Bundesministerium
Arbeit, Soziales, Gesundheit
und Konsumentenschutz

Schutz sensibler Daten

Position der Gesundheitssektionen VIII und IX des BMASGK

Inhalt

1. Einleitung

Die Verarbeitung von genetischen Daten und Gesundheitsdaten steht im Spannungsverhältnis zwischen Forschung und Wissenschaft, den technischen Möglichkeiten und dem rechtlichen Rahmen. Dieses Positionspapier dient dazu, einen Überblick darüber zu geben, warum die hier angesprochenen Daten in Zusammenhang mit Wissenschaft und Forschung besonders zu erwähnen sind.

Die jüngste Vergangenheit ist geprägt von neuen technischen Errungenschaften und analytischer Methodenentwicklung zur Auswertung immer größerer Datenmengen. „Big Data" ist in aller Munde und hat mit Sicherheit seine Berechtigung zur Gewinnung neuer wissenschaftlicher Erkenntnisse, die dem Gemeinwohl dienen. Andererseits steht diesem Nutzen der Schutz sensibler Daten – wie etwa genetischer Daten und Gesundheitsdaten – entgegen. Ein Rückschluss von gesundheitsbezogenen Daten auf das Individuum muss ausgeschlossen sein.

Nicht nur national, sondern auch international gibt es Bestrebungen zur Verbesserung des Gesundheitssystems durch die Anwendung der Registerforschung, wie auch zur Entwicklung individueller Therapien für Patienten. In diesem Zusammenhang sei beispielhaft die personalisierte Medizin zu nennen.

Gesundheitsdaten weisen grundsätzlich ein hohes Schutzniveau auf. Ziel dieser Position ist es, die notwendigen technischen und rechtlichen Vorgaben der Verarbeitung von mit ELGA verfügbar gemachten ELGA-Gesundheitsdaten und von genetischen Daten, insbesondere im Hinblick auf Wissenschaft und Forschung, darzulegen.

Das vorliegende Positionspapier ist gendersensibel formuliert, allerdings nur so weit, als nicht unionsrechtliche oder nationalrechtliche Bestimmungen zitiert werden, die nicht geschlechtergerecht formuliert sind, um diese nicht willkürlich zu ändern.

2. Datenschutz im Gesundheitswesen

Für die Verarbeitung besonderer Kategorien personenbezogener Daten („sensible Daten") sind die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO) sowie das Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl. I Nr. 165/1999, derzeit geltendes Recht.

Durch die DSGVO sollen insbesondere personenbezogenen Daten – unter personenbezogenen Daten werden gemäß Art. 4 Z 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen verstanden – geschützt werden. Die DSGVO klassifiziert auch pseudonymisierte Daten – nicht jedoch anonymisierte Daten – als personenbezogene Daten (vgl. ErwG 26 der DSGVO). Unter Pseudonymisierung wird gemäß Art. 4 Z 5 DSGVO die Verarbeitung personenbezogener Daten 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 identifizierten oder identifizierbaren natürlichen Person zugewiesen werden, verstanden. Gesundheitsdaten sowie genetische und biometrische[1] Daten stellen aufgrund ihrer „Sensibilität" eine besondere Kategorie personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO dar.

2.1 Gesundheitsdaten

Die DSGVO definiert Gesundheitsdaten als eine besondere Kategorie personenbezogene[r] Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (vgl. Art. 4 Z 15 DSGVO). Dem ErwG 35 der DSGVO folgend sind demnach alle personenbezogenen Daten umfasst, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen

[1] Mangels Relevanz wird auf diese in weiterer Folge nicht mehr eingegangen.

Gesundheitszustand der betroffenen Person hervorgehen. Maßgeblich ist nicht das Vorliegen einer Erkrankung, sondern insbesondere der Gesundheitszustand einer Person im Allgemeinen. Das bedeutet, dass ebenso der Inhalt einer medizinischen Behandlung samt medikamentöser Therapie als auch das Attestieren einer völligen Gesundheit einer Person umfasst sind[2]. Laut ErwG 35 der DSGVO sind darunter auch Informationen über die natürliche Person, die im Zuge der Anmeldung für Gesundheitsdienstleistungen sowie der Erbringung von Gesundheitsdienstleistungen iSd RL 2011/24/EU169 für die natürliche Person erhoben werden zu zählen. Unter Gesundheitsdaten sind darüber hinaus Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren zu verstehen. Ferner werden auch alle Formen der Organisation und Erbringung von Gesundheitsleistungen, unabhängig davon wie diese organisiert, erbracht und finanziert werden, erfasst[3].

Den obigen Ausführungen folgend überrascht es daher nicht, dass auch die Sozialversicherungsnummer als personenbezogenes Datum, welches der Spruchpraxis der Datenschutzbehörde außerhalb des sozialversicherungsrechtlichen Kontexts nicht – sofern keine gesonderte gesetzliche Grundlage dies vorsieht – verwendet werden darf, zu qualifizieren ist[4]. Gemäß Art. 87 DSGVO können Mitgliedstaaten nationale Kennziffern und Kennzeichen von allgemeiner Bedeutung und deren Verarbeitung – worunter auch die Sozialversicherungsnummer zu subsumieren ist – normieren, sofern die Rechte und Freiheiten der betroffenen Person durch geeignete Garantien iSd DSGVO gewahrt werden[5]. Laut *Feiler/Forgo* stellt die Sozialversicherungsnummer ein Gesundheitsdatum iSd DSGVO dar, *„wenn man davon ausgeht, diese diene der eindeutigen Identifizierung der betroffenen Person"*[6]. Hierzu führt *Hödl* zur Klarstellung aus wie folgt: *„Die Sozialversicherungsnummer ist per se noch kein Gesundheitsdatum, denn eine derartige Qualifikation kann sich nur kontextbezogen ergeben, wenn sie tatsächlich iZm einer sich auf den Gesundheitszustand der betroffenen Person beziehenden Verarbeitung verwendet wird (bei der Anmeldung in einem Krankenhaus), also wenn eine Gesundheitsdienstleistung in Anspruch genommen wird, nicht aber für andere Sozialleistungen, wie etwa in Angelegenheiten der Pensions- oder Arbeitslosenversicherung, da in diesem Fall nicht der Gesundheitszustand betroffen ist und die Sozialversicherungsnummer zu einem bloßen Identifikator wird."* [7] Auch die Datenschutzbehörde hat sich mit der Frage, ob die Sozialversicherungsnummer als Gesundheitsdatum iSd DSGVO zu qualifizieren ist, auseinandergesetzt. Im – nicht

[2] Siehe *Weichert* in *Kühling/Buchner* (Hrsg), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO/BDSG[2] (2018) Art. 4 Nr. 15 Rz 1.
[3] Vgl. *Weichert* in *Kühling/Buchner* (Hrsg), DSGVO-Kommentar Art. 4 Nr. 15 Rz 2; siehe auch *Hödl* in *Knyrim* (Hrsg), DatKomm (2018) Art. 4 DSGVO Rz 157.
[4] Siehe DSB 23. 5. 2014, DSB-D213.131/0002-DSB/2014; vgl. auch *Knyrim*, Darf ich die Sozialversicherungsnummer zur Personenidentifizierung verwenden? Dako 2016/46, 71.
[5] *Öhlböck* in *Knyrim* (Hrsg), DatKomm Art. 87 DSGVO Rz 4.
[6] Siehe *Feiler/Forgó,* EU-DSGVO Kurzkommentar (2017) Art. 4 Rz 35.
[7] *Hödl* in *Knyrim* (Hrsg), DatKomm Art. 4 DSGVO Rz 157.

rechtskräftigen – Bescheid vom 9. April 2019 hat sie ausgesprochen, dass die Sozialversicherung nur im Zusammenhang mit der Inanspruchnahme einer Gesundheitsdienstleistung als Gesundheitsdatum zu klassifizieren ist.[8]

Der hM folgend stellt die Information, ob eine Person krankenversichert ist (oder nicht), jedoch noch kein Gesundheitsdatum iSd DSGVO dar[9].

Dem ErwG 35 der DSGVO folgend sind auch Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben, abgeleitet wurden, und Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-Vitro-Diagnostikum stammen von der Definition von Gesundheitsdaten erfasst. Daraus ergibt sich, dass selbst jene Daten, die Rückschlüsse – wenn auch nur mittelbar – auf den Gesundheitszustand zulassen, als Gesundheitsdaten iSd DSGVO zu qualifizieren sind[10].

2.2 Genetische Daten

Die DSGVO enthält darüber hinaus – insbesondere aufgrund deren „besonderen Schutzwürdigkeit" – eine Legaldefinition der genetischen Daten. Gemäß Art. 4 Z 13 DSGVO handelt es sich bei genetischen Daten um personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

ErwG 34 der DSGVO führt in Ergänzung dazu aus wie folgt: *Genetische Daten sollten als personenbezogene Daten über die ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person definiert werden, die aus der Analyse einer biologischen Probe der betreffenden natürlichen Person, insb. durch eine Chromosomen-, Desoxyribonukleinsäure (DNS)- oder Ribonukleinsäure (RNS)-Analyse oder der Analyse eines anderen Elements, durch die gleichwertige Informationen erlangt werden können, gewonnen werden.*

[8] DSB 9.4.2019, DSB-D123.526/0001-DSB/2019.
[9] Vgl. *Weichert* in *Kühling/Buchner* (Hrsg), DSGVO-Kommentar Art. 4 Nr. 15 Rz 2; *Hödl* in *Knyrim* (Hrsg), DatKomm Art. 4 DSGVO Rz 157.
[10] Vgl. *Hödl* in *Knyrim* (Hrsg), DatKomm Art. 4 DSGVO Rz 158.

Anhand von Genanalysen ist, insbesondere aufgrund der Tatsache, dass sich die genetischen Daten eines Menschen im Laufe seines Lebens kaum ändern, eine sichere Identifizierung von Personen möglich. Bei Vorliegen von identifizierten Referenzdaten kann eine Zuordnung zu einer bestimmten Person ohne weiteres erfolgen, daher ist eine Anonymisierung praktisch nicht möglich.[11] Aufgrund der Einzigartigkeit von genetischen Daten können Prognosen über Gesundheit, Krankheit, Heilung, ethnische Herkunft und familiäre Abstammung erstellt werden, wodurch aufgrund der genetischen Merkmale ein hohes Diskriminierungsrisiko inhärent ist.[12] Jede spezielle Ausprägung eines Merkmals lässt Rückschlüsse auf eine Person und sohin deren Identifikation zu. Ebenso der DNS-Code eines Menschen ist als personenbezogenes Datum zu qualifizieren, dessen Rückführbarkeit jedoch aufgrund der gesetzlich festgelegten Rahmenbedingungen für die Durchführung von Genanalysen zumindest mit rechtlich zulässigen Mitteln nicht möglich ist.[13]

Genetische Daten nehmen auch im Bereich der der medizinischen, biotechnischen und historischen Forschung eine zentrale Rolle ein. In diesem Zusammenhang sei aufgrund der zunehmenden Relevanz – unter Berücksichtigung der Einschränkungen des Gentechnikgesetzes (GTG), BGBl. Nr. 510/1994 – auf die biotechnischen und informationstechnischen Anwendungen für alle möglichen Zwecke hingewiesen.[14]

2.3 Rechtsgrundlagen für die Verarbeitung besonderer Kategorien personenbezogener Daten

Grundsätzlich ist die Verarbeitung besonderer Kategorien personenbezogener Daten („sensible Daten"), worunter sowohl Gesundheitsdaten als auch genetische Daten zählen, gemäß Art. 9 Abs. 1 DSGVO verboten. In Art. 9 Abs. 2 DSGVO sind die Ausnahmen vom Verarbeitungsverbot besonderer Kategorien personenbezogener Daten geregelt.

In ErwG 51 S 1 und S 4 DSGVO wird in Ergänzung zu Art. 9 DSGVO ausgeführt wie folgt: *Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können. Derartige personenbezogene Daten sollten nicht verarbeitet werden, es sei denn, die Verarbeitung ist in den in dieser Verordnung dargelegten besonderen Fällen zulässig, wobei zu berücksichtigen ist, dass im Recht der Mitgliedstaaten besondere Datenschutzbestimmungen festgelegt sein können, um die Anwendung der Bestimmungen dieser Verordnung anzupassen, damit die Einhaltung einer rechtlichen Verpflichtung oder die*

[11] *Weichert* in *Kühling/Buchner* (Hrsg), DSGVO-Kommentar Art. 4 Nr. 13 Rz 5.
[12] Vgl. *Hödl* in *Knyrim* (Hrsg), DatKomm Art. 4 DSGVO Rz 144.
[13] Vgl. *Hödl* in *Knyrim* (Hrsg), DatKomm Art. 4 DSGVO Rz 138.
[14] Vgl. *Hödl* in *Knyrim* (Hrsg), DatKomm Art. 4 DSGVO Rz 141.

Wahrnehmung einer Aufgabe im öffentlichen Interesse oder die Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, möglich ist.

Den „sensiblen Daten" soll demnach ein höherer Schutz – der Art der Verarbeitung und der damit verbundenen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person angemessen – zukommen, insbesondere aufgrund des hohen Missbrauchspotentials und – im Falle der missbräuchlichen Verwendung - des hohen Schadenspotentials.[15]

Die Erlaubnistatbestände in Art. 9 Abs. 2 DSGVO enthalten einerseits Zulässigkeitsvoraussetzungen (siehe Art. 9 Abs. 2 lit. a, c, d, e und f) und regeln andererseits Anwendungsfälle (siehe Art. 9 Abs. 2 lit. b, g, h, i und j), die durch den Vorbehalt einer Rechtsgrundlage im Unionsrecht oder im nationalen Recht ergänzt werden.

Bei der Verarbeitung von besonderen Kategorien personenbezogener Daten im Behördenbereich kommt den Bestimmungen in Art. 9 Abs. 2 lit. g-j DSGVO, wodurch die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses erforderlich sein muss (lit. g), für Zwecke der Gesundheitsvorsorge, der Arbeitsmedizin, der Beurteilung der Arbeitsfähigkeit des Beschäftigten, der medizinischen Diagnostik, der Versorgung oder Behandlung im Gesundheits- oder Sozialbereich und der Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich gewährleistet (lit. h), aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit erlaubt (lit. i) oder für im öffentlichen Interesse liegenden Archivzwecke, für wissenschaftliche und historische Forschungszwecke sowie statistische Zwecke ermöglicht (lit. j) besondere Bedeutung zu.[16]

Auch eine ausdrückliche Einwilligung in die Verarbeitung von „sensiblen" personenbezogenen Daten (siehe Art. 9 Abs. 2 lit. a DSGVO) für einen oder mehrere festgelegte Zwecke bildet einen Zulässigkeitstatbestand. Gemäß Art. 9 Abs. 2 lit. a DSGVO besteht die Möglichkeit auf Grundlage des Unionsrechtes oder des nationalen Rechtes für bestimmte Verarbeitungen ein Verarbeitungsverbot zu normieren, wodurch die Einwilligung als Rechtfertigung ausgeschlossen wird. Ein solches Verarbeitungsverbot sieht die Bestimmung des § 67 Abs. 1 GTG vor, wonach es Arbeitgebern und Versicherern verboten ist, Ergebnisse aus genetischen Analysen von Arbeitnehmern, Arbeitsuchenden oder Versicherungsnehmern oder Versicherungswerbern zu erheben, zu verlangen, anzunehmen oder sonst zu verwerten.[17]

Ferner ist die Verarbeitung (insbesondere die Offenlegung im Verfahren) von besonderen Kategorien personenbezogener Daten zulässig, als sie zur Geltendmachung eines

[15] Vgl. *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim* (Hrsg), DatKomm Art. 9 DSGVO Rz 3 f.
[16] Vgl. *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim* (Hrsg), DatKomm Art. 9 DSGVO Rz 30.
[17] Vgl. *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim* (Hrsg), DatKomm Art. 9 DSGVO Rz 31, 33.

Rechtanspruchs vor Gerichten, in einem Verwaltungsverfahren oder außergerichtlich erforderlich ist.[18]

Art. 9 Abs. 4 erlaubt den Mitgliedstaaten zusätzliche Bedingungen, einschließlich Beschränkungen, einzuführen oder aufrechtzuerhalten, soweit die Verarbeitung von Gesundheitsdaten und genetischen Daten betroffen ist.

Eine derartige Beschränkung ist im Zusammenhang mit der Erforschung, Entwicklung und Nutzung der Gentechnik im GTG vorgesehen.

Zu beachten gilt im innerstaatlichen Recht zudem die im Verfassungsrang stehende Bestimmung des § 1 Abs. 2 S 2 DSG, die im Zusammenhang mit dem in § 1 Abs. 1 verbrieften Grundrecht auf Geheimhaltung stehen.

[18] Vgl. *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim* (Hrsg), DatKomm Art. 9 DSGVO Rz 45.

3. Das Forschungsorganisations-gesetz (FOG)

3.1 Wissenschaftliche Forschung und Datenschutz

Der Begriff „wissenschaftliche Forschungszwecke" ist der DSGVO und dem österreichischen Datenschutzrecht grundsätzlich bekannt und auch an verschiedenen Stellen erwähnt; die DSGVO enthält jedoch keine Legaldefinition des Begriffes „Forschung".

Der Begriff der wissenschaftlichen Forschung ist dem ErwG 159 der DSGVO entsprechend weit auszulegen:

Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken gelten. Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken im Sinne dieser Verordnung sollte weit ausgelegt werden und die Verarbeitung für beispielsweise die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen. Darüber hinaus sollte sie dem in Artikel 179 Absatz 1 AEUV festgeschriebenen Ziel, einen europäischen Raum der Forschung zu schaffen, Rechnung tragen. Die wissenschaftlichen Forschungszwecke sollten auch Studien umfassen, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden. Um den Besonderheiten der Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken zu genügen, sollten spezifische Bedingungen insbesondere hinsichtlich der Veröffentlichung oder sonstigen Offenlegung personenbezogener Daten im Kontext wissenschaftlicher Zwecke gelten. Geben die Ergebnisse wissenschaftlicher Forschung insbesondere im Gesundheitsbereich Anlass zu weiteren Maßnahmen im Interesse der betroffenen Person, sollten die allgemeinen Vorschriften dieser Verordnung für diese Maßnahmen gelten.

Den Erläuterungen zum DSG folgend soll „Wissenschaftliche Forschung"– wie auch schon nach den Erläuterungen zu § 46 DSG 2000 – nicht einen inhaltlich abgegrenzten Bereich bezeichnen – etwa in der Richtung, dass nur Grundlagenforschung erfasst und angewandte Forschung ausgeschlossen wäre –, sondern als Bereich verstanden werden, in dem eine bestimmte Methode der Vorgangsweise, nämlich eine „wissenschaftliche", angewendet wird. Wissenschaftliche Forschung im oben genannte Sinn kann durch Verantwortliche des öffentlichen oder des privaten Bereichs vorgenommen werden.[19]

[19] Vgl ErlRV 1664 BlgNR 25. GP 12.

Gemäß der international etablierten Definition im sog *Frascati*-Manual der OECD ist „Forschung und experimentelle Entwicklung" schöpferische und systematische Arbeit zur Erweiterung des Wissensstands – einschließlich des Wissens über die Menschheit, die Kultur und die Gesellschaft – und zur Entwicklung neuer Anwendungen auf Basis des vorhandenen Wissens.[20] Diese Definition wurde in das Forschungsorganisationsgesetz (FOG), BGBl. Nr. 341/1981, übernommen und umfasst die drei Tätigkeitsbereiche Grundlagenforschung, angewandte Forschung und experimentelle Entwicklung und entspricht damit grundsätzlich der weiten Definition von wissenschaftlichen Forschungszwecken der DSGVO.[21]

Art. 89 DSGVO normiert die Datenverarbeitung zu im öffentlichen Interesse liegenden Archiv-, Forschungs- und statistischen Zwecken. Art. 89 Abs. 1 DSGVO verlangt geeignete Garantien für die Rechte und Freiheiten der betroffenen Person, mittels derer sichergestellt werden soll, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere der Grundsatz der Datenminimierung – Ziel ist es demnach nur soviel Daten zu verarbeiten, wie für die Erreichung des jeweiligen wissenschaftlichen Forschungszweck erforderlich ist[22] – gewährleistet wird. Hier führt die Bestimmung in Art. 89 Abs. 1 DSGVO beispielhaft die Pseudonymisierung an. Es gilt jedoch immer zu überprüfen, ob der Zweck nicht auch mit anonymisierten Daten verwirklicht werden kann.[23] Die Verwendung von bPK (vgl. Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen [E-Government-Gesetz – E-GovG], BGBl. I Nr. 10/2004) stellt – nicht nur – im Bereich der wissenschaftlichen Forschung eine angemessene Maßnahme zur Gewährung der genannten geeigneten Garantien zum Schutz der Rechte und Freiheiten betroffener Personen dar. Art. 89 Abs. 2 DSGVO enthält eine Öffnungsklausel, die es den Mitgliedstaaten erlaubt, zugunsten der wissenschaftlichen Forschung Beschränkungen für eine Reihe von Betroffenenrechte vorzusehen, wenn diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.

Jede Verarbeitung von personenbezogenen Daten – so auch zu wissenschaftlichen Forschungszwecken – bedarf einer Rechtmäßigkeitsgrundlage iSd Art. 6 DSGVO. Bei der Verarbeitung besonderer Kategorien von personenbezogenen Daten sind die Rechtsgrundlagen des Art. 9 Abs. 2 DSGVO zu berücksichtigen. So erlaubt Art. 9 Abs. 2 lit j DSGVO die Verarbeitung besonderer Kategorien personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche und historische Forschungszwecke sowie für statistische Zwecke, soweit diese dafür erforderlich ist. Durch die in Art. 9 Abs. 2 lit. j DSGVO enthaltene Öffnungsklausel wird jedem Mitgliedstaat die Möglichkeit zur Erlassung spezifischer Bestimmungen eingeräumt.

[20] Vgl ErlRV 68 BlgNR 26. GP 26.
[21] *Löffler* in *Knyrim* (Hrsg), DatKomm Art 89 DSGVO Rz 24.
[22] *Knotzer*, Wissenschaftliche Forschung und Datenschutz: Eine kritische Analyse ausgewählter Aspekte der österreichischen Rechtslage, ZTR 2018, 213.
[23] Vgl. *Buchner/Tinnefeld* in *Kühling/Buchner* (Hrsg), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO/BDSG² (2018) Art. 89 Rz 16 f.

Auf nationaler Ebene sind in Österreich im Bereich der wissenschaftlichen Forschung insbesondere das DSG und das FOG zu beachten.

§ 7 DSG, in dem geregelt wird, unter welchen Voraussetzungen personenbezogene Daten grundsätzlich für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke verarbeitet werden dürfen, kommt jedoch nicht zur Anwendung, wenn materien-gesetzliche Regelungen die Verarbeitung von Daten zum Zweck der wissenschaftlichen Forschung vorsehen. Diese Regelungen sollen daher lex speciales zu den allgemeinen Regelungen des § 7 DSG darstellen und diesem vorgehen.[24] So gehen die Regelungen des FOG der Bestimmung in § 7 DSG als leges speciales vor[25], jedoch nicht zwangsläufig anderen materien-gesetzlichen Regelungen. Seinem Selbstverständnis nach, dem das BMASGK jedoch nicht folgt[26], handelt es sich beim FOG um ein Rahmengesetz, da einerseits die im 2. Abschnitt normierten Bestimmungen grundsätzlich spezieller als die im Datenschutzgesetz enthaltenen Bestimmungen sind und diesem daher vor gehen, andererseits aber die Bestimmungen der in § 2a FOG aufgezählten Gesetze unberührt bleiben, sofern im FOG nichts anderes geregelt wird.[27]

Das FOG regelt gemäß seinem § 1 Abs. 3 Z 1 insbesondere die Rahmenbedingungen für Verarbeitungen zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken sowie zu statistischen Zwecken im Sinne des Art. 89 Abs. 1 DSGVO.

Im 2. Abschnitt des FOG findet sich die Durchführung der Datenschutz-Grundführung samt ergänzender Regelungen und so regelt § 2d FOG die grundlegenden Bestimmungen zum Schutz personenbezogener Daten. In Übereinstimmung mit den Art. 9 Abs. 2 lit. j und Art. 89 Abs. 1 DSGVO enthält § 2d Abs. 1 FOG einen Katalog angemessener Maßnahmen, die insbesondere einzuhalten sind.

Jedenfalls einzuhalten sind sohin die allgemeinen Datensicherheitsmaßnahmen, nämlich

- die Pflicht zur Protokollierung,
- das Datengeheimnis,
- die Verarbeitung nur für Zwecke des FOG,
- das Benachteiligungsverbot,
- das Verbot der Veröffentlichung von bPK sowie
- die Reduktion des Personenbezugs.

[24] *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, Datenschutzgesetz Kommentar (2018) 104.
[25] *Knotzer*, Wissenschaftliche Forschung und Datenschutz, ZTR 2018, 206.
[26] Siehe etwa die Ausführungen zu § 66 Abs. 3 GTG (siehe Kapitel 4.2.).
[27] Vgl. ErlRV 68 BlgNR 26. GP 17.

Bei der Verarbeitungen gemäß § 2d Abs. 2 FOG, wie etwa der Verwendung von bPK-BF-FO, sind zusätzlich besondere Datensicherheitsmaßnahmen einzuhalten, nämlich jedenfalls

- die Offenlegung der Rechtsgrundlage im Internet,
- das Löschen von Namensangaben bei Ausstattung mit dem bPK,
- die ausdrückliche Aufgabenverteilung zwischen den Organisationseinheiten und zwischen den Mitarbeiter/innen,
- die Bindung der Verarbeitung an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter/innen,
- die Belehrungspflicht der Mitarbeiter/innen über (innerorganisatorische) Datenschutz- und Datensicherheitsvorschriften,
- die Regelung des Zutritts zu Räumlichkeiten, in denen die Datenverarbeitung erfolgt,
- die Regelung des Softwarezugriffs,
- der Schutz vor unbefugter Inbetriebnahme sowie
- die Dokumentationspflicht über bestimmte Maßnahmen.

Wird Registerforschung gemäß § 2d Abs. 2 Z 3 FOG (siehe Punkt 3.1.) in Anspruch genommen, sind neben den oben genannten allgemeinen und besonderen Datensicherheitsmaßnahmen noch weitere Maßnahmen einzuhalten, nämlich

- die Bestellung eines Datenschutzbeauftragten,
- der Nachweis der Verfügungsbefugnis,
- die Verarbeitung nur durch im Antrag genannte Personen sowie
- Löschung von allfälligen Namensangaben nach Erreichung der Zwecke.

Wissenschaftliche Einrichtungen (§ 2b Z 12 FOG), die keine öffentlichen Stellen gemäß § 2b Z 8 FOG sind, können bei Verletzung der Bestimmungen des 2. Abschnitts, die gleichzeitig auch Verstöße gegen die in Art. 83 Abs. 4 und 5 genannten Bestimmungen der DSGVO darstellen, gemäß Art. 83 Abs. 4 und 5 DSGVO bestraft werden.[28] Das heißt, es droht eine Geldbuße von bis zu EUR 20.000.000,--.

3.2 Registerforschung

Mit dem FOG wurde unter anderem die Rechtsgrundlage für Registerforschung geschaffen.[29]

[28] Vgl. ErlRV 68 BlgNR 26. GP 31.
[29] *Liebenwein/Bittermann*, Datenschutz in Wissenschaft und Forschung und seine österreichische Umsetzung, RdM-ÖG 2018/4, 15.

Unter Registern sind laut den Erläuternden Bemerkungen[30] nicht nur öffentlich einsehbare Register im Sinne des § 3 Z 18 des Bundesstatistikgesetzes 2000, sondern sämtliche Verzeichnisse, Datenbanken oder ähnliche Anwendungen oder Verarbeitungsplattformen (ErwG 92 DSGVO) zu verstehen, die bundesgesetzlich vorgesehen sind. Damit ein Register bundesgesetzlich vorgesehen ist, genügt eine bundesgesetzliche Bestimmung, wonach ein solches Register bestehen soll. Register – wie etwa die Implantatregister gemäß § 73a des Medizinproduktegesetzes (MPG), BGBl Nr. 657/1996 – sind auch dann, wenn sie durch Verordnung näher ausgestaltet werden, bundesgesetzlich vorgesehen, weil deren Existenz auf bundesgesetzlicher Ebene – im Falle der Implantatregister wäre dies § 73a MPG – vorgesehen ist.

Gemäß § 2d Abs. 2 Z 3 FOG dürfen wissenschaftliche Einrichtungen (§ 2b Z 12 FOG) von Verantwortlichen, die bundesgesetzlich vorgesehene Register – mit Ausnahme der in den Bereichen der Gerichtsbarkeit sowie der Rechtsanwälte und Notare im Rahmen des jeweiligen gesetzlichen Wirkungsbereichs geführten Register und des Strafregisters – führen, sowie im Falle von ELGA von der ELGA-Ombudsstelle, die Bereitstellung von Daten (§ 2b Z 5) innerhalb der in Art. 12 Abs. 3 DSGVO genannten Frist aus diesen Registern in elektronischer Form verlangen, wobei Namensangaben durch bereichsspezifische Personenkennzeichen „Forschung" (bPK-BF-FO) zu ersetzen sind, es sei denn die Namensangaben sind zur Erreichung von Zwecken gemäß Art. 89 Abs. 1 DSGVO erforderlich, wenn alle der folgenden Voraussetzungen vorliegen:

- die Verarbeitung erfolgt ausschließlich für Zwecke der Lebens- und Sozialwissenschaften;

- das Register ist in einer Verordnung gemäß § 38b FOG angeführt: Diese Verordnung ist im Einvernehmen zwischen dem Bundesminister für Bildung, Wissenschaft und Forschung und dem jeweils für das Register zuständigen Bundesminister zu erlassen und enthält jene Register, aus denen eine Bereitstellung der Daten erfolgt sowie die nähere Regelung der zu ersetzenden Kosten für die Bereitstellung;

- die Antragstellerin oder der Antragsteller ist eine wissenschaftliche Einrichtung gemäß § 2c Abs. 1 oder verfügt über eine gültige Bestätigung gemäß § 2c Abs. 2: Nur jene wissenschaftliche Einrichtungen, die bPKs verwenden dürfen, sind zur Registerforschung berechtigt. § 2c Abs. 1 FOG zählt auf, wer jedenfalls berechtigt ist, bereichsspezifische Personenkennzeichen einzusetzen. Abs. 2 statuiert die Voraussetzungen, nach welchen wissenschaftliche Einrichtungen, die nicht in Abs. 1 genannt sind, einen Antrag (Abs. 3) bei dem/der Bundesminister/in für Verkehr, Innovation und Technologie stellen können. Die Berechtigung wird mittels Bescheid für maximal 5 Jahre zuerkannt. Eine Liste dieser wissenschaftlichen Einrichtungen ist auf der Seite des BMVIT zu veröffentlichen;

[30] Vgl. ErlRV 68 BlgNR 26. GP 34.

- die Kosten für die Bereitstellung der Daten (§ 2b Z 5) ersetzt werden und

- falls ein Abgleich mit vorhandenen Daten beantragt wird, beim Antrag auf Bereitstellung der Daten die entsprechenden bPK gemäß § 13 Abs. 2 E-GovG der betroffenen Personen zur Verfügung gestellt werden.

Das Recht auf Registerforschung besteht unabhängig davon, ob das betreffende Register personenbezogene Daten (Art. 4 Z 1 DSGVO) enthält oder nicht.[31]

Rechtsschutz zur Durchsetzung des Rechts auf Registerforschung bietet § 2k Abs. 5 FOG. Demnach entscheidet das Bundesverwaltungsgericht über Anträge wegen Rechtswidrigkeit des Verhalten von Verantwortlichen, die die Register gemäß § 2d Abs. 2 Z 3 führen, sowie im Falle von ELGA von der ELGA-Ombudsstelle, in Angelegenheiten gemäß § 2d Abs. 2 Z 3.

[31] Vgl. ErlRV 68 BlgNR 26. GP 34.

4. Schützenswerte Daten und deren Rechtsgrundlagen

4.1 ELGA-Gesundheitsdaten

Die Elektronische Gesundheitsakte (ELGA) wird in § 2 Z 6 des Bundesgesetzes betreffend Datensicherheitsmaßnahmen bei der Verarbeitung elektronischer Gesundheitsdaten und genetischer Daten (Gesundheitstelematikgesetz 2012 – GTelG 2012), BGBl. I Nr. 111/2012, definiert als ein Informationssystem, das allen berechtigten ELGA-Gesundheitsdiensteanbietern (ELGA-GDA) und ELGA-Teilnehmer/inne/n ELGA-Gesundheitsdaten in elektronischer Form orts- und zeitunabhängig zur Verfügung stellt. Die gesetzlichen Grundlagen für ihre Verwendung sind das GTelG 2012, insbesondere sein 4. Abschnitt (Elektronische Gesundheitsakte [ELGA]), sowie die Verordnung der Bundesministerin für Gesundheit zur Implementierung und Weiterentwicklung von ELGA (ELGA-Verordnung 2015 – ELGA-VO 2015), BGBl. II Nr. 106/2015, deren Gegenstand gemäß § 1 Abs. 1 ELGA-VO 2015 die Implementierung und Weiterentwicklung von ELGA ist.

Die Verwendung von ELGA erfüllt ein erhebliches öffentliches Interesse gemäß den Art. 9 Abs. 2 lit. g bis j der DSGVO (vgl. § 13 Abs. 1 GTelG 2012) und besteht in den umfangreichen Verbesserungen, die in der öffentlichen Gesundheitsversorgung erzielt werden können (vgl. § 13 Abs. 1 Z 1 bis 6 GTelG 2012).

Zugriff auf ELGA haben nur ELGA-GDA, eine in § 2 Z 10 GTelG 2012 abschließend aufgezählte Teilmenge aller Gesundheitsdiensteanbieter (GDA) iSd § 2 Z 2 GTelG 2012. Durch diese Einschränkung soll sichergestellt werden, dass auf ELGA nur zur Steigerung der Qualität der medizinischen Versorgung und Effizienz in der in der konkreten Behandlungssituation zugegriffen wird.[32] ELGA-GDA sind alle Angehörigen des ärztlichen und zahnärztlichen Berufes, Apotheken, Krankenanstalten sowie Einrichtungen der Pflege, deren Betrieb einer Melde-, Anzeige- oder Bewilligungspflicht nach bundes- oder landesgesetzlichen Vorschriften sowie der behördlichen Aufsicht oder Kontrolle unterliegt. Explizit keine ELGA-GDA sind GDA mit hoheitlichen Befugnissen oder einem Naheverhältnis zu einer Behörde, Arbeitsmediziner/innen sowie für Versicherungsunternehmen, Versicherungsträger und dergleichen arbeitende (Zahn-) Ärzte/Ärztinnen.[33]

[32] Vgl. ErlRV 1936 BlgNR 24. GP 19.
[33] Ausführlich ErlRV 1936 BlgNR 24. GP 19 f.

In ELGA dürfen nur ELGA-Gesundheitsdaten verarbeitet werden (siehe deren Definition in § 2 Z 9 GTelG 2012). Es handelt sich um einen Spezialbegriff für eine Submenge von Gesundheitsdaten und genetischen Daten, nämlich jene personenbezogenen Daten, die zur weiteren Behandlung, Betreuung oder Sicherung der Versorgungskontinuität von ELGA-Teilnehmer/inne/n wesentlich sein könnten, beispielsweise Entlassungsbriefe, Laborbefunde und Medikationsdaten. Ausdrücklich in § 2 Z 9 GTelG 2012 normiert ist, dass es sich bei Geheimnissen aus dem Privatbereich des Patienten/der Patientin sowie Aufzeichnungen über Ergebnisse gemäß § 71a Abs 2 GTG, das sind Analysen zur Feststellung von Prädispositionen für unheilbare Krankheiten (sogenannte Typ-4-Analysen), keinesfalls um ELGA-Gesundheitsdaten handelt.
ELGA-GDA haben die ELGA-Gesundheitsdaten gemäß § 20 Abs. 1 und Abs. 2 GTelG 2012 in geeigneten Datenspeichern und Verweisregistern zu speichern. Mit Ausnahme der Medikationsdaten werden ELGA-Gesundheitsdaten dezentral gespeichert, das heißt, sie verbleiben dort, wo sie erstellt werden, nämlich bei den ELGA-GDA. Damit andere ELGA-GDA die ELGA-Gesundheitsdaten auch finden können, ist ihre Speicherung in Verweisregistern, die sozusagen das Inhaltsverzeichnis von ELGA sind, notwendig.[34]

In § 14 Abs. 2 GTelG 2012 wird abschließend aufgezählt, zu welchen Zwecken die durch ELGA verfügbar gemachten ELGA-Gesundheitsdaten personenbezogen verarbeitet werden dürfen. § 14 Abs. 3 GTelG 2012 normiert ein Verarbeitungsverbot, wonach das Verlangen, der Zugriff auf und die Verarbeitung von durch ELGA verfügbar gemachten ELGA-Gesundheitsdaten für bestimmte natürliche und juristische Personen jedenfalls verboten ist (vgl. Z 1 bis 8 leg cit)[35] und Z 9 leg cit normiert ausdrücklich, dass von diesem Verarbeitungsverbot auch alle sonstigen natürlichen und juristischen Personen, die nach dem GTelG 2012 nicht ausdrücklich dazu berechtigt sind, sowie für alle Zwecke, die im GTelG 2012 nicht ausdrücklich als zulässig bestimmt sind, umfasst sind (zur Registerforschung iSd FOG siehe Punkt 3.1.). Bei diesem Verarbeitungsverbot iSd § 14 Abs. 3 GTelG 2012 handelt es sich um eine sogenannte angemessene und spezifische Maßnahme zur Wahrung der Grundrechte und Interessen der betroffenen Person. Zusätzlich sehen das GTelG 2012 und die ELGA-VO 2015 noch eine Reihe weiterer solcher Maßnahmen vor, etwa die Pflicht zur technischen Sicherstellung des rollenbasieren Zugriffs gemäß § 3 Abs. 3 GTelG 2012 iVm Anlage 1 der Verordnung des Bundesministers für Gesundheit, mit der nähere Regelungen für die Gesundheitstelematik getroffen werden – Gesundheitstelematikverordnung 2013 (GTelV 2013), BGBl. II Nr. 506/2013, und die Pflicht zur eindeutigen Identifikation gemäß den §§ 18 f GTelG 2012, ebenso wie die in den §§ 17b bis 17j ELGA-VO 2015 verankerten Sicherheitsanforderungen am dem erforderlichen Zugriffsschutz.[36] Ebenso wie diese Datensicherheitsmaßnahmen stellt das Protokollierungssystem (§ 22 GTelG 2012) eine angemessene und spezifische Maßnahme zur Wahrung der Grundrechte und Interessen der betroffenen Person dar, da die Verarbeitung der ELGA-Gesundheitsdaten darüber nachvollzogen werden kann. Protokolliert

[34] Vgl. ErlRV 1936 BlgNR 24. GP 32.
[35] ErlRV 1457 BlgNR 25. GP 22.
[36] Vgl. ErlRV 1457 BlgNR 25. GP 23 f.

werden unter anderem die Zugriffe des ELGA-Gesundheitsdiensteanbieters oder der ELGA-Ombudsstelle sowie die Abfragekriterien.
Neben den technischen und organisatorischen Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person stehen den ELGA-Teilnehmer/inne/n eigene Teilnehmer/innen/rechte zu.[37] Sie garantieren den ELGA-Teilnehmer/inne/n Transparenz in Bezug auf die Verarbeitung ihrer personenbezogenen Daten und bieten ihnen gleichzeitig die Möglichkeit, die Verarbeitung der ELGA-Gesundheitsdaten einfach und effektiv zu kontrollieren.[38]

4.2 Genetische Daten

Der Schutz genetischer Daten hat in der österreichischen Rechtsordnung einen sehr hohen Stellenwert. So verbietet es das österreichische Gentechnikgesetz, genetische Daten Arbeitgebern und Versicherungen zur Verfügung zu stellen, außerdem enthält es spezifische Regelungen über die Handhabung dieser Daten in Krankenanstalten und im niedergelassenen Bereich, über ihre Offenlegung zwischen Verwandten sowie eben auch für ihre Verwendung für Forschungszwecke.

Der Umgang mit menschlichen genetischen Daten für Zwecke der Forschung ist in § 66 GTG geregelt und lautet:

Genetische Analysen am Menschen für wissenschaftliche Zwecke und zur Ausbildung

§ 66. (1) Genetische Analysen am Menschen für wissenschaftliche Zwecke und zur Ausbildung dürfen nur an de-identifizierten Proben durchgeführt werden. 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 genetischen 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.

(3) Die Bestimmungen der §§ 2d Abs. 1 und 3 bis 8, 2f Abs. 1 Z 6 und Abs. 3, 4, 6 und 7 sowie 2i Abs. 1, 2, 2j und 2k des Forschungsorganisationsgesetzes, BGBl. Nr. 341/1981, in der Fassung des Bundesgesetzes BGBl. I Nr. 31/2018, finden Anwendung.

[37] Vgl. ErlRV 1936 BlgNR 24. GP 5.
[38] Vgl. ErlRV 1457 BlgNR 25V. GP 23.

Diese Bestimmung ist gegenüber dem FOG als lex specialis zu sehen und geht ihm, welches ganz allgemein Forschungsdaten nach Verschlüsselung mit bereichsspezifischen Personenkennzeichen weitgehend zur Verarbeitung freigibt, vor. Die Verpflichtung im GTG zur De-Identifikation der Proben (und allfälliger nicht-medizinischer genetischer Daten), welche nur in den Einrichtungen erfolgen darf, die über eine gültige Einwilligung (Art. 4 Nr. 11 DSGVO) der betroffenen Person für diese Zuordnung verfügen, soll weitgehend verhindern, dass die genetischen Daten dieser Person und ihrer Verwandten/Nachkommen im Lauf der Zeit mit Fortschreiten der technischen Möglichkeiten auf diese rückführbar werden.

Die Regelungen des § 66 GTG stehen dabei einem internationalen Austausch von Forschungsdaten grundsätzlich nicht entgegen, sondern ermöglichen sie bei gleichzeitiger Sicherstellung der Nichtrückführbarkeit der genetischen Daten auf die Patienten/Probanden und ihre Verwandten/Nachkommen auch für die kommenden Generationen.

5. Technische Aspekte

Die Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten (Art. 4 Z 15 und Z 13 DSGVO) ist im 2. Abschnitt des Gesundheitstelematikgesetzes (GTelG 2012) StF: BGBl. I Nr. 111/2012) geregelt.

5.1 Identifier im Gesundheitswesen

Die eindeutige elektronische Identität im Gesundheitswesen ist das bereichsspezifische Personenkennzeichen (bPK) GH (§ 2 Z 2 des E-Government-Gesetzes – E-GovG, BGBl. I Nr. 10/2004). Dieses wird errechnet über die aus dem Stammzahlenregister SZR, dem konstitutiven Register aller Personen, ermittelte Stammzahl (§ 6 E-GovG). Das SZR ist ein virtuelles Register, das die Übermenge zum Zentralen Melderegister (ZMR) sowie dem Ergänzungsregister natürliche Personen (ErnP) darstellt.

Diese Form der Identifikation via bPK GH findet sich in allen zeitgemäßen eHealth-Lösungen, wie z.B. ELGA, wieder. Dadurch erst wird ein Zugriff durch Patienten via Bürgerkarte bzw Handysignatur ermöglicht. Um eine Verbindung zur Sozialversicherungsnummer, die laut Vorgaben des DSB nur für Zwecke der Sozialversicherung verwendet werden darf, herzustellen, wurde der Zentrale Patientenindex (ZPI, § 18 GTelG 2012) errichtet und mit bPK GH ausgestattet.

Somit ergeben sich in der Praxis folgende Identifikatoren für Personen im Gesundheitswesen:

- bPK GH /Funktion eID via Bürgerkarte bzw Handysignatur: deckt alle Personen ab
- Sozialversicherungsnummer/eCard: sozialversicherte Personen, Verbindung bPK GH via ZPI

Die Ermittlung der bPK GH von Patienten durch Gesundheitsdiensteanbieter (GDA) erfolgt entweder durch Stecken der eCard oder durch Abfrage des Stammzahlregisters im Wege der jeweiligen Applikation.

Die Zuordnung von Rollen im Gesundheitswesen (§ 5 GTelG 2012) erfolgt rechtsverbindlich über den eHealth Verzeichnisdienst eHVD (§ 9 GTelG 2012). Hier erfolgt eine Zuordnung der persönlichen Identität, also der bPK GH, von GDAs zu deren Rolle(n), wie bspw. Hebamme

oder Arzt/Ärztin, aber auch der Rolle von juristischen Personen wie z.B. Krankenanstalt oder Pflegeheim.

Die elektronische Zuweisung der Rolle bspw einer Hebamme erfolgt somit via Bürgerkarten-Login samt nachfolgender automatischer eHVD-Prüfung. Im Falle am eCard-Netz teilnehmender Ordinationen erfolgt die Rollenzuweisung via oCard. Diese Rollen sind ebenfalls im eHVD abgebildet. Die Abbildung der Rollen von Gesundheitsbehörden erfolgt via Rollenzuordnungen entsprechend der Behördenportalverbund-Vereinbarung.

Somit ergeben sich drei Varianten zur Rollenzuweisung im Gesundheitswesen:

1. durch Abfrage des eHVD nach Bürgerkarten/Handysignatur-Login des jeweiligen GDA

2. durch Rollenübermittlung auf Basis des Behördenportalverbundes für Gesundheitsbehörden

3. durch eCard-/oCard-Infrastrukur von Vertragspartnern der Sozialversicherung

Zum Zwecke von Statistiken und Auswertungen erfolgen weitere, irreversible „Hash"-Bildungen der bPK GH, ein höchstmögliches Datenschutzniveau zu erreichen.

5.2 Notwendige Verschlüsselungstechnik

Hinsichtlich Vertraulichkeit (§ 6 GTelG 2012) und Integrität (§ 7 GTelG 2012) ist festgelegt, dass die elektronische Übermittlung von Gesundheitsdaten und genetischen Daten über Netzwerke durchgeführt wird, die entsprechend dem Stand der Technik in der Netzwerksicherheit gegenüber unbefugten Zugriffen abgesichert sind, indem sie zumindest die Absicherung der Übermittlung von Daten durch kryptographische oder bauliche Maßnahmen, den Netzzugang ausschließlich für eine geschlossene oder abgrenzbare Benutzer/innen/gruppe sowie die Authentifizierung der Benutzer/innen vorsehen. Alternativ sind Protokolle und Verfahren zu verwenden, die die vollständige Verschlüsselung der Gesundheitsdaten und genetischen Daten bewirken und deren kryptographische Algorithmen in der Verordnung gemäß GTelG § 28 Abs. 1 Z 2 angeführt sind.

Ferner ist festgelegt, dass die allfällige Speicherung von Gesundheitsdaten und genetischen Daten in Datenspeichern, die einem Verantwortlichen (Art. 4 Z 7 DSGVO) bedarfsorientiert von einem Auftragsverarbeiter (Art. 4 Z 8 DSGVO) bereitgestellt werden („Cloud Computing"), nur dann erfolgt, wenn die Gesundheitsdaten und genetischen Daten mit

einem dem aktuellen Stand der Technik entsprechenden Verfahren verschlüsselt worden sind.

Ebenso haben Nachweis und Prüfung der Integrität elektronischer Gesundheitsdaten und genetischer Daten durch die Verwendung fortgeschrittener oder qualifzierter elektronischer Signaturen oder fortgeschrittener oder qualifzierter elektronischer Siegel gemäß der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. Nr. L 257 vom 28.08.2014 S. 73, in der Fassung der Berichtigung ABl. Nr. L 257 vom 29.01.2015 S. 19, zu erfolgen. Sollte ein entsprechend dem Stand der Technik abgesichertes Netzwerk gemäß § 6 Abs. 1 Z 1 GTelG 2012 verwendet werden, darf der Zugang zu diesem Netzwerk ausschließlich für im Vorhinein bekannte Gesundheitsdiensteanbieter möglich sein.

Diese Vorgaben befinden sich im Einklang mit Projektinitiativen der Europäischen Union im Sektor Gesundheit. Weiters unterstreichen diese Mindestvorgaben die ethische Verantwortung des Staates gegenüber Gesundheitsdaten und genetischen Daten der Bürger/innen.

6. Internationale Initiativen

6.1 ICPerMed

Bei dem Internationalen Konsortium für Personalisierte Medizin (ICPerMed)[39] handelt es sich um den Zusammenschluss von mehr als 30 europäischen und internationalen Partnern, vornehmlich aus den zuständigen Ministerien, Forschungsagenturen und der Europäischen Kommission mit dem Ziel, gemeinsame Anstrengungen zur Unterstützung der Forschung und Implementierung der personalisierten Medizin in den Mitgliedsstaaten zu erreichen. Österreich ist durch das BMASGK und das BMBWF in dieser Plattform vertreten. Um das Ziel zu erreichen, wurde ein entsprechender „Action Plan"[40] erarbeitet, der in Arbeitsgruppen und Konferenzen mit Leben erfüllt werden soll. Personalisierte Medizin bietet eine speziell auf den Patienten zugeschnittene Therapie, meist basierend auf der Auswertung genetischer Daten des Patienten. Dies impliziert in der Folge auch die Notwendigkeit des adäquaten Schutzes dieser besonders sensiblen Daten. Eine eigene Action mit dem Titel „Research projects to optimise data security, privacy and ownership within personalised medicine approaches" wurde dazu ins Leben gerufen. Es wird dazu von ICPerMed festgehalten, dass der Schutz aller Patientendaten von fundamentaler Wichtigkeit ist hinsichtlich zukünftiger Anwendungsgebiete der personalisierten Medizin und auch in Bezug auf den Ausschluss des Nutzens der erhobenen genetischen Daten durch Versicherungen und Arbeitgeber. Im Lichte neuer technischer Möglichkeiten zur Nutzung individueller Daten wie auch von „Big Data" muss ein verantwortungsbewusster Umgang mit diesen sensiblen Informationen gewährleistet sein. Entsprechende wissenschaftliche Ansätze sollen dazu erarbeitet werden.

6.2 1Mio Genomes Initiative

Die Deklaration „Towards access of at least 1 million sequenced Genomes in the EU by 2022" wurde am 10. April 2018 von 13 Mitgliedstaaten unterfertigt.[41] Bis Dezember 2018 traten dann weitere fünf Staaten – darunter Österreich – der Deklaration bei. Somit haben bis dahin folgende Mitgliedstaaten der EU die Deklaration unterschrieben: Österreich, Bulgarien, Kroatien, Tschechien, Zypern, Estland, Finnland, Griechenland, Italien, Litauen, Lettland, Luxemburg, Malta, Niederlande, Portugal, Slowenien, Spanien, Schweden,

[39] <icpermed.eu> (06.05.2019).
[40] <icpermed.eu/media/content/ICPerMed_Actionplan_2017_web.pdf> (06.05.2019).
[41] <ec.europa.eu/newsroom/dae/document.cfm?doc_id=50964> (06.05.2019).

Großbritannien. Als Beobachter sind Deutschland, Dänemark, Ungarn, Norwegen, Belgien, Irland, Polen und die Schweiz dabei.

Ziel dieser Initiative ist, dass bis 2022 mehr als eine Million menschliche Genome mit phänotypischen und klinischen Daten in der EU (wie auch EWR und EFTA) als Datensätze zur Verfügung stehen, um die klinische Forschung wie auch die therapeutische und präventive Nutzung im Gesundheitssystem zu verbessern. Weiters soll ein technischer wie auch rechtlicher Rahmen erstellt werden, innerhalb dessen die Nutzung erfolgen darf. In diversen Arbeitsgruppen soll die Thematik behandelt werden, insbesondere natürlich auch zur Datennutzung und zum Datenschutz.

Seltene Erkrankungen, Krebs und personalisierte Prävention sollen als Anwendungsbereiche fokussiert werden, um den Nutzen für die Bürger, Gesundheitsdienstleister, Forscher und Industrie aufzuzeigen.Die Initiative legt dar, dass diese Aktivitäten notwendig sind, um – unter Berücksichtigung der DSGVO – Fortschritte im Bereich des Verstehens genetisch assoziierter Erkrankungen und genetischer Prädispositionen zu machen. Derartige Entwicklungen sollen die Diagnose, Prävention und Behandlung – wie etwa die Anwendung personalisierter Medizin – genetisch bedingter Erkrankungen erleichtern. Zusätzlich soll durch eine verbesserte Kooperation der EU-Mitgliedstaaten die Wirtschaft gestärkt werden. Es wird betont, dass durch den sicheren, grenzüberschreitenden Zugang zu genetischen und Gesundheitsdaten zielgerichtete Forschung und Innovation sowie deren Translation zur klinischen Anwendung und Prävention ermöglicht werden soll[42].

Verwandte Themenbereiche:

- Halbzeitüberprüfung der Strategie für einen digitalen Binnenmarkt[43],
- Schlussfolgerungen des Rates vom 8 Dezember 2017 zum Gesundheitswesen in der digitalen Gesellschaft[44],
- Schlussfolgerungen des Rates vom 16. Juni 2017 zur Förderung einer von den Mitgliedstaaten ausgehenden freiwilligen Zusammenarbeit zwischen den Gesundheitssystemen[45],
- Schlussfolgerungen des Rates vom 07. Dezember 2015 zu personalisierter Medizin für Patienten[46]

[42] https://www.euapm.eu/pdf/EAPM_Declaration_Genome.pdf
[43] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über die Halbezeitüberprüfung der Strategie für einen digitalen Binnenmarkt. Ein vernetzter Binnenmarkt für alle, KOM (2017) 228 endg. vom 10.05.2017.
[44] Schlussfolgerungen des Rates vom 8 Dezember 2017 zum Gesundheitswesen in der digitalen Gesellschaft — Fortschritte bei der datengesteuerten Innovation im Gesundheitswesen, ABl 2017 C 440.
[45] Schlussfolgerungen des Rates vom 16. Juni 2017 zur Förderung einer von den Mitgliedstaaten ausgehenden freiwilligen Zusammenarbeit zwischen den Gesundheitssystemen, ABl 2017 C 206.
[46] Schlussfolgerungen des Rates vom 07. Dezember 2015 zu personalisierter Medizin für Patienten, ABl 2015 C 421.

7. Spezifische Schutzwürdigkeit von ELGA-Gesundheitsdaten und genetischen Daten

7.1 Technische Grenzen

7.1.1 Technische Unmöglichkeit der Registerforschung mit durch ELGA verfügbar gemachten ELGA-Gesundheitsdaten

Obwohl § 14 Abs. 3 Z 9 GTelG 2012 ausdrücklich ein Verarbeitungsverbot normiert, wonach das Verlangen, der Zugriff auf und die Verarbeitung von durch ELGA verfügbar gemachten ELGA-Gesundheitsdaten natürlichen und juristischen Personen, die nach dem GTelG 2012 nicht ausdrücklich dazu berechtigt sind, und für Zwecke, die im GTelG 2012 nicht ausdrücklich als zulässig bestimmt sind, jedenfalls verboten ist, ist die Registerforschung mit durch ELGA verfügbar gemachten ELGA-Gesundheitsdaten an sich zulässig. Bei § 2d Abs. 2 Z 3 FOG handelt es sich um eine lex posterior zu § 14 Abs. 3 GTelG 2012 und stellt der Grundsatz *„lex posterior derogat legi priori"* bei einer Normenkollision ein allgemeiner Grundsatz der Rechtswissenschaften dar.[47]

Obwohl die Registerforschung mit durch ELGA verfügbar gemachten ELGA-Gesundheitsdaten rechtlich zwar zulässig ist, ist sie aber technisch nicht möglich:

Gemäß § 2d Abs. 2 Z 3 FOG sind wissenschaftliche Einrichtungen berechtigt, von der ELGA-Ombudsstelle die Bereitstellung von Daten innerhalb der in Art. 12 Abs. 3 DSGVO genannten Frist aus ELGA in elektronischer Form zu verlangen. Zugriff auf ELGA haben in erster Linie aber nur die ELGA-GDA und die ELGA-Teilnehmer/innen. Die ELGA-Ombudsstelle ist kein ELGA-GDA und hat rechtlich nur im Anlassfall Zugriff auf die ELGA-Gesundheitsdaten der betroffenen Person und kann auch technisch nur auf die ELGA-Gesundheitsdaten einzelner betroffener Personen zugreifen; die Herausgabe aller in ELGA gespeicherten Daten sämtlicher ELGA-Teilnehmer/innen in pseudonymisierter Form („Big Data") ist der ELGA-Ombudsstelle technisch nicht möglich. Um die Anfrage einer wissenschaftlichen Einrichtung beantworten zu können, muss sich die ELGA-Ombudsstelle also den Betreibern von

[47] Vgl. *Kehrer*, Gesetzeskonforme Methodik. Die Auslegung von Rechtsvorschriften anhand der §§ 6 und 7 ABGB (2013) 47.

Datenspeichern und Verweisregistern bedienen: Medikationsdaten werden zentral gespeichert, Daten aus e-Befunden dezentral. Je nach Anfrage muss sich die ELGA-Ombudsstelle an einen (Medikationsdaten) oder an alle (Daten aus e-Befunden) Betreiber(n) von Datenspeichern und Verweisregistern mit dem Ersuchen wenden, ihr die bei ihnen jeweils gespeicherten Daten im Klartext herauszugeben. Nach Erhalt hat sie sie mit dem bPK BF-FO ausstatten zu lassen und an die anfragende wissenschaftliche Einrichtung zu übermitteln (wofür wegen der Komplexität der Vorgehensweise die Frist des Art. 12 Abs. 3 DSGVO als viel zu kurz angesehen wird). Die Herstellung eines kompletten Datenauszugs einer Daten- oder Patientenkategorie ist den Betreibern von Datenspeichern und Verweisregistern aber ebenso wenig technisch möglich wie der ELGA-Ombudsstelle, weswegen Registerforschung iSd FOG aktuell mit dem gesamten ELGA-System technisch nicht möglich ist.

7.2 Datenschutzrechtliche Grenzen

7.2.1 Datenschutzrechtliche Probleme im Hinblick auf die Registerforschung mit durch ELGA verfügbar gemachten ELGA-Gesundheitsdaten

Ein offensichtliches datenschutzrechtliches Problem stellt die fehlende gesetzliche Grundlage iSd Art. 28 Abs. 3 DSGVO für die Übermittlung der ELGA-Gesundheitsdaten durch die Betreiber von Datenspeichern und Verweisregistern dar. Es müssen also entsprechende Auftragsverarbeitungsverträge abgeschlossen werden, wobei ein Vertragsabschluss naturgemäß aber nicht erzwungen werden kann. Wird kein Auftragsverarbeitungsvertrag abgeschlossen und werden die ELGA-Gesundheitsdaten trotzdem der ELGA-Ombudsstelle übermittelt, handelt der jeweilige Betreiber von Datenspeichern und Verweisregistern nicht als ihr Auftragsverarbeiter, sprich, er übermittelt die ELGA-Gesundheitsdaten unrechtmäßig.

Gemäß § 15 Abs. 2 GTelG 2012 kann der Teilnahme an ELGA jederzeit generell oder partiell widersprochen werden, das heißt bezüglich allen ELGA-Gesundheitsdaten oder nur bestimmten. Der Widerspruch kann zu einem Zeitpunkt erfolgen, zu dem noch keine ELGA-Gesundheitsdaten gespeichert wurden, er kann aber auch erst zu einem Zeitpunkt erfolgen, zu dem diese schon vorhanden sind. In diesem Fall sind alle bis zum Zeitpunkt des Widerspruchs in den ELGA-Verweisregistern vorhandenen und vom Widerspruch erfassten Verweise und ELGA-Gesundheitsdaten einschließlich Medikationsdaten zu löschen; falls das Löschen aufgrund anderer gesetzlicher Dokumentationsverpflichtungen oder zur gerichtlichen oder außergerichtlichen Durchsetzung sowie Abwehr geltend gemachter rechtlicher Ansprüche ausgeschlossen ist, sind die Verweise für ELGA unzugänglich zu machen (vgl. § 15 Abs. 3 GTelG 2012). In diesem Fall ist also das ELGA-Gesundheitsdatum

noch vorhanden, nur nicht mehr mit dem entsprechenden elektronischen Verweis verknüpft. Die Verweise dienen zwar der Lokalisierung, haben aber keinen medizinischen Inhalt und sind nur beschlagwortet. Je nachdem, wie die Anfrage der wissenschaftlichen Einrichtung ausgestaltet ist, ergibt sich, inwieweit die elektronischen Verweise zur Beantwortung der Anfrage geeignet sind. Wenn der Verweis zur Eruierung der benötigten ELGA-Gesundheitsdaten kein passender Indikator ist, besteht die Gefahr, dass gespeicherte ELGA-Gesundheitsdaten, deren Verarbeitung widersprochen wurde, herausgegeben werden. Da die Mitarbeiter der ELGA-Ombudsstelle nicht berechtigt sind, ohne Auftrag des ELGA-Teilnehmers/der ELGA-Teilnehmerin auf deren ELGA-Gesundheitsdaten zuzugreifen, sind es auch die Betreiber von Datenspeichern und Verweisregistern als Auftragsverarbeiter der ELGA-Ombudsstelle nicht. Sollte sich also die Anfrage über die Beschlagwortung der elektronischen Verweise nicht beantworten lassen, würden die Betreiber von Datenspeichern und Verweisregistern bei der Suche nach den angefragten Daten ELGA-Gesundheitsdaten, deren Verarbeitung widersprochen wurde, jedenfalls unrechtmäßig verarbeiten, auch wenn sie nicht an die ELGA-Ombudsstelle übermittelt würden.

Ein größeres datenschutzrechtliches Problem ergibt sich aus § 16 Abs. 1 Z 2 lit. a GTelG 2012, wonach ELGA-Teilnehmer/innen das Recht haben, elektronische Verweise und ELGA-Gesundheitsdaten einschließlich Medikationsdaten für ELGA-Gesundheitsdiensteanbieter ein- oder ausblenden. In diesem Fall wird der Verweis nicht unzugänglich gemacht, sondern lediglich seine Sichtbarkeit eingeschränkt. Die Betreiber von Datenspeichern und Verweisregistern würden in diesem Fall die betroffenen ELGA-Gesundheitsdaten (aufgrund des vorhanden Verweises) jedenfalls der ELGA-Ombudsstelle übermitteln, obwohl man davon ausgehen darf, dass durch die Ausblendung die Verarbeitung dieser Daten gerade vermieden werden soll. Die Gründe, die zum Ausblenden und nicht zur Löschung des Verweises führten, liegen in der Sphäre der ELGA-Teilnehmer/innen und sind datenschutzrechtlich unbeachtlich, weil in beiden Fällen der Wille zum Ausdruck gelangt, dass die entsprechenden Daten nicht verarbeitet werden.

Werden ELGA-Gesundheitsdaten verarbeitet, weil sie den wissenschaftlichen Einrichtungen herausgegeben werden, obwohl der Teilnahme an ELGA widersprochen wurde oder die Sichtbarkeit eingeschränkt wurde, so werden dadurch die ELGA-Teilnehmer/innen/rechte unterlaufen. Die ELGA-Teilnehmer/innen/rechte sind aber eine angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person (vgl. Art. 9 Abs. 2 lit. g DSGVO, der eine Rechtsgrundlage für die Verwendung von ELGA ist).

Ein offensichtliches datenschutzrechtliches Problem ist die Übermittlung des Namens als Klartext an die ELGA-Ombudsstelle. Die ELGA-Ombudsstelle ist berechtigt, auf die ELGA-Gesundheitsdaten einzelner Personen im Bedarfsfall zuzugreifen, nämlich dann, wenn sie von

einem ELGA-Teilnehmer/einer ELGA-Teilnehmerin zu Rate gezogen wurde bzw sie mit einem Sachverhalt betraut wurde. Zwar sind die Mitarbeiter/innen der ELGA-Ombudsstelle zur Verschwiegenheit über alle ihnen in Ausübung ihres Berufes anvertrauten oder bekannt gewordenen Tatsachen verpflichtet, allerdings sind sie nicht berechtigt, ohne entsprechenden Auftrag des ELGA-Teilnehmer/der ELGA-Teilnehmerin, Kenntnis über deren ELGA-Gesundheitsdaten zu haben, was sich aber nicht vermeiden lässt, wenn der Name im Klartext übermittelt wird.

Neben den Teilnehmer/innen/rechten stellt das Protokollierungssystem (§ 22 GTelG 2012) eine angemessene und spezifische Maßnahme zur Wahrung der Grundrechte und Interessen der betroffenen Person dar, da die Verarbeitung der ELGA-Gesundheitsdaten darüber nachvollzogen werden kann. Protokolliert wird gemäß § 22 Abs. 2 GTelG 2012 jede Verarbeitung von ELGA-Gesundheitsdaten im Rahmen von ELGA, unter anderem die Zugriffe des ELGA-Gesundheitsdiensteanbieters oder der ELGA-Ombudsstelle sowie die Abfragekriterien. Zwar normiert auch § 2d Abs. 1 Z 1 FOG eine Verpflichtung, Zugriffe auf personenbezogene Daten, die auf Grundlage des 2. Abschnitts des FOG automationsunterstützt verarbeitet werden, lückenlos zu protokollieren, allerdings ist im Zusammenhang mit ELGA nicht geklärt, ob und wessen Zugriff im Fall einer Anfrage einer wissenschaftlichen Einrichtung protokolliert wird und in welchem Umfang: Im Falle der Registerforschung handelt es sich nicht um eine Verarbeitung von ELGA-Gesundheitsdaten im Rahmen von ELGA (vgl. § 14 Abs. 2 GTelG 2012), weswegen § 22 Abs. 2 GTelG 2012 nicht zur Anwendung kommt; § 2d Abs. 1 Z 1 FOG spricht nur von einer Pflicht zur lückenlosen Protokollierung der Zugriffe, gibt aber ebenso wenig wie die dazugehörigen Erläuterungen[48] den Umfang dieser Verpflichtung preis. Ein Spannungsverhältnis besteht in diesem Zusammenhang auch zwischen dem Recht der ELGA-Teilnehmer/innen gemäß § 16 Abs. 1 Z 1 iVm § 22 Abs. 4 GTelG 2012, Auskunft über die sie betreffenden Protokolldaten zu erhalten (was vom Auskunftsrecht iSd Art. 15 DSGVO umfasst ist) und § 2d Abs. 6 Z 1 FOG, wonach das Auskunftsrecht iSd Art. 15 DSGVO insoweit keine Anwendung findet, als dadurch die Erreichung von Zwecken gemäß Art. 89 Abs. 1 DSGVO voraussichtlich unmöglich gemacht oder ernsthaft beeinträchtigt wird. Die Nicht-Klärung dieser Punkte birgt die Gefahr der fehlenden Transparenz der Verarbeitung von ELGA-Gesundheitsdaten. Damit wäre diese Datensicherheitsmaßnahme unterlaufen.

Abschließend ist zu sagen, dass die organisatorischen und technischen Datensicherheitsmaßnahmen in Hinblick auf ELGA durch allfällige sekundäre Verwendungsmöglichkeiten von ELGA nicht unterlaufen werden dürfen, wobei gegebenenfalls zumindest ein gleichwertiger Ersatz dieser organisatorischen und technischen Datensicherheitsmaßnahmen vorzusehen ist.

[48] Vgl. ErlRV 68 BlgNR 26I. GP 31.

7.2.2 Nicht-Anonymisierbarkeit genetischer Daten

Anhand von Genanalysen ist, insbesondere aufgrund der Tatsache, dass sich die genetischen Daten eines Menschen im Laufe seines Lebens normalerweise nicht ändern, eine sichere Identifizierung von Personen möglich. Bei Vorliegen von identifizierten Referenzdaten kann eine Zuordnung zu einer bestimmten Person ohne weiteres erfolgen, daher ist eine Anonymisierung praktisch nicht möglich.[49] Außerdem geht die Betroffenheit über das Individuum hinaus und betrifft auch verwandte Personen. Deshalb ist der spezifische Schutz dieser Daten unabdingbar.

7.2.3 Erhöhung der Identifikationswahrscheinlichkeit durch große Datenmengen

Bei der Nutzung (pseudonymisierter) gesundheitsbezogener Daten, also der Verarbeitung besonderer Kategorien personenbezogener Daten („sensible Daten") ist insbesondere zu bedenken, dass sich die Wahrscheinlichkeit, Daten einer konkreten Person zuordnen zu können, durch große Datenmengen erhöht. Je mehr Daten über eine bestimmte Person bekannt sind, desto einfacher ist es, diese zu identifizieren. Durch eine Identifikation würden aber pseudonymisierte Daten zu Echtdaten, die nur unter sehr strengen Voraussetzungen dokumentiert und verarbeitet werden dürfen.

Diese Identifikation steht somit im Spannungsverhältnis zur Intention, keine Echtdaten sondern eben nur pseudonymisierte Daten verarbeiten zu wollen. Der Sinn der Pseudonymisierung besteht naturgemäß darin, verschiedene Daten einer konkreten Person zuordnen zu können, ohne ihre Identität zu kennen.

Eine große Datenmenge kann dadurch entstehen, dass (wenige) Daten über einen langen Zeitraum verarbeitet, Daten aus unterschiedlichen Datenerhebungen derselben oder verschiedener Stellen über das Pseudonym mit einander verknüpft werden oder der Kombination aus beiden Fällen.

Das Entstehen großer Datenmengen kann beispielsweise durch die Verankerung verpflichtender Löschfristen oder die Verwendung unterschiedlicher Pseudonyme bei verschiedenen Datenerhebungen verhindert oder zumindest eingeschränkt werden.

[49] *Weichert* in *Kühling/Buchner* (Hrsg), DSGVO-Kommentar Art. 4 Nr. 13 Rz 5.

Wie so oft im Bereich des Datenschutzes ist auch im Zusammenhang mit der Erhöhung der Identifikationswahrscheinlichkeit durch große Datenmengen eine fundierte Abwägung des Datenschutzes auf der einen und dem mit Datenerhebungen verbunden öffentlichen Interesse auf der anderen Seite erforderlich.

8. Zusammenfassung

Ziel dieser Position ist es, die notwendigen technischen und rechtlichen Vorgaben der Verarbeitung von mit ELGA verfügbar gemachten ELGA-Gesundheitsdaten und von genetischen Daten, insbesondere im Hinblick auf Wissenschaft und Forschung, darzulegen.

Für die Verarbeitung besonderer Kategorien personenbezogener Daten („sensible Daten") sind die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO) sowie das Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl. I Nr. 165/1999,derzeit geltendes Recht.

Gesundheitsdaten sowie genetische Daten stellen aufgrund ihrer „Sensibilität" eine besondere Kategorie personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO dar.

Die DSGVO definiert Gesundheitsdaten als eine besondere Kategorie personenbezogene[r] Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (vgl. Art. 4 Z 15 DSGVO). ErwG 35 der DSGVO erweitert diese Definition, sodass selbst jene Daten, die Rückschlüsse – wenn auch nur mittelbar – auf den Gesundheitszustand zulassen, als Gesundheitsdaten iSd DSGVO zu qualifizieren sind[50].

Die DSGVO enthält darüber hinaus auch eine Legaldefinition der genetischen Daten. Gemäß Art. 4 Z 13 DSGVO handelt es sich bei genetischen Daten um personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

Grundsätzlich ist die Verarbeitung besonderer Kategorien personenbezogener Daten („sensible Daten"), worunter sowohl Gesundheitsdaten als auch genetische Daten zählen, gemäß Art. 9 Abs. 1 DSGVO verboten. In Art. 9 Abs. 2 DSGVO sind die Ausnahmen vom Verarbeitungsverbot besonderer Kategorien personenbezogener Daten geregelt. Zu beachten gilt im innerstaatlichen Recht zudem die im Verfassungsrang stehende

[50] Vgl. *Hödl* in *Knyrim* (Hrsg), DatKomm Art. 4 DSGVO Rz 158.

Bestimmung des § 1 Abs. 2 S 2 DSG, die im Zusammenhang mit dem in § 1 Abs. 1 verbrieften Grundrecht auf Geheimhaltung stehen.

Der Begriff „wissenschaftliche Forschungszwecke" ist der DSGVO und dem österreichischen Datenschutzrecht grundsätzlich bekannt und auch an verschiedenen Stellen erwähnt; die DSGVO enthält jedoch keine Legaldefinition des Begriffes „Forschung", allerdings ist der Begriff dem ErwG 159 der DSGVO entsprechend weit auszulegen.

Art. 9 Abs. 2 lit j DSGVO erlaubt die Verarbeitung besonderer Kategorien personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche und historische Forschungszwecke sowie für statistische Zwecke, soweit diese dafür erforderlich ist. Durch die in Art. 9 Abs. 2 lit. j DSGVO enthaltene Öffnungsklausel wird jedem Mitgliedstaat die Möglichkeit zur Erlassung spezifischer Bestimmungen eingeräumt. Auf nationaler Ebene sind in Österreich im Bereich der wissenschaftlichen Forschung insbesondere das DSG und das FOG zu beachten. § 7 DSG kommt jedoch nicht zur Anwendung, wenn materien-gesetzliche Regelungen die Verarbeitung von Daten zum Zweck der wissenschaftlichen Forschung vorsehen. So gehen die Regelungen des FOG der Bestimmung in § 7 DSG als leges speciales vor[51], jedoch nicht zwangsläufig anderen materien-gesetzlichen Regelungen.

Im 2. Abschnitt des FOG findet sich die Durchführung der DSGVO samt ergänzender Regelungen und so regelt § 2d FOG die grundlegenden Bestimmungen zum Schutz personenbezogener Daten. In Übereinstimmung mit den Art. 9 Abs. 2 lit. j und Art. 89 Abs. 1 DSGVO enthält § 2d Abs. 1 FOG einen Katalog angemessener Maßnahmen, die insbesondere einzuhalten sind.

Die Elektronische Gesundheitsakte (ELGA) wird in § 2 Z 6 GTelG 2012 definiert als ein Informationssystem, das allen berechtigten ELGA-Gesundheitsdiensteanbietern (ELGA-GDA) und ELGA-Teilnehmer/inne/n ELGA-Gesundheitsdaten in elektronischer Form orts- und zeitunabhängig zur Verfügung stellt. Die gesetzlichen Grundlagen für ihre Verwendung sind das GTelG 2012, insbesondere sein 4. Abschnitt (Elektronische Gesundheitsakte [ELGA]), sowie die ELGA-VO 2015.Zugriff auf ELGA haben nur ELGA-GDA, eine in § 2 Z 10 GTelG 2012 abschließend aufgezählte Teilmenge aller Gesundheitsdiensteanbieter (GDA) iSd § 2 Z 2 GTelG 2012. In ELGA dürfen nur ELGA-Gesundheitsdaten iSd § 2 Z 9 GTelG 2012 verarbeitet werden. ELGA-GDA haben die ELGA-Gesundheitsdaten gemäß § 20 Abs. 1 und Abs. 2 GTelG 2012 in geeigneten Datenspeichern und Verweisregistern zu speichern. Das GTelG 2012 und die ELGA-VO 2015 sehen eine Reihe angemessener und spezifischer Maßnahme zur Wahrung der Grundrechte und Interessen der betroffenen Person vor, etwa das Verarbeitungsverbot iSd § 14 Abs. 3 GTelG 2012, die Pflicht zur technischen Sicherstellung des rollenbasieren Zugriffs gemäß § 3 Abs. 3 GTelG 2012 iVm Anlage 1 GTelV 2013 und die Pflicht zur eindeutigen Identifikation gemäß den §§ 18 f GTelG 2012, ebenso wie die in den §§ 17b bis 17j ELGA-VO 2015 verankerten Sicherheitsanforderungen am dem erforderlichen

[51] *Knotzer*, Wissenschaftliche Forschung und Datenschutz, ZTR 2018, 206.

Zugriffsschutz, das Protokollierungssystem (§ 22 GTelG 2012) sowie die ELGA-Teilnehmer/innen/rechte.

Da es sich bei § 2d Abs. 2 Z 3 FOG um eine lex posterior zu § 14 Abs. 3 GTelG 2012 handelt, ist Registerforschung mit durch ELGA verfügbar gemachte ELGA-Gesundheitsdaten zwar an sich rechtlich zulässig, aber technisch nicht möglich: Die Herausgabe aller in ELGA gespeicherten Daten sämtlicher ELGA-Teilnehmer/innen in pseudonymisierter Form („Big Data") ist weder der ELGA-Ombudsstelle noch den Betreibern der Datenspeicher und Verweisregister technisch möglich.

Zur technischen Unmöglichkeit gesellen sich zahlreiche datenschutzrechtliche Probleme, die bis dato ungeklärt sind. Insgesamt ist festzuhalten, dass die organisatorischen und technischen Datensicherheitsmaßnahmen in Hinblick auf ELGA durch allfällige sekundäre Verwendungsmöglichkeiten von ELGA nicht unterlaufen werden dürfen, wobei gegebenenfalls zumindest ein gleichwertiger Ersatz dieser organisatorischen und technischen Datensicherheitsmaßnahmen vorzusehen ist. Der Umgang mit menschlichen genetischen Daten für Zwecke der Forschung ist in § 66 GTG geregelt. Diese Bestimmung ist gegenüber dem FOG als lex specialis zu sehen und geht ihr daher vor. Die Verpflichtung im GTG zur De-Identifikation der Proben (und allfälliger nicht-medizinischer genetischer Daten), welche nur in den Einrichtungen erfolgen darf, die über eine gültige Einwilligung der betroffenen Person für diese Zuordnung verfügen, soll weitgehend verhindern, dass die genetischen Daten dieser Person und ihrer Verwandten/Nachkommen im Lauf der Zeit mit Fortschreiten der technischen Möglichkeiten auf diese rückführbar werden.

Die Regelungen des § 66 GTG stehen dabei einem internationalen Austausch von Forschungsdaten grundsätzlich nicht entgegen, sondern ermöglichen sie bei gleichzeitiger Sicherstellung der Nichtrückführbarkeit der genetischen Daten auf die Patienten/Probanden und ihre Verwandten/Nachkommen auch für die kommenden Generationen.

Das FOG sieht eine bestimmte Verschlüsselungstechnik vor, die aber nicht in der Lage ist, die spezifische Schutzwürdigkeit im Gesundheitswesen zu erfüllen.

Anhand von Genanalysen ist, insbesondere aufgrund der Tatsache, dass sich die genetischen Daten eines Menschen im Laufe seines Lebens normalerweise nicht ändern, eine sichere Identifizierung von Personen möglich. Bei Vorliegen von identifizierten Referenzdaten kann eine Zuordnung zu einer bestimmten Person ohne weiteres erfolgen, daher ist eine Anonymisierung praktisch nicht möglich.[52] Außerdem geht die Betroffenheit über das Individuum hinaus und betrifft auch verwandte Personen. Darüber hinaus erhöht sich die

[52] *Weichert* in *Kühling/Buchner* (Hrsg), DSGVO-Kommentar Art. 4 Nr. 13 Rz 5.

Identifikationswahrscheinlichkeit auch durch das Vorliegen großer Datenmengen. Deshalb ist der spezifische Schutz dieser Daten unabdingbar.

Aus den oben genannten Gründen ergibt sich die besondere Schutzwürdigkeit von ELGA-Gesundheitsdaten und genetischen Daten.

Impressum

Medieninhaber und Herausgeber:
Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz (BMASGK),
Stubenring 1, 1010 Wien
Verlags- und Herstellungsort: Wien
Autorinnen und Autoren: DI Dr. Eva Claudia Lang, Mag. Eva-Maria Pfandlsteiner, LL.M., Dr. Gabriele Satzinger, Ing. Robert Scharinger BSc (Hons) MSc MBCS, Mag. Barbara Schmeissl, Mag. Thomas Worel
Wien, 2. September 2019

Bestellinfos: Kostenlos zu beziehen über das Broschürenservice des Sozialministeriums unter der Telefonnummer 01 711 00-86 2525 oder per E-Mail unter broschuerenservice@sozialministerium.at.

Bundesministerium für
Arbeit, Soziales, Gesundheit
und Konsumentenschutz
Stubenring 1, 1010 Wien
+43 1 711 00-0
sozialministerium.at