn und Inhalt der Norm sind so auszulegen, dass vor der Erhebung der genetischen Daten jedenfalls ausdrückliche und mögliche schriftliche Einwilligungen der Probenspender eingeholt werden müssen. Es ist davon auszugehen, dass insbesondere die "ausdrückliche Einwilligung" im Vordergrund steht, wie sie auch in Artikel 9 Abs. 1 lit a DSGVO vorgesehen ist. Die Schriftform ist kein Kriterium der "ausdrücklichen" Einwilligung, was aus Gründen der Beweislast allerdings ratsam ist.[224] Da es sich bei einem Probenmaterial um eine körperliche Sache[225] handelt, fällt es unter das Eigentumsrecht. Das Erfordernis der Einwilligung ist daher nicht nur unter dem Aspekt des Datenschutzes zu betrachten. Der § 66 Abs. 3 GTG verweist wiederum auf den § 2f FOG, der anzuwenden sei. Dieser legitimiert „*Wissenschaftliche Einrichtungen (§ 2b Z 12)“* dazu „[...] *Forschungsmaterial (§ 2b Z 6) für Zwecke gemäß Art. 89 Abs. 1 DSGVO insbesondere* [...]“ zu „[...] ***sammeln, archivieren und systematisch*** [...]*“* zu „ [...] ***erfassen*** *und dazu* ***sämtliche Daten*** *(§ 2b Z 5)* [...]*“* zu „ [...] ***verarbeiten****, die erforderlich sind, um einen optimalen Zugang zu Daten (§ 2b Z 5) und Forschungsmaterial*

[222] *EDSA*, Stellungnahme 3/2019 zu den Fragen und Antworten zum Zusammenspiel der Verordnung über klinische Prüfungen und der Datenschutz-Grundverordnung (DSGVO), Rz 20.
[223] § 66 Abs 1 GTG idF 1994.
[224] *Feiler/Forgó*, EU-DSGVO Art 7 Rz 2.
[225] § 292 ABGB.

für Zwecke gemäß Art. 89 Abs. 1 DSGVO („Repositories“) zu gewährleisten, [...]*“.*[226] [Hervorhebungen durch die Verfasserin] In den Erläuterungen wird klargestellt, dass auch "Sammlungen", worunter das Sammeln von Forschungsmaterial und personenbezogenen Daten zu verstehen ist, mit der Einwilligung nach Artikel 4 Z 11 DSGVO rechtlich legitimiert werden können.[227] Hierbei ist zu beachten, dass das FOG nur für wissenschaftliche Einrichtungen[228] anwendbar ist. Wohingegen das GTG eine im Gesetz definierte Einschränkung auf wissenschaftliche Einrichtungen nicht kennt.

In diesem Zusammenhang ist nicht nur auf den Datenschutz und die Eigentumsrechte zu achten, die hier weiter unberücksichtigt bleiben, sondern auch auf das europäische Recht, das seinerseits im Vertrag über die Europäische Union auf gemeinsame Grundwerte verweist, insbesondere in Fragen der Menschenwürde und des Persönlichkeitsschutzes, in dem Bereich, in dem die Biomedizinkonvention tätig ist.[229] Im Übereinkommen zum Schutz der Menschenrechte und der Menschenwürde im Hinblick auf die Anwendung von Biologie und Medizin heißt es in Artikel 16 unter Bezugnahme auf Artikel 5, dass die betroffene Person über den Zweck und die Art einer Maßnahme sowie über deren Folgen und Risiken adäquat aufgeklärt werden muss, dass die Einwilligung ausdrücklich und speziell für diesen Fall zu erteilen und zu dokumentieren ist, dass sie freiwillig ist und jederzeit widerrufen werden kann.[230] Zudem bestimmt Artikel 22, dass eine biologische Probe, die während einer Maßnahme gewonnen wurde, nur zu dem Zweck gelagert werden darf, zu dem sie entnommen wurde. Eine anderweitige Nutzung erfordert ein geeignetes Verfahren zur Information und Einwilligung.[231] Im Zusatzprotokoll zum Übereinkommen über Menschenrechte und Biomedizin, betreffend biomedizinische Forschung heißt es zudem, dass keine Forschung an einer Person ohne die informierte, freie, ausdrückliche, spezifische und dokumentierte Zustimmung der Person durchgeführt werden darf. Diese Zustimmung kann

[226] § 2f Abs 1 FOG.
[227] ErlRV 68 BlgNR XXVI. GP, 40.
[228] § 2b Z 12 FOG „natürliche Personen, Personengemeinschaften sowie juristische Personen, die Zwecke gemäß Art. 89 Abs. 1 DSGVO verfolgen, d.h. insbesondere Tätigkeiten der Forschung und experimentellen Entwicklung (Z 10) vornehmen, ungeachtet dessen, ob dies a) zu gemeinnützigen Zwecken (§§ 34 ff der Bundesabgabenordnung, BGBl. Nr. 194/1961) oder nicht oder b) im universitären, betrieblichen oder außeruniversitären Rahmen erfolgt;“.
[229] *Stelzer,* Datenschutz im Gentechnikrecht, in Stelzer (Hrsg), Biomedizin – Herausforderung für den Datenschutz (2005) 97.
[230] Übereinkommen zum Schutz der Menschenrechte und der Menschenwürde im Hinblick auf die Anwendung von Biologie und Medizin: Übereinkommen über Menschenrechte und Biomedizin des Europarates, Art 15 und 16, SEV Nr. 164.
[231] Übereinkommen zum Schutz der Menschenrechte und der Menschenwürde im Hinblick auf die Anwendung von Biologie und Medizin: Übereinkommen über Menschenrechte und Biomedizin des Europarates, Art 22, SEV Nr. 164.

von der Person in jeder Phase der Forschung frei widerrufen werden.[232] Österreich ist bis heute nicht, obwohl seitens der Bioethikkommission im Bundeskanzleramt bereits 2002[233] empfohlen, der Biomedizinkonvention des Europarats beigetreten. Auch wenn sich Österreich den Bestimmungen der Biorechtskonvention nicht offiziell unterworfen hat, so handelt es sich doch um europäische Grundwerte in Hinblick auf die Menschenwürde und des Persönlichkeitsschutzes.[234]

Gemäß § 2a FOG geht das FOG anderen Bestimmungen in den jeweiligen Bundesgesetzen vor, wenn dieses selbst speziellere Bestimmungen enthält.[235] Der Absatz 3 enthält einen Verweis auf § 2d Abs. 3 („broad consent"), § 2f Abs. 1 Z 6 („Repositories von Forschungsmaterial[236] und Daten") und unter anderem § 2f Abs. 4 („Biologische Proben- und Datensammlungen") FOG. Wie oben ausgeführt, widerspricht der „broad consent" in seiner jetzigen Form im FOG dem Artikel 4 Z 11 DSGVO und unter der Prämisse, dass der § 66 Abs. 1 GTG durch das Datenschutz-Anpassungsgesetz 2018 – Wissenschaft und Forschung (WFDSAG 2018) inhaltlich nicht verändert wurde, hat dieser im Zusammenhang mit der genetischen Analyse für wissenschaftliche und Ausbildungszwecke keine Rechtsgültigkeit. Die Einwilligung nach Artikel 4 Z 11 DSGVO ist alternativ zu § 2f Abs. 1 FOG für die Erhebung von Forschungsmaterial und -daten heranzuziehen. Da die Bestimmung in § 66 Abs. 1 GTG an sich eine spezifischere Bestimmung ist, da sie zwar wissenschaftliche Forschungszwecke regelt, dies aber auf dem spezifischen Gebiet der Gentechnik[237], hat § 2f Abs. 1 FOG ebenfalls im Zusammenhang mit gentechnischen Analysen unangewendet zu bleiben. Mit Absatz 4 soll eine Regelung für die Verarbeitung im Rahmen biologischer Proben- und Datensammlungen auf der Grundlage von Artikel 9 Abs. 2 lit. i und j DSGVO geschaffen werden, der klarstellt, dass eine gesonderte Einwilligung im Sinne von Artikel 9 Abs. 2 lit. a DSGVO unter anderem für Verarbeitungen für Zwecke gemäß Artikel 89 Abs.

[232] Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research, Council of Europe Treaty Series - No. 195.
[233] *Bioethikkommission beim Bundeskanzleramt*, Beschluss der Bioethikkommission beim Bundeskanzleramt vom 11. Februar 2002 betreffend die Empfehlung für einen Beitritt Österreichs zur Biomedizinkonvention des Europarates, <https://www.bundeskanzleramt.gv.at/themen/bioethikkommission/publikationen-bioethik.html> (letzter Aufruf 12.10.2020).
[234] *Stelzer,* Datenschutz im Gentechnikrecht, in Stelzer (Hrsg), Biomedizin – Herausforderung für den Datenschutz (2005) 97 f.
[235] § 2a FOG.
[236] § 2b Z 6 FOG „körperliche Sachen, die für Zwecke gemäß Art. 89 Abs. 1 DSGVO von Bedeutung sein können, wie insbesondere: a) biologische, genetische, geologische oder sonstige Proben oder b) Bild-, Film-, Ton- oder Videomaterial oder c) Schriftgut gemäß § 25 Abs. 2 des Denkmalschutzgesetzes (DMSG), BGBl. Nr. 533/1923;".
[237] § 2a FOG; § 66 GTG.

1 DSGVO nicht erforderlich ist.[238] Der Artikel 9 Abs. 2 lit. j DSGVO ist als Ausgleichregelung gemäß Artikel 85 DSGVO zu verstehen, die das grundsätzliche Verarbeitungsverbot von Daten besonderer Kategorie für wissenschaftliche Forschungszwecke durchbricht. Diese Verarbeitung ist aber nur dann zulässig, wenn geeignete Garantien, wie in Artikel 89 Abs. 1 DSGVO, in den nationalen Gesetzen vorgesehen sind. Artikel 89 Abs. 1 DSGVO selbst liefert nur eine sehr allgemeine und beispielhafte Definition von angemessenen Garantien im Sinne der Einhaltung von Datensicherheitsmaßnahmen und des Grundsatzes der Datensparsamkeit.[239] In jedem Fall sind der Situation entsprechend angemessene Garantien anzuwenden, und es muss ein höherer Standard angestrebt werden, wenn dies zum angemessenen Schutz der Interessen der betroffenen Person erforderlich ist. Es handelt sich um ein Forschungsprivileg, das als ein solches behandelt werden muss.[240] Auch hier gilt wieder das bereits Ausgeführte. § 66 Abs. 1 GTG ist lex specialis, weshalb § 2f Abs. 4 FOG auch in diesem Fall nicht durch eine spätere generelle Norm derogiert werden kann.

7.2.2 § 66 Abs. 2 GTG

Absatz 2 des § 66 GTG behandelt die Offenlegung durch Übermittlung. Die Veröffentlichung oder Vernetzung der Ergebnisse einer zu Forschungs- oder Ausbildungszwecken durchgeführten genetischen Analyse ist zulässig, wenn die De-Identifikation der Proben, der nicht-genetischen medizinischen Daten und der genetischen Daten durchgeführt wurde und die betroffene Person nicht bestimmbar ist. Dies mit Ausnahme des Absatzes 1, in dem die Zuordnung der nicht-genetischen medizinischen Daten und der genetischen Daten zu den jeweiligen Probenspendern zulässig ist, in der Einrichtung, die eine Einwilligung nach Artikel 4 Z 11 DSGVO hat, da in diesem Fall die Person in jedem Fall identifizierbar ist.[241] Nicht geregelt wurde, für wen die betroffene Person nicht bestimmbar sein darf. Aufgrund der Besonderheit genetischer Daten im Sinne ihrer Einzigartigkeit und besonderen Schutzwürdigkeit und Tragweite ist diese Regelungslücke problematisch, da die Vernetzung die Weitergabe von Daten an andere impliziert und die Veröffentlichung in der heuti-

[238] ErlRV 68 BlgNR XXVI. GP, 41.
[239] Art 89 Abs 1 VO (EU) 2016/679.
[240] *Pötters,* in Gola (Hrsg), Datenschutz-Grundverordnung[2] Rz 8 (2018); *Hense*, in Sydow (Hrsg), Europäische Datenschutz-Grundverordnung[2] Rz 10 (2018).
[241] § 66 Abs 2 GTG; *Stelzer*, Datenschutz im Gentechnikrecht, in Stelzer (Hrsg), Biomedizin – Herausforderung für den Datenschutz (2005) 99.

gen Zeit nicht rückgängig zu machen ist (z.B. Veröffentlichungen im Internet) und jene Datenverarbeiter selbst entscheiden können, ob eine Person nicht identifizierbar ist und dies alles ohne Wissen und Zustimmung der Betroffenen.

8. Definition von „De-Identified Data“ (HIPAA - Health Insurance Portability and Accountability Act)

Das amerikanische Recht kennt den Begriff "De-Identifikation" oder auf Englisch „De-Identification“. Die De-Identifikation ist ein Mittel, mit dem Organisationen personenbezogene Informationen aus Daten entfernen können, die sie sammeln, nutzen, speichern und mit anderen Organisationen austauschen. Die De-Identifikation ist keine einzelne Technik, sondern eine Reihe von Ansätzen, Algorithmen und Werkzeugen, die auf verschiedene Arten von Daten mit unterschiedlicher Wirksamkeit angewendet werden können. Die medizinische Forschung in den Vereinigten Staaten lebt vom Austausch von de-identifizierten Patienteninformationen, der durch den Health Insurance Portability and Accountability Act (HIPAA), der primären US-Regelung zum Schutz der Privatsphäre medizinischer Daten, ermöglicht wird.[242]

Diese „Privacy Rule“ schützt alle personenbezogenen Gesundheitsinformationen, die als geschützte Gesundheitsinformationen („Protected Health Information“ - PHI) bezeichnet werden und von einer unter HIPAA fallenden Organisation (Zu den erfassten Organisationen gehören Gesundheitsdienstleister, Krankenkassen und Abrechnungszentren für das Gesundheitswesen. Krankenhäuser, Ärzte und andere Fachleute und Einrichtungen des Gesundheitswesens, die Behandlungen anbieten) erhoben oder empfangen werden. Personenbezogene Gesundheitsinformationen werden definiert als Informationen, einschließlich demographischer Informationen, die sich auf die vergangene, gegenwärtige oder zukünftige physische oder psychische Gesundheit, die Gesundheitsversorgung oder die vergangene, gegenwärtige oder zukünftige Zahlung für die Bereitstellung von Gesundheitsleistungen für eine Person beziehen, Informationen die entweder die Person identifizieren oder bezüglich derer es eine begründete Annahme gibt, dass die Informationen zur Identifizierung der Person verwendet werden könnte. Die Privacy Rule schützt keine personenbezogenen Gesundheitsinformationen, die von einer anderen Organisation als einer betroffenen Einheit erfasst oder gespeichert werden. Sie gilt auch nicht für Informationen, die

[242] *Garfinkel,* De-Identification of Personal Information, 1 <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf> (letzter Aufruf 11.11.20).

in Übereinstimmung mit der Privacy Rule de-identifiziert wurden. Es gibt keine Restriktionen für die Verwendung oder Offenlegung von de-identifizierten Gesundheitsinformationen.[243]

HIPAA definiert zwei Ansätze zur De-Identifikation durch Entfernung von Protected Health Information“ (PHI): 1) Die Expertenbestimmungsmethode (§164.514(b)(1)) - Diese sieht einen Experten vor, der den Datensatz analysiert und ein geeignetes Mittel zur De-Identifikation bestimmt, welches das Risiko einer Re-Identifikation minimiert; oder 2) die Safe-Harbor-Methode (§164.514(b)(2)). HIPAA selbst schreibt nicht vor, welche der beiden Methoden gewählt werden muss. Es liegt im Ermessen der Datenverarbeiter, das Risiko zu messen und zu bestimmen, welche De-Identifizierungsmethoden auf die Daten angewendet werden sollten, um das Re-identifizierungsrisiko zu minimieren.[244]

8.1 Die Expertenbestimmungsmethode

Bei der "Expertenbestimmungsmethode“ muss ein Experte einen Datensatz analysieren und ein geeignetes Mittel zur De-Identifikation bestimmen, dass das Risiko einer Re-Identifikation minimiert. Diese Person muss über angemessene Kenntnisse und Erfahrungen mit allgemein anerkannten statistischen und wissenschaftlichen Prinzipien und Methoden verfügen, um Daten nicht individuell identifizierbar zu machen. Bei der Anwendung dieser Grundsätze und Methoden wird sichergestellt, dass das Risiko einer Re-Identifikation sehr gering ist und die Informationen, allein oder in Kombination mit anderen realistischerweise verfügbaren Informationen, von einem potentiellen Empfänger verwendet werden könnten, um eine bestimmte Person zu identifizieren, die das Subjekt der Informationen ist; und, dokumentiert die Methoden und Ergebnisse der Analyse, die eine solche Feststellung rechtfertigen.[245] Die Umsetzung der Expertenbestimmungsmethode erfordert ein spezifisches technisches Wissen über De-Identifikations- und Re-Identifikationsrisiken.[246]

---

[243] *Institut of Medicine of the National Academies*, Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research, 158 <https://www.nap.edu/read/12458/chapter/1> (letzter Aufruf 12.11.20).
[244] *Privacy Analytics,* White Paper Safe Harbor Vs the Statistical Method, 5 <http://gate250.com/tc2/SafeHarborvstheStatisticalMethodWhitePaper.pdf> (letzter Aufruf 18.11.20).
[245] <https://www.law.cornell.edu/cfr/text/45/164.514> (letzter Aufruf 18.11.20).
[246] *Privacy Analytics,* White Paper Safe Harbor Vs the Statistical Method, 4 <http://gate250.com/tc2/SafeHarborvstheStatisticalMethodWhitePaper.pdf> (letzter Aufruf 18.11.20).

Weder die HIPAA Privacy Rule noch die „Implementation Guidance, die vom Department of Health and Human Services Office of Civil Rights“[247] zur Verfügung gestellt werden, enthalten Standards oder Qualifikationen für den Experten. Sie legen auch nicht fest, wie das Risiko einer Re-Identifikation berechnet oder quantifiziert werden soll, noch geben sie das akzeptable Mindestrisiko einer Re-Identifikation an, außer dass es sehr gering sein muss. Die Expertenbestimmungsmethode legt fest, dass allgemein anerkannte statistische und wissenschaftliche Prinzipien und Methoden dem Experten bekannt sein und von ihm angewandt werden müssen, was ein Verständnis der einschlägigen Literatur über statistische Methoden zur De-identifikation voraussetzen würde.[248]

8.2 "Safe-Harbor"-Methode

Die "Safe-Harbor"-Methode ermöglicht es einer erfassten Organisation, Daten als de-identifizierte Daten zu behandeln, indem 18 spezifische Datentypen[249] für "die betroffene Person oder Verwandte, Arbeitgeber oder Menschen im selben Haushalt der Betroffenen" entfernt werden. Dazu gehören Namen, regionale Unterteilungen, Bezirk, Straßennamen, Postleitzahl, Telefonnummern, Faxnummer, E-Mailadresse, Sozialversicherungsnummern, Patienten IDs, IP-Adressen, jede andere eindeutige Identifikationsnummer, Merkmal oder Code etc.[250] Diese 18 Datentypen müssen entfernt oder generalisiert werden.[251] Beispiel für den Sammelbegriff "jede andere eindeutige Identifikationsnummer, jedes andere

---

[247] *Office of Civil Rights*, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.> (letzter Aufruf 18.11.20).

[248] *Garfinkel,* De-Identification of Personal Information, 23 <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf> (letzter Aufruf 20.11.20).

[249] „[...] A) Names (B) All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all ZIP codes with the same three initial digits co tains more than 20,000 people; and (2) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000 (C) All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older (D) Telephone numbers (E) Fax numbers (F) Email addresses (G) Social security numbers (H) Medical record numbers (I) Health plan beneficiary numbers (J) Account numbers (K) Certificate/license numbers (L) Vehicle identifiers and serial numbers, including license plate numbers (M) Device identifiers and serial numbers (N) Web Universal Resource Locators (URLs) (O) Internet Protocol (IP) addresses (P) Biometric identifiers, including finger and voiceprints (Q) Full-face photographs and any comparable images (R) Any other unique identifying number, characteristic, or code [...]”.

[250] *Garfinkel,* De-Identification of Personal Information, 23 f <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf> (letzter Aufruf 20.11.20).

[251] *Privacy Analytics,* White Papter Safe Harbor Vs the Statistical Method, 43<http://gate250.com/tc2/SafeHarborvstheStatisticalMethodWhitePaper.pdf> (letzter Aufruf 20.11.20).

Merkmal oder jeder andere Code" können Nummern der Aufzeichnungen klinischer Studien, eindeutige Schlüssel, die von einem Geburtsdatum abgeleitet sind, eindeutige Identifikatoren, die Patienten in elektronischen Krankenakten zugewiesen werden, sein. Alle anderen Informationen, die nicht durch diese 18 Datenkategorien abgedeckt sind, können in einen Datensatz aufgenommen werden, und der Datensatz würde als de-identifiziert betrachtet, wie z.B. Beruf des Patienten, diagnostische Codes, verabreichte Medikamente und angeordnete Labortests.[252] Bei beiden Methoden darf die betroffene Organisation, die die De-Identifikation durchführt, keine tatsächliche Kenntnis darüber haben, dass die Informationen allein oder in Kombination mit anderen Informationen verwendet werden könnten, um eine Person zu identifizieren, die Gegenstand der Informationen ist. Im Vergleich zur Methode der Feststellung durch Experten bietet die Safe-Harbor-Methode das Versprechen einer unkomplizierten Anwendung von Regeln, eines wiederholbaren Prozesses und eines sicheren Ergebnisses: eines Datensatzes, der rechtlich de-identifiziert ist.[253] Die Beweggründe für die De-Identifikation sind simpel. Wenn eine Person anhand eines Datensatzes nicht identifiziert werden kann, kann niemand direkt geschädigt werden, so dass diese Daten problemlos weitergegeben werden können.[254] Wenn Daten einmal als de-identifiziert gelten, werden sie nicht mehr vom HIPAA reguliert und können ohne Einschränkung für jeden Zweck verwendet werden.[255]

Die Safe Harbor Methode enthält keine explizite Aussage darüber, wie das Re-Identifikationsrisiko gemessen wird und was das akzeptable Re-Identifikationsrisiko oder die Risikoschwelle ist. Die vom „Department of Health and Human Services“ vorgelegten Konsultationen und Begründungen[256] zur Safe Harbor Methode deuten jedoch darauf hin, dass die Einzigartigkeit der Population das Maß für das Re Identifikationsrisiko ist. Es gab Versuche, das tatsächliche Re-Identifikationsrisiko von Safe-Harbor-Datensätzen empirisch zu messen. Eine oft zitierte Studie[257] kam zu dem Schluss, dass 0,04 % der US-Bevölkerung in Bezug auf Geschlecht, Alter in Jahren und die ersten drei Ziffern ihrer

[252] *El Emam*, Guide to the De-Identification of Personal Health Information (2013) 13 ff.
[253] *Garfinkel,* De-Identification of Personal Information, 24 <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf> (letzter Aufruf 22.11.20).
[254] *Sweeney/Von Loewenfeldt/Perry,* Saying it’s Anonymous Doesn't Make It So: Re-identifications of “anonymized” law school data, 12 <https://techscience.org/a/2018111301/> (letzter Aufruf 22.11.20).
[255] *McGraw,* Building public trust in uses of Health Insurance Portability and Accountability Act de-identified data, Journal of the American Medical Informatics Association (2013) 29 (30).
[256] *Department of Health and Human Services*, Standards for privacy of individually identifiable health information, <https://www.govinfo.gov/content/pkg/FR-2002-08-14/pdf/02-20554.pdf> (letzter Aufruf 16.11.20).
[257] *Sweeney*, Patient Identifiability in Pharmaceutical Marketing Data, <https://dataprivacylab.org/projects/identifiability/pharma1.pdf> (letzter Aufruf 16.11.20).

Postleitzahl einzigartig ist. Eine wichtige Annahme, die hier getroffen wurde, ist, dass der Widersacher, der eine Re-Identifizierung versucht, nicht weiß, wer sich in dem Datensatz befindet. Wenn es sich bei einem bestimmten Datensatz beispielsweise um eine Zufallsstichprobe der US-Bevölkerung handelt, ist die Annahme im Prinzip richtig, dass der Opponent nicht weiß, wer sich in diesem bestimmten Datensatz befindet. Das Wissen darüber, welche Mittel ein Dritter haben könnte, kann nicht als irrelevant für die Bestimmung des Re-Identifikationsrisikos abgetan werden. Personen können offenbaren, dass sie selbst im Datensatz enthalten sind, z.B. indem sie gegenüber ihren Kollegen oder in ihren sozialen Netzwerken erwähnen, dass sie an einer Studie teilnehmen. Es kann allgemein bekannt sein, wessen Daten sich im Datensatz befinden, wie zum Beispiel bei Interviews in einem Unternehmen, bei denen die Teilnehmer einen halben Tag Arbeit für die Teilnahme versäumt haben. Der Datensatz kann jeden in einer bestimmten Gruppe repräsentieren; zum Beispiel ein Register von Personen mit einer seltenen und sichtbaren angeborenen Anomalie. Wenn jemand diese Anomalie hat, wird sie mit einer hohen Wahrscheinlichkeit in dieses Register aufgenommen, oder wenn es in einem Dorf nur eine Hausärztin gibt, dann werden womöglich alle Bewohner in einem Datensatz dieser Ärztin erfasst.[258] Safe Harbor berücksichtigt nicht die Einzigartigkeit von genetischen Daten. Daher werden sie als Teil der 18 Datentypen nicht ausdrücklich eliminiert oder verändert. So berücksichtigt Safe Harbor beispielsweise auch keine Längsschnittdaten, die Informationen über die Dauer eines Krankenhausaufenthalts und die Zeit zwischen den Aufenthalten enthalten können.[259]

9. Verordnung (EU) 2018/1807 („Free Flow of Data“)

Die Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union[260], die seit Mai 2019 in Kraft ist, soll regeln, wie nicht-personenbezogene Daten verarbeitet werden dürfen. Sie soll Rechtssicherheit für Unternehmen schaffen, die aufgrund dieser Verordnung ihre Daten nun überall in der EU verarbeiten können, und soll die Möglichkeit bieten, nicht mehr von bestimmten Anbietern ab-

[258] *El Emam*, Guide to the De-Identification of Personal Health Information (2013) 15 f.
[259] *El Emam*, Methods for the de-identification of electronic health records for genomic research, Genome Med (2011) 1 (3).
[260] Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, ABl 2018/303.

hängig zu sein.[261] Nicht-personenbezogene Daten sind eben all jene Daten die nicht unter die Definition personenbezogener Daten der DSGVO fallen. Entweder waren sie nie personenbezogen, wie Sachdaten z.B. von Sensoren generierte Wetterdaten, oder technische Daten über den Wartungsbedarf einer Maschine, oder Daten, die zwar einmal personenbezogen waren aber anonymisiert wurden.[262] Berücksichtigt werden auch gemischte Datensätze, die aus personenbezogenen und nicht-personenbezogenen Daten bestehen. Sind die Datensätze trennbar, gelten die jeweils anwendbaren Verordnungen. Ist eine Trennung von personenbezogenen und nicht-personenbezogenen Datensätzen nicht möglich, kommt die DSGVO vollumfänglich zur Anwendung.[263] Beiden gemeinsam ist, dass ihre jeweiligen Rahmenbedingungen zum freien Datenverkehr beitragen sollen.[264] Der Kern der beiden Verordnungen ist jedoch gegensätzlich. In der DGSVO stehen der Mensch und seine personenbezogenen Daten im Vordergrund bei der Verordnung über den freien Verkehr nicht-personenbezogener Daten der ökonomische Vorteil wirtschaftlich tätiger Institutionen.

9.1 Anonymisierung anhand der Verordnung (EU) 2018/1807 („Free Flow of Data“)

Gemäß Erwägungsgrund 9 der Verordnung sind aggregierte Daten ein Beispiel für nicht personenbezogene Daten oder anonymisierte Datensätze für Analysen mit großen Datenmengen, Daten für die Präzisionslandwirtschaft, z.B. zur Optimierung des Einsatzes von Pestiziden oder Wasser, oder Daten für die Instandhaltung von industriellen Maschinen. Der letzte Satz des Erwägungsgrundes enthält eine Herleitung einer Definition der Anonymisierung. Demzufolge können anonymisierte Daten mit neuen technologischen Entwicklungen wieder in personenbezogene Daten umgewandelt werden – in diesem Fall handelt es sich um personenbezogene Daten, die unter die Bestimmungen der DSGVO fallen.[265] Hier wird im Gegensatz zur absoluten Anonymisierungstheorie davon ausgegan-

[261] MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nichtpersonenbezogener Daten in der Europäischen Union, COM (2019) 250 final, 2.
[262] MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nichtpersonenbezogener Daten in der Europäischen Union, COM (2019) 250 final, 5 f.
[263] MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nichtpersonenbezogener Daten in der Europäischen Union, COM (2019) 250 final, 9.
[264] MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nichtpersonenbezogener Daten in der Europäischen Union, COM (2019) 250 final, 21.
[265] ErwGr 9 VO (EU) 2018/1807.

gen, dass die Anonymisierung reversibel ist, was impliziert, wie es auch die Artikel-29-Datenschutzgruppe seinerzeit in ihrer Stellungnahme formulierte, dass die Anonymisierung keine einmalige Maßnahme ist und dass die bestehenden Restrisiken ständig neu beurteilt werden müssen.[266] Wenn anonymisierte Daten vorliegen, aber aufgrund technologischer Entwicklungen die Möglichkeit der Re-Identifikation besteht, dann sind diese Daten bereits aufgrund der Möglichkeit nicht mehr als anonym, sondern als personenbezogene Daten anzusehen.[267]

Im Gegensatz zu Erwägungsgrund 26 der DSGVO konzentriert sich der Gesetzgeber hier nur auf technologische Entwicklungen als Ausgangspunkt für die Beurteilung der Anonymisierung, die in der Praxis meist unberücksichtigt bleiben, weil sie nicht fassbar sind und zu einer Ausweitung der Anwendbarkeit des Datenschutzrechts führen würden. Erwägungsgrund 26 umfasst alle Mittel, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, einschließlich technologischer Entwicklungen. Nach allgemeinem Ermessen könnte man meinen, dass nur solche technologischen Entwicklungen zur Anwendung kommen, die in naher Zukunft und mit hoher Wahrscheinlichkeit zu erwarten sind.[268] Wenn die Möglichkeit, anonymisierte Daten mit Hilfe technologischer Entwicklungen in personenbezogene Daten umzuwandeln, auch wenn nur jene in naher Zukunft berücksichtigt werden, bereits ausreicht, ohne dass bereits eine tatsächliche Umwandlung stattgefunden hat, damit diese Daten als personenbezogen gelten, erscheint ein wesentlich strengerer Ansatz bei der Definition der Anonymisierung, wie im Erwägungsgrund 26 DSGVO, naheliegend. Denn die Möglichkeit neuer technischer Entwicklungen kann nie zur Gänze ausgeschlossen werden.

In den zugehörigen Leitlinien verweist die Europäische Kommission erneut auf den Erwägungsgrund 26[269] was auf eine Tendenz hindeutet, dass beide Definitionen im Einklang zu sehen sind und der Gesetzgeber insbesondere die Einbeziehung technologischer Entwicklungen in die Risikoabschätzung durch deren Verankerung in Erwägungsgrund 9 noch einmal hervorheben möchte. Relativ ist der Personenbezug faktisch nur insofern, als Da-

[266] *Art-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken WP 216 0829/14/DE, 4 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf> (letzter Aufruf 11.12.20).
[267] ErwGr 9 VO (EU) 2018/1807.
[268] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 313 f.
[269] MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nichtpersonenbezogener Daten in der Europäischen Union, COM (2019) 250 final, 6.

ten, die heute als anonym gelten, durch die Entwicklung der Technologie in der Zukunft identifiziert werden können.[270]

10. Anonymisierung anhand des Daten-Governance-Gesetzes (Entwurf)

Die EU-Kommission hat im November 2020 einen Gesetzesentwurf vorgelegt, um den Austausch von Datensätzen innerhalb der Europäischen Union zu erleichtern. Ziel ist es sein, den Datenaustausch innerhalb der EU und zwischen den verschiedenen Sektoren zu fördern und dadurch für die Gesellschaft einen Nutzen zu schaffen, die Kontrolle und das Vertrauen, sowohl der Bevölkerung, als auch der Unternehmen in ihre Daten zu erhöhen und ein alternatives europäisches Modell für die Datenverarbeitungspraktiken der großen Technologieplattformen bereitzustellen.[271] Ein Vorteil soll darin bestehen, dass der Wirtschaft und Gesellschaft in der EU mehr Daten zur Verfügung gestellt werden. Europäische Datenräume sollen den vertraulichen und kostengünstigen Zugang zu Daten aus der gesamten EU, sowohl aus dem öffentlichen Sektor, als auch dem privat-wirtschaftlichen Bereich ermöglichen.[272] Anders als die DSGVO, erklärt sich das Daten-Governance-Gesetz sowohl für personenbezogene, als auch für nicht-personenbezogene Daten als anwendbar. Folglich verwendet auch der vorliegende Gesetzesentwurf eine dem Datenschutzrecht fremde Terminologie und schafft eine Form des Eigentums an solchen Daten im Sinne einer Dateninhaberschaft.[273]

Das Kapitel II des Entwurfes behandelt die „WEITERVERWENDUNG[274] BESTIMMTER KATEGORIEN GESCHÜTZTER DATEN IM BESITZ ÖFFENTLICHER STELLEN“. Dieses Kapitel gilt für jene öffentlichen Stellen[275], die unter anderem die Hoheit über personenbe-

[270] *Weichert*, Der Personenbezug von Geodaten, DuD (2007), 17 (19).
[271] *Europäische Kommission*, Pressemitteilung Kommission schlägt Maßnahmen zur Förderung der gemeinsamen Datennutzung und zur Unterstützung europäischer Datenräume vor, <https://ec.europa.eu/commission/presscorner/detail/de/ip_20_2102> (letzter Aufruf 30.11.20).
[272] *Europäische Kommission*, Verordnung über Daten-Governance – Fragen und Antworten, <https://ec.europa.eu/commission/presscorner/detail/de/QANDA_20_2103> (letzter Aufruf 30.11.20).
[273] *Forgó,* Datenaltruismus – mit Formular und Behörde, Der Standard (2020), <https://www.derstandard.at/story/2000122074854/datenaltruismus-mit-formular-und-behoerde> (letzter Aufruf 02.01.2021).
[274] Art 2 Z 2 Daten-Governance-Gesetz „Weiterverwendung“ die Nutzung von Daten, die im Besitz öffentlicher Stellen sind, durch natürliche oder juristische Personen für kommerzielle oder nichtkommerzielle Zwecke, die sich von dem ursprünglichen Zweck im Rahmen des öffentlichen Auftrags, für den die Daten erstellt wurden, unterscheiden, abgesehen vom Austausch von Daten zwischen öffentlichen Stellen ausschließlich im Rahmen der Erfüllung ihres öffentlichen Auftrags;“.
[275] Art 2 Z 11 Daten-Governance-Gesetz „öffentliche Stelle“ den Staat, Gebietskörperschaften, Einrichtungen des öffentlichen Rechts oder Verbände, die aus einer oder mehreren dieser Körperschaften oder einer oder mehreren dieser Einrichtungen des öffentlichen Rechts bestehen;“.

zogene Daten haben, welche unter den Datenschutz fallen.[276] Demzufolge haben öffentliche Stellen, welche gemäß nationalem Recht dazu legitimiert wurden, das Recht zu entscheiden, ob sie den Zugang zu den Daten zur weiteren Verwendung gewähren oder verweigern. In jedem Fall sind die Bedingungen für die Gewährung des Zugangs für eine solche Weiterverwendung öffentlich zugänglich zu machen.[277]

Artikel 5 Abs. 3 Daten-Governance-Gesetz (Fassung in englischer Sprache): *„Public sector bodies **may impose an obligation** to re-use only pre-processed data where such pre-processing **aims to anonymize** or pseudonymise **personal data*** […]." [Hervorhebungen durch die Verfasserin]

Nach diesem Artikel haben öffentliche Stellen das Recht, Datenverarbeitern die Verpflichtung aufzuerlegen, dass nur vorverarbeitete Daten weiterverwendet werden dürfen, wenn diese Vorverarbeitung den Zweck hat, personenbezogene Daten zu anonymisieren oder zu pseudonymisieren oder vertrauliche Geschäftsinformationen und Geschäftsgeheimnisse zu löschen.

Die Verpflichtung, dass die Vorverarbeitung den Zweck haben muss, personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, impliziert, dass es nicht erforderlich ist, dass dies tatsächlich geschieht. Nach dem Wortlaut reicht es aus, zu versuchen, sie zu anonymisieren oder pseudonymisieren, ohne die Verpflichtung, tatsächlich nur anonymisierte oder pseudonymisierte Daten weiter zu verwenden. Die Pflicht zur Pseudonymisierung von personenbezogenen Daten ergibt sich bereits aus dem Prinzip der Datenminimierung nach Artikel 5 Abs. 1 lit. c DSGVO.[278] Demnach müssen personenbezogene Daten angemessen, zweckentsprechend und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.[279] Im Zusammenhang mit der Verarbeitung für Archivierungszwecke im öffentlichen Interesse, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke müssen Datenverarbeiter vor der Verwendung der personenbezogenen Daten auch prüfen, ob diese Zwecke mit anonymisierten Daten erfüllt

[276] Art 3 Abs 1 Daten-Governance-Gesetz.
[277] Art 5 Abs 1 Daten-Governance-Gesetz.
[278] *Hödl* in Knyrim (Hrsg), DatKomm Art 4 DSGVO Rz 63 (Stand 1.12.2018); *Bergauer/Gosch*, Die Pseudonymisierung personenbezogener Daten gemäß der DSGVO - zugleich eine Replik auf Geuer/Wollmann, Verarbeitung von pseudonymen Daten mit besonderem Fokus auf Art 26 und 28 DS-GVO, jusIT 2020 63 (66); DSB 13. 9. 2018, DSB-D123.070/0005-DSB/2018.
[279] Art 5 Abs 1 lit c VO (EU) 2016/679.

werden können. Falls die Verwendung anonymisierter Daten nicht möglich ist, muss geprüft werden, ob pseudonymisierte Daten ausreichen. Ist auch dies für die genannten Zwecke nicht zweckmäßig, muss der Schutz der betroffenen Personen durch andere adäquate Maßnahmen gewährleistet werden.[280] Der derzeitige Verordnungstext, der die Weiterverwendung personenbezogener Daten, die sich im Besitz von öffentlichen Stellen befinden, erlaubt, ohne konkrete Vorgaben für den Schutz dieser Daten zu machen, sondern lediglich ein wünschenswertes Ziel festschreibt, ohne es erreichen zu müssen, verhindert einen umfassenden Schutz der Rechte der Betroffenen.

Eine Definition der Anonymisierung ist im vorgeschlagenen Verordnungstext nicht vorgeschrieben. Lediglich im derzeitigen Erwägungsgrund 11 findet sich ein Ansatz einer Herleitung (Fassung in englischer Sprache): „[...] *Depending on the case at hand, before its transmission, personal data* ***should be fully anonymised****, so as to* ***definitively not allow the identification*** *of the* ***data subjects****,* [...]*"* [Hervorhebungen durch die Verfasserin]

„Definitiv ausgeschlossen" suggeriert eine Absolutheit, die dem Ansatz der Anonymisierung des Erwägungsgrundes 26 des DSGVO widerspricht, da dieser eine risikobasierte Definition der Anonymisierung vorsieht.

11. Ein Schutzkonzept für anonymisierte Daten

Der Begriff "Datenschutz" ist nicht neu. Er wurde bereits in den 1960er und 1970er Jahren eingeführt. Zweck des Datenschutzes ist es, den Einzelnen vor dem Missbrauch seiner personenbezogenen Daten zu schützen. Der Datenschutz ist von der Vorstellung bestimmt, dass jeder Mensch das Recht hat, selbst zu entscheiden, was mit seinen personenbezogenen Daten passiert.[281] Der Einzelne soll vor Verletzungen seiner Persönlichkeitsrechte durch den Umgang mit seinen personenbezogenen Daten geschützt werden.[282]

Was aber passiert, wenn eine Person in einer Personengruppe aufgeht und nicht mehr bestimmbar oder identifizierbar ist? Hat diese Person ihr Recht verloren, über ihre Daten

[280] *Pauly,* in Paal/Pauly (Hrsg), Datenschutz-Grundverordnung Art 89 Rz 12 (2017).
[281] *Souhrada-Kirchmayer*, Zur Geschichte des europäischen Datenschutzrechts, in Olechowski/ Neschwara/ Lengauer (Hrsg), Grundlagen der österreichischen Rechtskultur (2010) 499 f.
[282] *Jahnel/Pallwein-Prettner/Marzi*, Datenschutzrecht[2] (2018) 17.

zu entscheiden, weil sie nicht mehr auf sie als Einzelperson zurückgeführt werden können, aber dennoch ursprünglich von ihr stammen? Sind diese Daten die einmal einen Personenbezug hatten weniger schützenswert, wenn sie den Einzelpersonenbezug verlieren? Sind es dann Daten, die nicht schutzwürdig sind? Ist die Abgrenzung des Geltungsbereichs des Datenschutzrechts durch personenbezogene oder nicht-personenbezogene Daten im 21. Jahrhundert noch angemessen?

Dies sind Fragen, die gestellt werden müssen. Zumal der europäische Gesetzgeber selbst in seiner jüngst erlassenen Verordnung darauf hinweist, dass die Möglichkeit der Konvertierung der Anonymisierung bereits den Anwendungsbereich des Datenschutzrechts eröffnet[283] und die Europäische Kommission in der begleitenden Leitlinie selbst ausführt, dass die Anonymisierung nicht als absolut angesehen werden kann und es ein fortlaufender Prozess sein muss, zu prüfen ob Daten tatsächlich noch anonym sind.[284]

11.1 Gruppen

Eine Aussage über Personen in einer Gruppe kann personenbezogen sein, wenn sich die Aussage auf alle Personen in der Gruppe bezieht. Grundsätzlich ist es für die Bestimmbarkeit nicht erforderlich, dass sich eine Angabe nur auf eine Person bezieht. Eine Angabe kann sich auf zwei oder mehrere Personen beziehen. (z.B. Christoph und Anna haben zwei Kinder)[285] Ab welchem Punkt eine Person in einer Gruppe nicht mehr identifizierbar ist, ist umstritten. Geht man davon aus, dass 4 Personen in einer Gruppe identische Merkmale haben, so kann man jeder dieser 4 Personen eine Wahrscheinlichkeit von 25% zuordnen. Dies solle aber nur eine Information über eine Wahrscheinlichkeit sein. Je niedriger oder höher die Wahrscheinlichkeit liegt, desto lockerer oder enger ist der Personenbezug herzustellen.[286] Hierbei bleibt unberücksichtigt, dass jede einzelne Person diese Merkmale hat, so dass die 25% Wahrscheinlichkeit, diese bestimmten Merkmale zu haben, bereits eine Identifizierbarkeit vermag. In einer Empfehlung aus dem Jahr 2015 verwies die österreichische Datenschutzbehörde auf eine Empfehlung der damaligen Datenschutzkommission, in der sie feststellte, dass die Zahl von 5 Personen sicherzustellen

[283] ErwGr 9 VO (EU) 2018/1807.
[284] MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nichtpersonenbezogener Daten in der Europäischen Union, COM (2019) 250 final, 6.
[285] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 314.
[286] *Weichert*, Der Personenbezug von Geodaten, DuD (2007), 17 (19).

scheint, dass es nicht möglich ist, Rückschlüsse auf bestimmte Personen zu ziehen. Zudem wurde empfohlen, eine Trennung in männliche und weibliche Personen - und damit auch die Identifizierung von für diese Gruppe typischen Krankheiten (wie z.B. Erkrankungen der Geschlechtsorgane) - nur dann vorzunehmen, wenn mehr als fünf Personen zu einer dieser Gruppen gehören.[287] Eine Information über eine Personengruppe ist bereits eine Information darüber, dass jemand zu einer bestimmten Personengruppe gehört. Allein diese Information kann zu einer Diskriminierung des Einzelnen führen. Wobei es unerheblich ist, ob eine Information eindeutig einer Person dieser Gruppe zugeordnet werden kann. Genau wie eine Aussage, die für die Personengruppe, aber nicht für jeden Einzelnen gilt, ist sie für jemanden anderen nicht zutreffend.[288] Haase führt hierzu ein anschauliches Beispiel an: *„Für ein Krankenhaus ist eine Stelle zu besetzen. Der Krankenhausbetreiber erfährt, dass drei der acht Bewerber eine höchst ansteckende Krankheit haben. Angenommen die Angabe über diese Krankheut könnte nicht den einzelnen Personen zugeordnet werden, wäre die Wahrscheinlichkeit hoch, dass keiner der Bewerber genommen wird.“*[289] Schon die Aussage über Personen einer Gruppe kann Auswirkungen auf die gesamte Gruppe als solche haben. Der Telos des Datenschutzrechts muss dahingehend erweitert werden, dass nicht nur Daten im Sinne von Informationen über eine Person schützenswert sind, sondern auch die Personengruppe als solche.[290]

11.1.1 Havasupai Indian Tribe Case

Ein anschauliches Beispiel für die Folgen des Missbrauchs von Daten, die sich auf eine Gruppe von Menschen beziehen, ist die Studie über den Havasupai-Stamm. Im Jahr 2004 leitete der Volksstamm eine Klage gegen die Arizona State University (ASU) ein, in der der Stamm behauptete, dass Forscher an der ASU Blutproben von Mitgliedern des Stammes für die Erforschung der genetischen Grundlagen von Diabetes gesammelt hätten, die Blutproben anschließend jedoch für eine Vielzahl von Forschungsarbeiten verwendet hätten, darunter Migration, Inzucht und Schizophrenie, die nicht direkt für Diabetes relevant seien.[291] Die Havasupai reichten mehrere Klageschriften ein. Sie behaupteten, dass die un-

[287] DSB 30.03.2015, DSB-D215.611/0003-DSB/2014.
[288] *Pahlen-Brandt*, Datenschutz braucht scharfe Instrumente Beitrag zur Diskussion um „personenbezogene Daten“, DuD (2008), 34 (37).
[289] *Haase,* Datenschutzrechtliche Fragen des Personenbezugs (2015) 315.
[290] *Pahlen-Brandt*, Datenschutz braucht scharfe Instrumente Beitrag zur Diskussion um „personenbezogene Daten“, DuD (2008), 34 (37).
[291] *Miller*, Sharing clinical research data in the United States under the health insurance portability and accountability act and the privacy rule, Trials (2010), 1 (3).

sachgemäße Verwendung ihrer Blutproben sowohl in ihre Privatsphäre als auch in die "kulturelle und religiöse Privatsphäre" des Stammes eingedrungen sei und ihnen schweren Schaden, extreme Bedrängnis und emotionales Trauma zugefügt habe. Darüber hinaus behaupteten sie, dass dieses Fehlverhalten zu einem wachsenden Misstrauen gegenüber der medizinischen Versorgung geführt habe, da viele Stammesmitglieder nun Angst hätten, in die Gesundheitsklinik zu gehen, ärztliche Hilfe zu suchen und Blutproben für medizinische Diagnose oder Behandlung zu geben.[292] Der Fall des Havasupai-Stammes zeigt, dass selbst wenn sich die Ergebnisse selbst nicht auf ein Individuum beziehen, den Forschungsteilnehmenden ein Nachteil daraus erwachsen kann. Unter diesen Umständen kann eine Forschung, die stigmatisierende und störende Ergebnisse liefert, zu einer schweren kollektiven Benachteiligung führen, der sich negativ auf alle Gruppenmitglieder auswirkt.[293] Auch eine Anonymisierung der Proben bzw. der aus der Analyse resultierenden Daten, obwohl dies bei genetischen Daten zweifelhaft ist, hätte die Stammesmitglieder nicht davor bewahrt.[294]

Die Universität zahlte 700.000 US-Dollar an 41 Mitglieder des Stammes und gab deren Blutproben zurück. Damit wurden die Vorwürfe beigelegt, dass Forschende der Universität die Blutproben von Stammesmitgliedern unrechtmäßig für genetische Forschung verwendet hatten. Der Fall wirft ein Licht auf die ungelöste Kontroverse darüber, was eine angemessene informierte Zustimmung für biologische Proben darstellt, die zu Forschungszwecken entnommen wurden, um sie zu lagern und in zukünftigen, möglicherweise nicht verwandten Studien zu verwenden.[295]

11.2 Big Data mit anonymen Daten

„Big Data" bezeichnet große Datenmengen, „[...] *die u.a. aus Bereichen wie Internet und Mobilfunk, Finanzindustrie, Energiewirtschaft, Gesundheitswesen und Verkehr und aus Quellen wie intelligenten Agenten, sozialen Medien, Kredit- und Kundenkarten, Smart-Metering-Systemen, Assistenzgeräten, Überwachungskameras sowie Flug- und Fahrzeu-*

[292] *Van Assche/Gutwirth/Sterckx,* Protecting Dignitary Interests of Biobank Research Participants: Lessons from Havasupai Tribe v Arizona Board of Regents, Law, Innovation and Technology (2013), 54 (61).
[293] *Van Assche/Gutwirth/Sterckx,* Protecting Dignitary Interests of Biobank Research Participants: Lessons from Havasupai Tribe v Arizona Board of Regents, Law, Innovation and Technology (2013), 54 (70 f).
[294] *Van Assche/Gutwirth/Sterckx,* Protecting Dignitary Interests of Biobank Research Participants: Lessons from Havasupai Tribe v Arizona Board of Regents, Law, Innovation and Technology (2013), 54 (68).
[295] *Harmon*, Indian Tribe Wins Fight to Limit Research of Its DNA, The New York Times (2010) <https://www.nytimes.com/2010/04/22/us/22dna.html> (letzter Aufruf 02.01.2021).

gen stammen [...]*"*[296] oder auf eine andere Weise gesammelt, zugänglich gemacht und statistisch analysiert werden. Big Data verspricht, Probleme zu identifizieren und zu lösen, indem die Daten analysiert werden, bevor sie sich in der Gesellschaft auswirken.[297] Die Neuerung bei Big Data besteht darin, die Effizienz der statistischen Auswertungen zu verbessern.[298] Die Analyse großer Datenmengen kann helfen, die Makroebene statistischer Korrelationen zu bestimmen und diese zur Erklärung aller denkbaren Zusammenhänge zu nutzen. Das primäre Ziel solcher Analysen ist die Vorhersage und Steuerung von Ereignissen. Dabei steht nicht der einzelne Mensch in einer Gruppe im Vordergrund, sondern seine gesellschaftliche Rolle - als Patient, als Konsument, als Mitbürger oder als Wähler.[299] Werden Daten einer Person A, B und C verwendet, die vor der Analyse anonymisiert werden, besteht kein unmittelbares Risiko für den Schutz der personenbezogenen Daten dieser Personen. Wenn das anonymisierte Ergebnis als Grundlage für die Erstellung von Profilen der Personen D, E und F verwendet wird, wird diese nicht personenbezogene Analyse diese Personen dennoch betreffen, wenn auch nicht unmittelbar.[300] Statistische Aussagen gelten für alle. Wer seine Daten, zum Beispiel in einer Umfrage für eine Big Data-Sammlung preisgibt und sie speichern und analysieren lässt, schafft nicht nur Risiken für sich selbst, sondern immer auch für andere, die sich in einer ähnlichen Situation befinden. Die Auswertungen, die aus den Daten derjenigen generiert werden, die ihre Einwilligung erteilt haben, gelten auch für diejenigen, die es abgelehnt haben, ihre Daten zur Verfügung zu stellen.[301] Bereits 1969 stellte das deutsche Bundesverfassungsgericht in seinem Beschluss fest, dass der Umgang mit Daten nicht nur dann problematisch sein kann, wenn ein unmittelbarer Personenbezug besteht. (*„Mit der Menschenwürde wäre es nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist.")*[302]

---

[296] *Bendel*, Big Data, Gabler Wirtschaftslexikon <https://wirtschaftslexikon.gabler.de/definition/big-data-54101> (letzter Aufruf 02.01.2020).
[297] *Weichert,* Big Data und Datenschutz - Chancen und Risiken einer neuen Form der Datenanalyse, ZD (2013), 251 ff.
[298] *Richter,* Big Data, Statistik und die Datenschutz-Grundverordnung, DuD (2016), 581 (582).
[299] *Roßnagel*, Big Data – Small Privacy? - Konzeptionelle Herausforderungen für das Datenschutzrecht, ZD (2013), 562.
[300] *Richter,* Big Data, Statistik und die Datenschutz-Grundverordnung, DuD (2016), 581 (582).
[301] *Roßnagel*, Big Data – Small Privacy? - Konzeptionelle Herausforderungen für das Datenschutzrecht, ZD (2013), 562 (566).
[302] BVerfG, 16.07.1969 - 1 BvL 19/63.

11.3 Gesetzlich verankertes Re-Identifikationsverbot

Das in Japan geltende Datenschutzgesetz sieht eine eigene definierte Kategorie anonymisierten Daten vor: „Anonymisiert verarbeitete Informationen" („anonymously processed information").[303] Anonym verarbeitete Informationen bedeutet in diesem Gesetz Informationen über eine Person, die durch die Verarbeitung personenbezogener Daten erlangt werden können, so dass es nicht möglich ist, eine bestimmte Person zu identifizieren, wenn entsprechende festgelegte Maßnahmen ergriffen werden, noch kann der Personenbezug wiederhergestellt werden.[304] Das japanische Kabinett setzte einen Ausschuss von Juristen und Technikern ein, der sich mit der Frage befasste, ob eine Anonymisierung allein mit technischen Methoden möglich ist. Dieser kam zu dem Ergebnis, dass eine absolute Anonymisierung allein mit technischen Maßnahmen nicht realisierbar sei und daher eine zusätzliche gesetzliche Regelung notwendig ist.[305] Sie basiert auf der Annahme, dass immer ein Restrisiko der Re-Identifikation besteht und daher dem Datenverarbeiter besondere Pflichten auferlegt werden, dass dieser jedoch keinen Erlaubnistatbestand für die Verarbeitung dieser Daten an sich benötigt.[306] Das Datenschutzgesetz schreibt spezifische, vom Datenverarbeiter zu ergreifende Maßnahmen zur Datensicherheit zwingend vor. Dazu gehören die Löschung des Personenbezuges sowie die Verwendung anonymisierter Daten. Eine Besonderheit des japanischen Datenschutzgesetzes ist das gesetzliche Verbot der Re-Identifikation, welches dem europäischen Datenschutzrecht unbekannt ist. Allerdings sieht das japanische Datenschutzgesetz bei Nichtbeachtung keine Sanktionen vor.[307]

Der Ansatz, ein gesetzliches Verbot der Re-Identifizierung einzuführen, ist durchaus reizvoll. Damit wird anerkannt, dass eine absolute Anonymisierung faktisch nicht möglich ist, zumindest keine, die nicht ständig neu bewertet werden muss. Gäbe es ein entsprechen-

---

[303] *Fujiwara,* Die datenschutzrechtliche Diskussion um autonomes Fahren in Japan, in Roßnagel/Hornung (Hrsg), Grundrechtsschutz im Smart Car. DuD-Fachbeiträge (2019) 446.
[304] *Geminn/Laubach/Fujiwara,* Schutz anonymisierter Daten im japanischen Datenschutzrecht, ZD (2018), 413 (417); <https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf> (letzter Aufruf 07.12.20).
[305] *Geminn/Laubach/Fujiwara,* Schutz anonymisierter Daten im japanischen Datenschutzrecht, ZD (2018), 413 (414).
[306] *Fujiwara,* Die datenschutzrechtliche Diskussion um autonomes Fahren in Japan, in Roßnagel/Hornung (Hrsg), Grundrechtsschutz im Smart Car. DuD-Fachbeiträge (2019) 446.
[307] *Roßnagel/Geminn*, Stärkung der Datenschutzprinzipien, in Roßnagel/Hornung in Zusammenarbeit mit dem TeleTrusT Deutschland e.V, Datenschutz-Grundverordnung verbessern[1] (2020) 5 (167).

des gesetzliches Re-Identifizierungsverbot für diejenigen Verarbeitungsvorgänge, die keinen Personenbezug erfordern, würde sich eine Diskussion über die Perspektive der Bestimmbarkeit möglicherweise erübrigen. Wird eingeräumt, dass immer ein Restrisiko der Identifizierbarkeit verbleibt, dieses Risiko aber durch ein gesetzlich sanktioniertes Verbot minimiert wird, entspricht dies jedenfalls dem datenschutzrechtlichen Schutzgedanken gegenüber dem Einzelnen.

12. Schlussfolgerung

Die uneinheitliche Gesetzgebung und Auslegung der Definition der Anonymisierung, sei es auf europäischer, mitgliedstaatlicher oder drittstaatlicher Ebene, führt zu Rechtsunsicherheit bei Anwendern und Betroffenen. Die Lösung ist möglicherweise nicht eine allumfassende Definition von anonymisierten Daten bzw. der Anonymisierung, sondern verschiedene Definitionen, die je nach Datenkategorie, Zweck der Verarbeitung und dem potenziellen Risiko für die Rechte und Freiheiten der betroffenen Personen variieren. Personenbezogene Daten besonderer Kategorie wird bereits ein höheres Schutzniveau zugesprochen.[308] Diese Überlegung auf den Grad der Anonymisierung anzuwenden und an unterschiedliche Verarbeitungssituationen anzupassen, könnte eine Möglichkeit sein, mehr Rechtssicherheit in den jeweiligen Anwendungsbereichen zu schaffen.

Die Vermischung von alten und neuen Rechtsdefinitionen und die unscharfe Abgrenzung zwischen Pseudonymisierung und Anonymisierung in den dargestellten österreichischen Bestimmungen erschweren die rechtskonforme Einhaltung und einheitliche Auslegung dieser. Eine Nachjustierung ist hier zwingend erforderlich.

Fakt des 21. Jahrhunderts ist es, dass nicht nur die technologischen Möglichkeiten rasant voranschreiten, sondern dass auch Daten und humanes Material unter dem Deckmantel der Forschung in einem Ausmaß gesammelt, genutzt und ausgetauscht werden, das kaum noch zu fassen ist. Die Möglichkeiten, sich zusätzliches Wissen anzueignen, egal ob es sich um ein Unternehmen, eine staatliche Einrichtung oder eine natürliche Person selbst handelt, sind bei der Auslegung der möglichen Mittel nicht mehr von der Hand zu weisen. Der Telos des Datenschutzrechts ist es, die Menschen hinter den Daten zu schützen und ihr Selbstbestimmungsrecht zu wahren. Der Gesetzgeber hat die Aufgabe umfassende

[308] ErwGr 51 S1 VO (EU) 2016/679.

Garantien zum Schutz der Grundrechte und Grundfreiheiten, jeder einzelnen Person, bei der Verarbeitung ihrer personenbezogenen Daten vorzusehen. Die rechtlichen Möglichkeiten, die der Gesetzgeber Datenverarbeitern im Sinne der Wissenschaftsfreiheit einräumt, erfordern gerade in Zeiten unbegrenzter Erhebungs- und Austauschmöglichkeiten von Daten ein Überdenken des Schutzkonzepts dieser und der rechtlichen Anforderungen, um nicht nur die Einzelperson bei der Verarbeitung ihrer personenbezogenen Daten zu schützen, sondern auch das Missbrauchspotential von Daten zu erkennen, die weder direkt noch indirekt einer Person zuordenbar sind. Es liegt in der Verantwortung der Gesetzgeber sowie jedes Einzelnen, einen umfassenden Schutz aller Daten, die von einer natürlichen Person stammen, stammen könnten oder stammten, zu gewährleisten.

13. Abstract

Zur Einführung in die Thematik wird die Definition der Anonymisierung in der EU-Datenschutzrichtlinie und der Datenschutz-Grundverordnung sowie die Theorie der Perspektive der Bestimmbarkeit erörtert und die Problematik der Anonymisierung von genetischen Daten skizziert. Im Folgenden wird die Definition der Anonymisierung in ausgewählten relevanten Gesetzen in Österreich, die bei der Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken anzuwenden sind, analysiert. Anschließend werden weitere europäische Rechtsakte, die ebenfalls eine Definition der Anonymisierung enthalten, und das US-Gesetz HIPAA (Health Insurance Portability and Accountability Act) vorgestellt. Der Begriff der Anonymisierung wird anhand von Erläuterungen, wissenschaftlichen Abhandlungen und Fachliteratur diskutiert. Besonderes Augenmerk wird darauf gelegt, welchen Zweck die jeweiligen Rechtsakte verfolgen und inwieweit das Konzept der Anonymisierung überholt ist.

To introduce the topic, the definition of anonymization in the Data Protection Directive and the General Data Protection Regulation as well as the theory of the perspective of identifiability will be discussed and the problem of anonymization of genetic data will be outlined. In the following, the definition of anonymization in selected relevant laws in Austria, which are to be applied when processing personal data for scientific research purposes, will be analyzed. Afterwards, other European legal acts that also contain a definition of anonymization and the US law HIPAA (Health Insurance Portability and Accountability Act) are presented. The concept of anonymization is discussed using legislative commentaries, scientific papers, and academic literature. Special attention will be paid to the purpose of the respective laws and to what extent the concept of anonymization is outdated.

14. Literaturverzeichnis

Monographien

El Emam, Guide to the De-Identification of Personal Health Information (Auerbach Publications 2013)

Haase, Datenschutzrechtliche Fragen des Personenbezugs (Mohr Siebeck 2015)

Hornung, Die digitale Identität (Alexander Roßnagel in Zusammenarbeit mit dem TeleTrusT Deutschland e.V 2005)

Pöttgen, Medizinische Forschung und Datenschutz (Peter Lang Internationale Verlag der Wissenschaften 2008)

Vossekuhl, Der Schutz genetischer Daten (Springer 2013)

Kommentare, Handbücher

Dohr/Pollirer/Weiss/Knyrim (Hrsg), DSG Datenschutzrecht[2] (Manz 2017)

Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (C.H.BECK Lexis Nexis 2017)

Feiler/Forgó, EU-DSGVO (Verlag Österreich 2017)

Gola (Hrsg), Datenschutz-Grundverordnung[2] (C.H.BECK 2018)

Heidrich/Forgó/Moos, Datenschutz im Internet, in Forgó/Helfrich/Schneider (Hrsg) (2019)

Jahnel/Pallwein-Prettner/Marzi, Datenschutzrecht[2] (Facultas 2018)

Knyrim (Hrsg), DatKomm (Manz Stand 01.12.2018)

Knyrim (Hrsg), Datenschutz-Grundverordnung DSGVO (Manz 2016)

Paal/Pauly (Hrsg), Datenschutz-Grundverordnung (C.H.BECK 2017)

Simitis (Hrsg), Kommentar zum Bundesdatenschutzgesetz[8] (Nomos 2014)

Sydow (Hrsg), Europäische Datenschutz-Grundverordnung[2] (Nomos 2018)

Sammelwerke

Bergauer, Indirekt personenbezogene Daten - datenschutzrechtliche Kuriosa, in Jahnel (Hrsg), (2011), 55

Conrad/Hausen, § 36 Datenschutz im Internet, in Auer-Reinsdorff/Conrad (Hrsg) (2019), 2079

Custers, Scope and Context, in T.M.C. ASSER PRESS (2019), 1

Fujiwara, Die datenschutzrechtliche Diskussion um autonomes Fahren in Japan, in Roßnagel/Hornung (Hrsg), (2019), 446

Grimm, Biobanken, in Aigner/Kletečka/Kletečka-Pulker/Memmer (Hrsg), Handbuch Medizinrecht (Stand 1.3.2020, rdb.at)

Kollek, Der naturwissenschaftliche Blickwinkel, in Sokol (Hrsg) (2003), 15

Menzel, Die rechtliche Sicht, in Sokol (Hrsg) (2003), 6

Milisits/Pfandlsteiner, Wie funktioniert ELGA für ELGA-GDA?*,* in Aigner/Kletečka/Kletečka-Pulker/Memmer (Hrsg), Handbuch Medizinrecht (Stand 1.3.2020, rdb.at)

Milisits/Pfandlsteiner, Das Protokollierungssystem (§ 22 GTelG 2012), in Aigner/Kletečka/Kletečka-Pulker/Memmer (Hrsg), Handbuch Medizinrecht (Stand 1.3.2020, rdb.at)

Peissl, Datenschutz im medizinischen Bereich, in Stelzer (Hrsg) (2005),11

Roßnagel/Geminn, Stärkung der Datenschutzprinzipien, in Roßnagel/Hornung in Zusammenarbeit mit dem TeleTrusT Deutschland e.V, Datenschutz-Grundverordnung verbessern[1] (2020) 5

Schneider, § 15 Datenschutz in der Informationstechnik, in Specht/Mantz (2019), 1

Souhrada-Kirchmayer, Zur Geschichte des europäischen Datenschutzrechts, in Olechowski/ Neschwara/ Lengauer (Hrsg) (2010), 499

Sorger, Verwendung von Gesundheitsdaten im Lichte der §§ 46, in Jahnel (Hrsg), (2010), 194

Stelzer, Datenschutz im Gentechnikrecht, in Stelzer (Hrsg), (2005), 97

Fachzeitschriften

Aigner, Datenschutz - Patientenschutz aus gesundheitspolitischer Sicht, RdM 2012, 84

Aigner/Leisch, ELGA - Die Elektronische Gesundheitsakte, RdM 2013, 23

Arning/Forgó/Krügel, Datenschutzrechtliche Aspekte der Forschung mit genetischen Daten, DUD (2006) 700

Bergauer/Gosch, Die Pseudonymisierung personenbezogener Daten gemäß der DSGVO - zugleich eine Replik auf Geuer/Wollmann, Verarbeitung von pseudonymen Daten mit besonderem Fokus auf Art 26 und 28 DS-GVO, jusIT 2020, 63

Breyer, Der datenschutzrechtliche Schutz von Körpersubstanzen,
die Patienten zu Analysezwecken entnommen wurden, MedR (2004), 660

Eckhardt, EuGH: Dynamische IP-Adressen und die Grundsatzfrage zum Anwendungsbereich des Datenschutzrechts Der Grundsatz zur Bestimmung des sachlichen Anwendungsbereichs des Datenschutzrechts, ZIR 2017; 6

El Emam, Methods for the de-identification of electronic health records for genomic research, Genome Med (2011), 3

Finck/Pallas, They who must not be identified—distinguishing personal from non-personal data under the GDPR, International Data Privacy Law 2020, 11

Geminn/Laubach/Fujiwara, Schutz anonymisierter Daten im japanischen Datenschutzrecht, ZD (2018), 413

Gerlach, Personenbezug von IP-Adressen, CR 2013, 478

Geuer/Wollmann, Verarbeitung von pseudonymen Daten mit besonderem Fokus auf Art 26 und 28 DS-GVO, jusIT 2020, 18

Gosch, Pseudonymisierung und Verschlüsselung sensibler Daten, jusIT 2019/39, 108

Haidinger, Was sind personenbezogene Daten?, Dako 2014, 17

Haimberger/Geuer, Anonymisierende Wirkung der Pseudonymisierung, Dako 2018, 57

Heidrich/Wegener, Datenschutzrechtliche Aspekte bei der Weitergabe von IP-Adressen, DuD 2010, 172

Herbst, Rechtliche und ethische Probleme des Umgangs mit Proben und Daten bei großen Biobanken, DuD (2016), 371

Hofmann/Hödl, Schwerpunkt: Open Source Biologie und Datenschutz, DuD (2013), 227

Jahnel, EuGH: Dynamische IP-Adressen sind personenbezogene Daten, jusIT 2016; 252

Karg, Anonymität, Pseudonyme und Personenbezug revisited?, DuD 2015, 520

Kirchberg-Lennartz/Weber, Ist die iP-adresse ein personenbezogenes Datum? DuD 2010, 479

Kotschy, Replik zu den Anmerkungen von Dietmar Jahnel zu den Auswirkungen der Vorabentscheidung des EuGH 19. 10. 2016, C-582/14 (Breyer) auf den Begriff der "personenbezogenen Daten" nach § 4 Z 1 DSG 2000, jusIT 2017, 27

Krügel, Das personenbezogene Datum nach der DS-GVO, ZD 2017, 455

Mathieu/Löhnhardt/Grütz/Weil/Drepper/Krawczak, Ethische und rechtliche Implikationen der Speicherung humaner Genomdaten, Medizinische Genetik (2003), 278

McGraw, Building public trust in uses of Health Insurance Portability and Accountability Act de-identified data, Journal of the American Medical Informatics Association (2013) 29

Meyerdierks, Sind IP-Adressen personenbezogene Daten? MMR 2009, 8

Miller, Sharing clinical research data in the United States under the health insurance portability and accountability act and the privacy rule, Trials (2010), 1

Pahlen-Brandt, Datenschutz braucht scharfe Instrumente Beitrag zur Diskussion um „personenbezogene Daten“, DuD (2008), 34

Richter, Big Data, Statistik und die Datenschutz-Grundverordnung, DuD (2016), 581

Roßnagel, Big Data – Small Privacy? - Konzeptionelle Herausforderungen für das Datenschutzrecht, ZD (2013), 562

Stahl, Analyse der Genregulation DNAChiptechnologie, Chem. Unserer Zeit (2005), 188

Thiele, EuGH: Vorratsdatenspeicherung reloaded, jusIT (2020), 224

Voigt, Datenschutz bei Google, MMR 2009, 377

Wegener/Heidrich, Neuer Standard - Neue Herausforderungen: IPv6 und Datenschutz, CR 2011, 479
Weichert, Genetische Genealogie und Datenschutz, DuD (2019) 149

Weichert, Big Data und Datenschutz - Chancen und Risiken einer neuen Form der Datenanalyse, ZD (2013), 251

Weichert, Der Personenbezug von Geodaten, DuD (2007), 17

Wellbrock, Datenschutzrechtliche Aspekte des Aufbaus von Biobanken für Forschungszwecke, MedR 2003, 77

Van Assche/Gutwirth/Sterckx, Protecting Dignitary Interests of Biobank Research Participants: Lessons from Havasupai Tribe v Arizona Board of Regents, Law, Innovation and Technology (2013), 54

Venzke, Die Personenbezogenheit der IP-Adresse Lange diskutiert und immer noch umstritten?, ZD (2011), 114

Von Freier, Getrennte Körperteile in der Forschung zwischen leiblicher Selbstverfügung und Gemeinbesitz, MedR (2005), 321

Andere Quellen

Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research, Council of Europe Treaty Series - No. 195

Arikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff »personenbezogene Daten« WP 136

Artikel-29-Datenschutzgruppe, Stellungnahme 5/2014 zu Anonymisierungstechniken WP 216

Artikel-29-Datenschutzgruppe, Arbeitspapier über genetische Daten WP 91

Artikel-29-Datenschutzgruppe, Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), WP 131

Artikel-29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01

ARTICLE 29 Data Protection Working Party, Working Document on Genetic Data, WP 91

Bendel, Big Data, Gabler Wirtschaftslexikon

BERICHT DER KOMMISSION Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46), KOM (2003) 265 endg.

Bioethikkommission beim Bundeskanzleramt, Beschluss der Bioethikkommission beim Bundeskanzleramt vom 11. Februar 2002 betreffend die Empfehlung für einen Beitritt Österreichs zur Biomedizinkonvention des Europarates

Data Protection Commission, Guidance on Anonymisation and Pseudonymisation

Department of Health and Human Services, Standards for privacy of individually identifiable health information

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche

Der Europäische Datenschutzbeauftragte, Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen — „Gesamtkonzept für den Datenschutz in der Europäischen Union“ (2011/C 181/01)

ENTSCHEIDUNG DER KOMMISSION vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl 2000/215

Europäische Datenschutzausschuss, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten

Europäische Datenschutzausschuss, Stellungnahme 3/2019 zu den Fragen und Antworten zum Zusammenspiel der Verordnung über klinische Prüfungen und der Datenschutz-Grundverordnung (DSGVO)

Europäische Kommission, Pressemitteilung Kommission schlägt Maßnahmen zur Förderung der gemeinsamen Datennutzung und zur Unterstützung europäischer Datenräume vor

Europäische Kommission, Pressemitteilung Kommission schlägt umfassende Reform des Datenschutz-rechts vor, um Nutzern mehr Kontrolle über ihre Daten zu geben und die Kosten für Unternehmen zu verringern

Europäische Kommission, Verordnung über Daten-Governance – Fragen und Antworten

Europäisches Parlament, BERICHT über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) - (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

Forgó, Datenaltruismus – mit Formular und Behörde, Der Standard (2020)

Garfinkel, De-Identification of Personal Information, National Institute of Standards and Technology Internal Report 8053

Haimberger, Aktuelle datenschutzrechtliche Herausforderungen in der medizinischen und pharmazeutischen Forschung (2020)

Harmon, Indian Tribe Wins Fight to Limit Research of Its DNA, The New York Times (2010)

Institut of Medicine of the National Academies, Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research

Medizinische Universität Wien, Stellungnahme 3/SN-322/ME 25. GP 3.

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN Der Schutz der Privatsphäre in einer vernetzten Welt Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM (2012) 9 endg.

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nichtpersonenbezogener Daten in der Europäischen Union, COM (2019) 250 final

Nationaler Ethikrat, Biobanken für die Forschung Stellungnahme

Office of Civil Rights, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule

Privacy Analytics, White Paper Safe Harbor Vs the Statistical Method

Sweeney, Patient Identifiability in Pharmaceutical Marketing Data

Sweeney/Von Loewenfeldt/Perry, Saying it’s Anonymous Doesn't Make It So: Re-identifications of “anonymized” law school data

Übereinkommen zum Schutz der Menschenrechte und der Menschenwürde im Hinblick auf die Anwendung von Biologie und Medizin: Übereinkommen über Menschenrechte und Biomedizin des Europarates, Art 22, SEV Nr. 164.

Internetquellen

<https://de.wikipedia.org/wiki/IP-Adresse>

<https://www.deepl.com/translator#en/de/reasonably%20likely%7Cziemlich%20wahrscheinlich>

<https://www.oesterreich.gv.at/lexicon/S/Seite.990212.html>

<https://www.bmdw.gv.at/Ministerium/DasBMDW/Stammzahlenregisterbehoerde/Bereichsspezifische_Personenkennzeichen/Beschreibung-von-bereichsspezifischen-Personenkennzeichen.html>

<https://www.duden.de/rechtschreibung/Genetik>

<https://biobank.medunigraz.at/spenderinnen/>

<https://directory.bbmri-eric.eu/menu/main/contact>

<https://shop.lykon.de/products/mydna-slim?variant=31460524720185>

<https://www.law.cornell.edu/cfr/text/45/164.514>

<https://de.statista.com/themen/75/weltbevoelkerung/>

<https://www.derstandard.at/story/2000122074854/datenaltruismus-mit-formular-und-behoerde>

15. Judikaturverzeichnis

DSB 14.1. 2019, DSB-D123.224/0004-DSB/2018

DSB 13.9. 2018, DSB-D123.070/0005-DSB/2018

DSB 30.3.2015, DSB-D215.611/0003-DSB/2014

EuGH 06.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net u. a)

EuGH 13.09.2018, C-287/17 (Ceska pojistovna a.s.)

EuGH 19.10.2016, C-582/14 (Breyer)

EuGH 19.06.2014, C‑345/13 (Karen Millen Fashions Ltd.)

EuGH 24.11.2011, C-70/10 (Scarlet Extended)

EuGH 24.11.2005, C-136/04 (Deutsches Milch-Kontor GmbH)