Rechtliche Rahmenbedingungen für Sekundärnutzung gespendeter Gesundheitsdaten in Österreich

Das Smart FOX Data Governance Framework

Version 1.0 (August 2026)

Autoren (alphabetisch sortiert)

- Lorenz Dolanski-Aghamanoukjan, BSc (GÖG)
- Univ.-Prof. Dr. Nikolaus Forgó (UNIVIE)
- Theresa Henne, LL.M., BA (UNIVIE)
- Saskia Kaltenbrunner, MRes (UNIVIE)
- Elisabeth Klager, MSc (LBI DHPS)
- Benjamin Schuster, BSc (LBI DHPS)
- Ekin Fidel Tanriverdi, BA, MSc (GÖG)
- Mag.[a] iur. Anna Tauber, BA (UNIVIE)
- Kristina Weishäupl, MSc, MSc, BSc (GÖG)

Review

- DI Dr. Klaus Donsa, BSc (AIT, Projektleitung)

Das Projekt Smart FOX wird von der Österreichischen Forschungsförderungsgesellschaft FFG finanziert (FFG-Fördernummer: 907741).

Empfohlene Zitierweise / How to cite:

Dolanski-Aghamanoukjan, L., Forgó, N., Henne, T., Kaltenbrunner, S., Klager, E., Schuster, B., Tanriverdi, E. F., Tauber, A., & Weishäupl, K. (2026). *Rechtliche Rahmenbedingungen für Sekundärnutzung gespendeter Gesundheitsdaten in Österreich: Das Smart FOX Data Governance Framework* (Version 1.0). Smart FOX Konsortium. Review: K. Donsa. https://doi.org/10.25365/phaidra.1066

Inhaltsverzeichnis

1. Ziel des Deliverables 6

2. Aufbau des Deliverables 7

3. Einleitung in die Rechtsgrundlagen 8

4. Datenzugang und Datenspende 9

4.1. Wem gehören Daten? *9*

4.1.1. Daten als Eigentum 9

4.1.2. Datenschutzrecht 11

4.1.3. Urheberrecht 31

4.1.4. Weitere EU-Rechtsgrundlagen 35

4.2. Wie werden Datenspendende geschützt? *42*

4.2.1. Grundrechte 42

4.2.2. Persönlichkeitsschutz 43

4.2.3. Betroffenenrechte 49

4.3. Datenschutzfolgeabschätzung und Ausnahmen *57*

5. Wie kann Datenspende in Österreich rechtlich funktionieren? 60

5.1. Einschränkungen der Sekundärnutzung von ELGA-Daten *60*

5.2. Rechtliche Verbote und Möglichkeiten für die Verarbeitung von Gesundheitsdaten innerhalb von Smart FOX *64*

Option 1: Weitergabe von ELGA-Daten durch Patient:innen 64

Option 2: Verwendung von ELGA-standardisierten Daten 66

5.3. Datenaltruismus unter dem DGA *67*

5.4. Zur Datenspende motivieren: Datenspende gegen Vergütung *68*

6. Einbindung von Patient:innen in die Projektarbeit (Beitrag von LBI DHPS) 74

6.1.Unsicherheiten und Bedenken zur Nutzung der Daten vom Patient:innenbeirat *74*

6.2. Dauer und Umfang der Spende (Dauerauftrag oder Einzelspende) *75*

6.3. Spendendanimation *75*

6.4. Begriff „Spende“ *75*

6.5. Erwartungshaltung an persönlichen Nutzen *76*

6.6. Wichtigkeit von Aufklärung und Information *76*

7. Datenspendeszenarien in Smart FOX 77

7.1. Gerichtete und ungerichtete Datenspende *77*

7.2. Rechtliche Implikationen der ungerichteten Spende von ELGA-standardiserten Gesundheitsdaten *80*

7.2.1. Patient:innenwunsch, ELGA-standardisierte Daten zu spenden 80

7.2.2. Recherche und Information über die Gesundheitsdatenspende 80

7.2.3. Definition des Zwecks der Gesundheitsdatenspende durch Patient:innen 80

7.2.4. Spende der Gesundheitsdaten 81

7.2.5. Nutzung der gespendeten Gesundheitsdaten 82

7.3. Rechtliche Implikationen der gerichteten Spende von ELGA-standardisierten Gesundheitsdaten *82*

7.3.1. Konzeption einer klinischen Studie durch die Forschenden 83

7.3.2. Organisatorische Vorbereitung der klinischen Studie 84

7.3.3. Set-Up der FOX BOX 84

7.3.4. Durchführung der klinischen Studie 85

7.3.5. Data Linkup zwischen ELGA-standardisierten Daten und Biobanken-Daten oder klinischen Registern 86

7.3.6. Analyse der erhobenen Daten 86

7.4. Follow-Up bei klinisch relevanten Zufallsbefunden („incidental findings“) *89*

7.5. Datenspende durch Minderjährige *92*

7.6. Die Datenspende durch nicht-entscheidungsfähige Personen *95*

7.7. Gesundheitsdaten als Teil des Nachlasses *97*

7.8. Data Linkup *99*

7.8.1. Daten aus anderen Quellen 99

7.8.2. Re-Kontaktierung 100

7.8.3. Erhöhte Risiken bei der Datenverknüpfung 100

7.8.4. Herzinsuffizienz-Register und CRC-Kohorte 101

8. Ausblick für die Sekundärdatennutzung in Österreich 103

8.1. Datennutzung im öffentlichen Interesse *103*

8.2. Möglichkeit der Registrierung als datenaltruistische Organisation *105*

8.3. Möglichkeit der Registrierung als Datenvermittlungsdienst *109*

8.4. Verändert der EHDS die österreichische Rechtslage? (Beitrag von GÖG) *111*

8.4.1 Allgemeines 113

8.4.2 HDAB 114

8.4.3 Datenhalter:innen 115

8.4.4 Datennutzer:innen 116

8.4.5 Fazit 116

9. Schlussbemerkungen 118

10. Literaturverzeichnis 119

11. Abkürzungsverzeichnis 122

1. Ziel des Deliverables

Im Rahmen des vorliegenden Dokuments werden die rechtlichen Rahmenbedingungen für die Sekundärnutzung von ELGA-standardisierten Daten, die Perspektive von Bürger:innen und eine Analyse der Anforderungen eines European Health Data Spaces hinsichtlich der Gesundheitsdatenspende in Österreich dargestellt. Dabei wird darauf eingegangen, unter welchen Umständen die Spende von Gesundheitsdaten rechtskonform passieren kann, welche Voraussetzungen dafür vorzuliegen haben und welche Aspekte hinsichtlich des Schutzes von Bürger:innen zu beachten sind. Im Vordergrund stehen hierbei die einfache Anwendung und der praxisorientierte Aufbau mit dem Ziel, den Inhalt verständlich und umsetzbar zu gestalten.

Der Inhalt sowie die Struktur des Deliverables orientieren sich maßgeblich an den Bedürfnissen und Anforderungen des Konsortiums des Forschungsprojekts Smart FOX. Im Rahmen eines Online-Fragebogens und der sechs Smart FOX Learning Clubs wurde erhoben, welche rechtlichen Fragen für die Konsortialmitglieder von Bedeutung sind. Dementsprechend setzt sich das vorliegende Data Governance Framework mit jenen Governance-Fragen auseinander, welche im Lauf der 24 Projektmonate relevant für das Projekt waren.

Bei dem vorliegenden Dokument handelt es sich um die finale Version des Data Governance Framework, die auf dem ersten Entwurf, der nach neun Monaten Projektlaufzeit richtungsweisend für die Entwicklung des Austrian Health Data Donation Space[1] dienen sollte, sowie einer zweiten, im April 2025 entworfenen Version aufbaut. Mit dieser zweiten Version des Data Governance Frameworks wurden inhaltlich die gerichtete und die ungerichtete Datenspende den User Stories folgend rechtlich analysiert, die informationelle Selbstbestimmung erläutert sowie Data Linkup und die Datenschutzfolgeabschätzung (und deren Ausnahmen) untersucht.

Für Rückmeldungen, weiterführende Fragen oder Anregungen sind die Verfasser:innen des Dokuments äußerst dankbar – gerne per E-Mail an anna.tauber@univie.ac.at.

[1] „Ein virtueller Datenraum, der es Bürger:innen ermöglicht, ihre Gesundheitsdaten für die sekundäre Nutzung in der Forschung zu spenden. Er nutzt bestehende Standards, Technologien und IT-Infrastrukturen und folgt den Prinzipien des Referenzarchitekturmodells (IDS-RAM-4) der International Data Spaces Association (IDSA).“ (Definition aus dem Glossar von Smart FOX, https://www.smart-fox.at/glossar/).

2. Aufbau des Deliverables

Das vorliegende Data Governance Framework besteht aus drei Hauptteilen – diese handeln von der Datenspende, möglichen Spendeszenarien des Forschungsprojekts Smart FOX sowie einem Ausblick auf Sekundärdatennutzung in Österreich.

Im ersten Teil wird eine Einleitung zum Eigentum an Daten, dem Datenschutz, dem Urheberrecht und anderen dabei zu bedenkenden Rechtsgrundlagen gegeben. Außerdem wird der rechtliche Rahmen hinsichtlich einer Datenspende beleuchtet: Neben dem für die Elektronische Gesundheitsakte maßgeblichen Gesundheitstelematikgesetz wird auf Datenaltruismus und die Vergütung als Motivationsfaktor in der Datenspende eingegangen. Anschließend wird behandelt, wie die datenspendenden Personen gesetzlich geschützt werden und wie Bürger:innen das Konzept der Datenspende betrachten.

Der zweite Teil ist auf Spendeszenarien fokussiert, die im Rahmen des Forschungsprojekts aufkamen, in Verbindung mit den *use cases* von Smart FOX. Dabei wird die Datenspende durch minderjährige oder nicht-entscheidungsfähige Personen behandelt. Außerdem werden Gesundheitsdaten als Teil des Nachlasses von Verstorbenen untersucht. Die Unterscheidung zwischen gerichteter und ungerichteter Datenspende wird ebenso aufbereitet wie klinisch relevante Zufallsbefunde, das Recht auf informationelle Selbstbestimmung und Data Linkup.

Schließlich wird im dritten Teil ein Ausblick auf die Zukunft der Sekundärdatennutzung in Österreich gegeben. Besonders die Datennutzung im öffentlichen Interesse, die datenaltruistische Organisation und Veränderungen der österreichischen Rechtslage durch den European Health Data Space bilden Fokuspunkte in diesem Abschnitt.

Kapitel 4.4 (Einbindung der Patient:innen in die Projektarbeit) wurde vom LBI DHPS verfasst, Kapitel 6.3 (Verändert der EHDS die österreichische Rechtslage) von der GÖG und alle anderen Kapitel von der Universität Wien.

3. Einleitung in die Rechtsgrundlagen

Die Nutzung von Gesundheitsdaten ist in Österreich ein sensibles und durch das Gesundheitstelematikgesetz (GTelG) streng reguliertes Thema, insbesondere in Bezug auf die Elektronische Gesundheitsakte (ELGA). Diese Infrastruktur dient der Speicherung und Verarbeitung von gesundheitsbezogenen Daten der österreichischen Bevölkerung zum Zweck der allgemeinen Gesundheitsversorgung.

Diese gesetzlichen Regelungen zur Nutzung der Gesundheitsdaten stehen im Spannungsfeld zwischen dem Schutz der Privatsphäre und dem potenziellen Nutzen für Forschung, Gesundheitssysteme und Wirtschaft, wie etwa durch die Datenschutzgrundverordnung (DSGVO) und das Forschungsorganisationsgesetz (FOG). Neben den nationalen Vorschriften beeinflusst auch die Europäische Datenstrategie in Form des Data Government Act (DGA) und Data Act (DA) maßgeblich den Umgang mit diesen sensiblen Daten.

Zu beachten ist, dass natürliche Personen durch Grundrechte und Persönlichkeitsrechte geschützt werden – diese Rechte sind in verschiedenen Rechtsgrundlagen verankert, besonders nennenswert sind allerdings das Allgemeine Bürgerliche Gesetzbuch (ABGB), das Urheberrechtsgesetz (UrhG), die Charta der Grundrechte der Europäischen Union (GRC) und die Europäische Menschenrechtskonvention (EMRK).

4. Datenzugang und Datenspende

4.1. Wem gehören Daten?

„Wem gehören Daten?“ ist eine Frage, welche im Forschungsprojekt Smart FOX eine zentrale Rolle spielt. Diese Frage wurde z.B. auch im ersten Learning Club behandelt,[2] da die Nutzung von Daten, und somit die Datenspende, davon abzuhängen scheint. Bevor in Betracht gezogen werden kann, Daten für Forschungszwecke zu spenden, muss geklärt werden, wer überhaupt die Möglichkeit hat, dies zu tun. Es gibt jedoch kein eindeutiges rechtliches Konzept des Eigentums über Daten, daher wird in diesem Abschnitt dargelegt, welche Rechte und Pflichten stattdessen in Bezug auf das Forschungsprojekt Smart FOX relevant sind.

4.1.1. Daten als Eigentum

Aus rechtlicher Perspektive wird zumeist nicht von Eigentum an Daten gesprochen, da dieses Konzept rechtlich stark umstritten und nicht in den relevanten Gesetzen, wie etwa der DSGVO, enthalten ist.[3] Daten „gehören“ also *per se* niemanden; stattdessen gibt es unterschiedliche Rechte, die verschiedene Akteur:innen an Daten haben können. Es existiert viel Literatur, die „data ownership“[4] als ein mögliches zukünftiges Rechtskonzept diskutiert oder als ethische Forderung stellt. Es lohnt sicher daher, kurz zu erörtern, warum das Konzept „data ownership“ keinen zielführenden analytischen Rahmen für Smart FOX darstellt.

Bisherige Forschung behandelt das Problem von „data ownership“ unterschiedlich – je nachdem, ob es aus ethischer, rechtlicher, politischer oder kommerzieller Perspektive adressiert wird.[5] Aus ethischer Sicht ergeben sich hier oft Forderungen nach „ownership“ der Betroffenen.[6] Diese werden meist mit dem Argument verneint, dass Eigentum an Daten eben nicht existiert, da Daten nicht die Hand wechseln können wie herkömmliches Eigentum. Hummel et al. aber argumentieren, dass diese ethischen Forderungen nicht einfach beiseitegeschoben werden sollten, sondern dass es bei

[2] Siehe zu den Learning Clubs: https://www.smart-fox.at/projektergebnisse/learning-clubs/.
[3] Siehe dazu z.B. *Wessels/Laubach/Buxmann*, Personenbezogene Daten in der digitalen Ökonomie – Eine wirtschaftliche und juristische Betrachtung, in: *Ochs/Friedewald/Hess/Lamla* (eds) Die Zukunft der Datenökonomie. Medienkulturen im digitalen Zeitalter, Springer VS; oder *Asswad/Gómez* Data Ownership: A Survey. Information 2021, 12, 465.
[4] Siehe dazu z.B. *Hummel/Braun/Dabrock*, Own Data? Ethical Reflections on Data Ownership, Philosophy & Technology 2021, 545.
[5] *Mirchev/Mircheva/Kerekovska*, The Academic Viewpoint on Patient Data Ownership in the Context of Big Data: Scoping Review, Journal of Medical Internet Research 2020.
[6] *Hummel/Braun/Dabrock*, Own Data? Ethical Reflections on Data Ownership, Philosophy & Technology 2021, 545.

ethischen Diskussionen um „data ownership“ im Kern darum geht, Betroffenen mehr Kontrolle über ihre Daten zu geben. Wie Ballantyne schreibt, ist „data ownership“ hauptsächlich als Metapher zu sehen, die eine Reihe an Beziehungen zwischen Menschen und Daten vereinfacht darstellt.[7]

Auch aus ethischer Sicht kann es jedoch sein, dass die Vorstellung von Daten als Eigentum nicht etwa die ideale Lösung für Betroffene darstellt.[8] Es mag zwar scheinen, dass Menschen dadurch Forderungen nach der Kontrolle über ihre eigenen Daten erheben können – die Logik der Daten als Eigentum führt jedoch auch dazu, dass Menschen ihre Daten verkaufen und Ansprüche darüber verlieren könnten. Die Idee von Daten als Eigentum hängt also eng mit Fragen der Vergütung für Daten zusammen (siehe dazu Kapitel 5.3) und muss sich denselben Kritikpunkten stellen: dass Daten dadurch transaktional und kommodifiziert werden.

Da sich aus dem Rechtsrahmen eine Reihe von Rechten und Pflichten bezüglich Daten herleiten lässt, jedoch aber kein Eigentum, empfehlen die Verfasser:innen dem Konsortium des Forschungsprojekts Smart FOX, **sich auf Rechte und Pflichten gegenüber den betroffenen Personen zu konzentrieren und das Konzept des Dateneigentums als ethische Diskussion zu beachten, Daten jedoch nicht als juristisch eigentumsfähig zu behandeln**. Einerseits würde diese Betrachtungsweise nicht dem Rechtsrahmen entsprechen. Andererseits wäre die Annahme von Dateneigentum evtl. auch konzeptuell eher hinderlich als hilfreich. Denn aus praktischer Sicht werden Daten eben nicht genau wie Eigentum weitergegeben oder verkauft. Daten können vervielfältigt werden und die Einwilligung zur Weitergabe von Daten bedeutet rechtlich auch nicht, dass Betroffene keine Rechte mehr an ihnen haben. Des Weiteren ist die Datenerhebung ein Prozess der Ko-Kreation – und Eigentum an den erhobenen Daten somit schwer zu argumentieren.[9]

In der Praxis ist für das Forschungsprojekt Smart FOX wohl relevanter zu klären, welche unterschiedlichen Rechte es an Daten gibt und welche Anforderungen sich daraus ergeben. Insbesondere relevant sind hier das Datenschutzrecht und das Urheberrecht: Daher folgt in den nächsten Kapiteln ein Überblick dieser beiden Rechtsgebiete, mit Fokus auf den für Smart FOX relevanten Aspekten.

[7] *Ballantyne*, How should we think about clinical data ownership?, Journal of Medical Ethics 2020, 289.
[8] *Cofonet*, Beyond Data Ownership, Law Review 2021-2022 501 (523).
[9] *Ballantyne*, How should we think about clinical data ownership?, Journal of Medical Ethics 2020, 289.

4.1.2. Datenschutzrecht

4.1.2.1. Der europäische und österreichische datenschutzrechtliche Rahmen

Das Datenschutzrecht regelt den Umgang mit personenbezogenen Daten und den Schutz der Privatsphäre in Bezug auf Daten. Die DSGVO reguliert auf der Ebene der Europäischen Union (EU) die Verarbeitung personenbezogener Daten und ist somit auch in Österreich direkt anwendbar und zu beachten.[10]

Da die DSGVO eine europarechtliche Verordnung ist, gilt sie direkt auf nationalstaatlicher Ebene und musste nicht erst national umgesetzt werden. Grundsätzlich ist der Datenschutz also in EU-Ländern harmonisiert. Trotzdem können Unterschiede auf nationalstaatlicher Ebene entstehen. Dies kann durch sogenannte Öffnungsklauseln passieren, welche in der DSGVO enthalten sind und in Bezug auf manche Fragen den Mitgliedsstaaten einen gewissen, klar definierten Handlungsfreiraum lassen. Für Fragen des Datenschutzrechts in Österreich gilt es also, oft auch das nationale Datenschutzgesetz (DSG) heranzuziehen, bzw. für die Forschung das FOG oder andere speziellere Normen, wie z.B. das GTelG. [11] [12] [13]

Das DSG und das FOG regeln teilweise ähnliche Bereiche – es gibt also Überschneidungen, in deren Fall das Zusammenspiel zwischen DSG und FOG nicht endgültig geklärt ist.[14] So regeln sowohl § 7 DSG als auch § 2d FOG die Einwilligung und die Forschungsausnahme als Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten. Die Unklarheit über das Zusammenspiel dieser Rechtsvorschriften im DSG und im FOG stammt hauptsächlich daher, dass die konkrete Anwendbarkeit des FOGs auf Forschungszwecke zu verstehen geben würde, dass § 2d FOG eine speziellere Norm ist und somit vorrangig zu § 7 DSG zur Anwendung kommen sollte. Die österreichische Datenschutzbehörde wendet jedoch weiterhin § 7 DSG an. [15] Die Datenschutzbehörde selbst scheint die Rechtslage also so zu interpretieren, dass § 7 DSG weiterhin

[10] 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.
[11] Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten.
[12] Bundesgesetz über allgemeine Angelegenheiten gemäß Art. 89 DSGVO und die Forschungsorganisation.
[13] Bundesgesetz betreffend Datensicherheitsmaßnahmen bei der Verarbeitung elektronischer Gesundheitsdaten und genetischer Daten (Gesundheitstelematikgesetz 2012 – GTelG 2012).
[14] *Lachmayer/Souhrada-Kirchmayer*, Datenschutzrecht in der wissenschaftlichen Forschung, zfhr 2018, 153 (157)).
[15] DSB 07.06.2018, DSB-D202.207/0001-DSB/2018.

zur Anwendung kommen kann, trotz der wohl herrschenden Meinung in der Literatur[16], dass § 2d FOG die allgemeinere Bestimmung des DSG verdrängt. Es ist insbesondere für die Einwilligung relevant zu klären, welche Regelung vorrangig zur Geltung kommt. Daher wird in Kapitel 4.2.3 zu den Betroffenenrechten noch genauer darauf eingegangen. Zunächst werden in den folgenden Abschnitten jedoch die datenschutzrechtlichen Grundlagen für das Forschungsprojekt erklärt, jeweils mit Verweis auf die relevanten Bestimmungen der DSGVO, des DSG und des FOG.

Hervorzuheben ist bereits an dieser Stelle, dass die diversen neuen Rechtsakte auf europäischer Ebene, wie etwa der Data Governance Act (DGA), der European Health Data Space (EHDS) oder auch der AI Act (AIA), die Geltung der Rechtsvorschriften der DSGVO im Grundsatz unberührt lassen. Der am 19. November 2025 präsentierte Vorschlag für eine Digital-Omnibus Verordnung[17] hat das Potenzial, etablierte Grundsätze der Datenverarbeitung grundlegend zu verändern, ist jedoch derzeit eben nur ein Vorschlag.

4.1.2.2. Definition von personenbezogenen Daten

Die Definition von personenbezogenen Daten scheint zwar auf den ersten Blick simpel, ist jedoch eine kurze Erklärung wert – u.A. auch, weil dazu in den Rechtswissenschaften immer noch Uneinigkeit besteht.

Personenbezogene Daten werden in der DSGVO als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (…) beziehen“, definiert (Art 4 DSGVO). **Pseudonymisierte Daten**, also Daten, welche indirekt auf Personen zurückgeführt werden können, gelten ebenfalls als personenbezogene Daten und fallen in den Anwendungsbereich der DSGVO. **Anonymisierte Daten** fallen nicht in den Anwendungsbereich der DSGVO. Die Unterscheidung zwischen pseudonymisierten und anonymisierten Daten ist deshalb eine der meistdiskutierten Fragen in diesem Bereich der Rechtswissenschaften. Es gibt für die Evaluierung von Einzelfällen viel Material, an welchem man sich orientieren kann. [18] Oft ist die Unterscheidung allerdings trotzdem nicht einfach und führt zu Rechtsunsicherheiten.

[16] *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, Datenschutzgesetz (2018) §7 Rz 10; Feiler/Forgó, EU-DSGVO und DSG: Kommentar, 527.
[17] Europäische Kommission, Vorschlag für eine Digital-Omnibus-Verordnung. https://digital-strategy.ec.europa.eu/de/library/digital-omnibus-regulation-proposal
[18] Eine Unterscheidung zwischen anonymen und pseudonymen Daten findet sich in der DSGVO wieder, allerdings nur in den Erwägungsgründen (ErwGr 26). Zusätzlich gibt es Material der Art-29-Datenschutzgruppe, z.B. Stellungnahme 5/2014 zu Anonymisierungstechniken. Auch Urteile auf EU-Ebene können herangezogen werden, am prominentesten dazu *EuGH-Breyer* (EuGH 19.10.2016, C,-582/14 – Breyer).

Zur Unsicherheit trägt die Tatsache bei, dass **nationale Datenschutzbehörden** sich für unterschiedliche Implementierungen der Unterscheidung zwischen anonymisierten und pseudonymisierten Daten entschieden haben.[19] Da es sich bei Smart FOX um ein österreichisches Forschungsprojekt mit österreichischen Konsortium-Partnern handelt, gilt es, sich für die Interpretation an jener der österreichischen Datenschutzbehörde zu orientieren. Diese hat bisher tendenziell einen risikobasierten Ansatz gewählt, demnach es ein gewisses Zuordnungsrisiko geben kann und Daten trotzdem als anonymisiert bezeichnet werden können. In Wahrscheinlichkeiten ausgedrückt liegt eine Anonymisierung vor, wenn die Daten auf eine Gruppe von zumindest sechs Personen hinweisen und darüber hinaus nicht reidentifizierbar sind.[20] Sollte das Forschungsprojekt in Zukunft in irgendeiner Form auf andere Länder erweitert werden, so gilt es, sich an jener nationalen Datenschutzbehörde mit dem restriktivsten Zugang zu orientieren.

Selbst wenn eine weniger strenge Interpretation von personenbezogenen Daten gewählt wird, ist es nach derzeitigem Stand im Forschungsprojekt **Smart FOX** nicht möglich, mit komplett anonymisierten Daten zu arbeiten. Es gilt nämlich zu bedenken, dass es für Smart FOX wertvoll ist, nicht nur einzelne Datenpunkte wie z.B. einzelne eMedikationsdaten zu verarbeiten, sondern Daten, die verknüpft werden können und ein genaues Bild über die Gesundheit einer Person abgeben, welches möglicherweise so individuell ist, dass es das Risiko der Re-Identifizierbarkeit erhöht (trotz Löschung von Namen, Geburtsdaten, etc.).

Aus diesen Gründen geht das Projekt davon aus, dass personenbezogene Daten gespendet werden. Die Verarbeitung fällt also in den **Anwendungsbereich der DSGVO** und die in der DSGVO erforderlichen Maßnahmen müssen umgesetzt werden. Das Smart FOX-Konsortium arbeitete daher von Anfang an daran, entsprechende Mechanismen zu entwickeln, um diese notwendigen Maßnahmen umzusetzen.

Neue Rechtsakte, insbesondere der EHDS, bauen auf diesem **System der Unterscheidung** zwischen Anonymisierung und Pseudonymisierung auf – sie bieten jedoch keine neuen Anhaltspunkte, um die Definitionen endgültig zu klären und zu harmonisieren.[21]

[19] Siehe dazu z.B. *Podda/Vigna*, Anonymization Between Minimization and Erasure: The Perspectives of French and Italian Data Protection Authorities, *in Kö/Francesconi/Kotsis/Tjoa/Khalil* (Hrsg), Electronic Government and the Information Systems Perspective: 10th International Conference, EGOVIS 2021, Vol. 12926, Proceedings (2021), 103.
[20] DSB 14.1.2019, DSB-D123.224/0004-DSB/2018; DSB 30.3.2015, DSB-D215.611/0003-DSB/2014.
[21] *He*, From Privacy-Enhancing to Health Data Utilisation: The Traces of Anonymisation and Pseudonymisation in EU Data Protection Law, DISO 2, 2023, 16.

4.1.2.3 Synthetische Daten

Synthetische Daten werden oft als „artificial data that mimic the properties of and relationships in real data"[22] definiert und gelten als innovative Methode, um personenbezogene Daten zu schützen und dennoch Forschung durchführen zu können.[23] Diese Datenart wird zwar z.B. in der KI-VO erwähnt, ist dort jedoch nicht näher definiert.[24]

Die KI-VO selbst bezieht sich auf „anonymisierte[…], synthetische[…] oder sonstige[…] nicht personenbezogene[…] Daten" (Art 59 (1) (b)) und deutet dadurch an, dass synthetische Daten nicht als personenbezogene Daten zu verstehen sind. Dies ist jedoch umstritten.[25] Unterschiedliche Definitionen beziehen sich oft nur darauf, dass Daten synthetisch generiert wurden.

Die einzige rechtssichere Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten bleibt weiterhin die Definition der DSGVO (Art 4 Abs 1 DSGVO). Unter der DSGVO gibt es keine eigene Kategorie für synthetische Daten, diese sind eben einfach Daten mit oder ohne Personenbezug. Es kommt daher auf die Reidentifizierbarkeit der Ergebnisse an und nicht darauf, ob die Daten synthetisch generiert oder verändert wurden. Es ist also auf einer case-by-case-Basis zu evaluieren, ob ein Reidentifizierungsrisiko besteht. Bei vorhandenem Reidentifizierungsrisiko sind die synthetischen Daten als personenbezogen zu handhaben.

Ungeachtet dessen, ob das Ergebnis evtl. als reidentifizierbar gilt oder nicht, werden synthetische Daten zurzeit viel erforscht und im Gesundheitsbereich scheinen hohe Erwartungen an synthetische Daten vorhanden zu sein, um rechtliche Hürden zu überwinden und Datenschutzrisiken zu reduzieren oder zu eliminieren. Wichtig ist dabei jedoch zu bedenken, dass, wie Jacobsen (2023) schreibt, keine Technologie „zero risk" ist, und dass die Darstellung als solche evtl. dazu führt, dass Risiken ignoriert werden.[26]

Das Forschungsprojekt Smart FOX selbst produziert keine synthetischen Daten und nutzt diese auch nicht direkt. Gespendete Gesundheitsdaten könnten jedoch in *use cases* genutzt werden, in welchen synthetische Daten erstellt werden. Der allgemeine rechtliche Rahmen zur Generierung

[22] Pasculli/Virgolin/Myles/Vidovszky/Fisher/Biasin/Mourby/Pappalardo/D'Amico/Torchia/Chebykin/Carbone/Emili/Roeshammer, Synthetic Data in Healthcare and Drug Development: Definitions, Regulatory Frameworks, Issues, CPT: Pharmacometrics & Systems Pharmacology 2025, 14(5).
[23] Bellovin/Dutta/Reitinger, Privacy and Synthetic Datasets 2019, Stanford Technology Law Review, 22(1).
[24] So in Art 10 Abs 5 lit a und Art 59 Abs 1 lit b der KI-VO.
[25] Beduschi, Synthetic data protection: Towards a paradigm change in data regulation? Big Data & Society 2024.
[26] Jacobsen, Machine learning and the politics of synthetic data, Big Data & Society, 2023.

synthetischer Daten ist daher nicht direkt relevant für Smart FOX, es gilt jedoch Folgendes zu beachten:

- Die Verarbeitung personenbezogener Daten, um aus diesen synthetische Daten zu generieren, stellt jedenfalls eine Verarbeitung personenbezogener Daten im Sinne der DSGVO dar.
- Wenn bereits absehbar, sollten Betroffene über die geplante Generierung synthetischer Daten in der Einwilligung im Sinne der Informiertheit über die Verarbeitungsprozesse informiert werden.
- Wenn dies zum Zeitpunkt der Einwilligung noch nicht absehbar ist, etwa bei der ungerichteten Datenspende, so kann die Generierung synthetischer Daten als eine Option bei der Einwilligung angeboten werden. Da unter der DSGVO die Einwilligung „für den konkreten Fall, in informierter Weise“ erfolgen muss (ErwGr 32 DSGVO), muss die Datenverarbeitung in der Einwilligung möglichst konkret beschrieben sein, wozu auch die Generierung synthetischer Daten gehört, insb wenn dies unter Umständen neue Risiken für Betroffene birgt (z.B. wenn synthetische Daten länger aufbewahrt werden sollen als die Ursprungsdaten).
- Wenn Betroffene aus den generierten synthetischen Daten reidentifizierbar sind, so gelten diese weiterhin als personenbezogene Daten, welche nur mit einer gültigen Rechtsgrundlage weiterverarbeitet werden dürfen.
- Falls generierte synthetische Daten nicht mehr reidentifizierbar sind und die Ursprungsdaten nach dem Generierungsprozess gelöscht werden, so kann dies als Datenlöschung gelten und die Verarbeitung der synthetischen Daten erfolgt nicht mehr im Rahmen der DSGVO.

4.1.2.4. Besondere Datenkategorien

Unter den personenbezogenen Daten werden verschiedene Datenkategorien unterschieden. Die sogenannten besonderen Datenkategorien sind in **Art 9 DSGVO** aufgelistet – dazu zählen unter anderem genetische Daten und Gesundheitsdaten. Diese besonderen Datenkategorien begründen ein besonderes Risiko für Betroffene und es gibt deshalb in der DSGVO zusätzliche Schutzmaßnahmen und Einschränkungen der Verarbeitung besonderer Datenkategorien.

Es gibt zwar auch hier oftmals offene (rechtliche) Fragen und Graubereiche zur **Definition von Gesundheitsdaten** (z.B. Lifestyle-Daten).[27] Beim Forschungsprojekt Smart FOX, das auf die Verwendung von strukturierten Gesundheitsdaten abzielt, ist jedoch eindeutig, dass besondere

[27] *Tzanou*, Health Data Privacy under the GDPR (2021),7.

Datenkategorien verarbeitet werden und daher die Regelungen der DSGVO für diese Kategorien anwendbar sind. Dieses Framework ist also unter dem Gesichtspunkt verfasst, dass die Regelungen für besondere Datenkategorien auf Smart FOX zutreffen, und diese Regelungen sind daher in die Analyse im Rahmen dieses Dokuments eingeflossen.

4.1.2.5. Grundsätze in der DSGVO

Art 5 DSGVO hält in Abs 1 folgende Grundsätze für die Verarbeitung personenbezogener Daten fest[28]:

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (lit a)

Damit eine Verarbeitung rechtmäßig ist, muss eine gültige Rechtsgrundlage unter Art 6 DSGVO vorliegen. Die für Smart FOX relevanten Rechtsgrundlagen werden dementsprechend im nächsten Kapitel erläutert. Dieser Absatz bedeutet des Weiteren, dass die Verarbeitung auf eine für die betroffene Person nachvollziehbare Art und Weise geschehen muss und dass die betroffenen Personen über Datenerhebung, Nutzung, Umfang der Verarbeitung, Zweck, Risiken, Vorschriften, Garantien und Rechte aufgeklärt werden müssen. Da im Forschungsprojekt Smart FOX von einer Verarbeitung der Gesundheitsdaten mit Einwilligung ausgegangen wird, geschieht die Aufklärung darüber im Rahmen der Einwilligung. Es ist jedoch hervorzuheben, dass auch bei Verarbeitungen, welche sich nicht auf eine Einwilligung stützen, der Grundsatz der Transparenz gilt und dementsprechend Wege gefunden werden müssen, um diesen zu erfüllen.

Zweckbindung (lit b)

Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht auf eine Weise weiterverarbeitet werden, welche mit diesen Zwecken unvereinbar ist. Es wird in diesem Absatz klargestellt, dass die Weiterverarbeitung zu wissenschaftlichen Forschungszwecken nicht als unvereinbar mit den ursprünglichen Zwecken gilt. Dies ist also eine Ausnahme bzw. Privilegierung, die für Forschungsprojekte in Frage kommt.

Datenminimierung (lit c)

Die Datenverarbeitung muss dem Zweck angemessen, erheblich und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Dieser Grundsatz kann oft im Forschungskontext eine schwierige Frage darstellen. Bei Forschung, die auf einer hohen Datenmenge basiert, z.B. mit Machine-Learning-Methoden, sind das notwendige Maß an Daten sowie welche Verarbeitung dem

[28] Der genaue Wortlaut ist jeweils in Art 5 der DSGVO nachzulesen, die für Smart FOX relevantesten Aspekte sind hier hervorgehoben.

Zweck angemessen ist nur schwer zu definieren, da oft anfangs nicht feststeht, welche Methode zweckführend sein wird und welche Daten die Forschungsergebnisse tatsächlich verbessern werden.

Richtigkeit (lit d)

Daten sollen sachlich richtig und auf dem neuesten Stand sein. Dazu gehören Maßnahmen zur Löschung oder Berichtigung unrichtiger Daten.

Speicherbegrenzung (lit e)

Daten dürfen in personenbezogener Form nur so lange gespeichert werden, wie es für die Zwecke der Verarbeitung erforderlich ist. Auch hier gibt es eine Sonderregelung für die Forschung, welche besagt, dass personenbezogene Daten, die ausschließlich für wissenschaftliche Forschungszwecke verarbeitet werden, „länger" gespeichert werden dürfen – unter dem Vorbehalt, dass geeignete technische und organisatorische Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen durchgeführt werden. Der Wortlaut „länger" präzisiert nicht, ob Daten eventuell gar nicht gelöscht werden müssen. Es ist jedoch jedenfalls bei der Festlegung der Speicherdauer auch der Grundsatz der Datenminimierung zu bedenken, da die Datenverarbeitung auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein sollen.

Integrität und Vertraulichkeit (lit f)

Eine angemessene Sicherheit muss bei der Datenverarbeitung gewährleistet werden, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung oder vor unbeabsichtigter Zerstörung oder Schädigung.

Nach Art 5 Abs 2 DSGVO ist „der Verantwortliche" verantwortlich für die Einhaltung dieser Grundsätze. Die Rolle und Definition der Verantwortlichen werden in Kapitel 4.1.2.7 weiter ausgeführt.

4.1.2.6. Rechtsgrundlagen

Damit eine Datenverarbeitung rechtmäßig ist (Art 5 Abs 1 lit a DSGVO), muss eine gültige Rechtsgrundlage nach Art 6 der DSGVO vorliegen. In diesem Artikel sind **sechs mögliche Rechtsgrundlagen** enthalten, welche jedoch nicht alle relevant für das Forschungsprojekt Smart FOX sind. Daher wird in den nächsten Absätzen auf zwei davon näher eingegangen.

Wenn es sich bei den Daten um sensible Daten handelt (in der DSGVO „**besondere Datenkategorien**" genannt und definiert in Art 9), gibt es zusätzliche Einschränkungen bei der Datenverarbeitung. Diese ist grundsätzlich verboten – es sei denn, es liegt einer der taxativ

aufgezählten Tatbestände unter Art 9 Abs 2 DSGVO vor. Demnach reicht es für die Verarbeitung von besonderen Datenkategorien nicht, wenn eine gültige Rechtsgrundlage unter Art 6 vorhanden ist, sondern es muss zunächst einer der Tatbestände in Art 9 Abs 2 DSGVO vorliegen. Smart FOX stützt sich, während des Projekts und nach derzeitigem Stand auch bei zukünftigen Plänen, auf die ausdrückliche Einwilligung in Art 9 Abs 2 lit a DSGVO, im Zusammenhang mit der Einwilligung als Rechtsgrundlage in Art 6 Abs 1 DSGVO. Dies wird im nächsten Unterkapitel weiter ausgeführt, gefolgt von einer Erklärung der Forschungsausnahme als Rechtsgrundlage und warum diese derzeit keine Alternative für Smart FOX darstellt, aber in Zukunft für die im Kontext von Smart FOX angestrebte Sekundärnutzung von Gesundheitsdaten relevant sein könnte.

Die Einwilligung als Rechtsgrundlage für die Datenverarbeitung in Smart FOX

Um Missverständnissen vorzubeugen, ist wichtig klarzustellen, dass das Konzept der Einwilligung durch Betroffene nicht nur dem Datenschutzrecht entstammt. Ethische und medizinrechtliche Standards (wie auch in den Deklarationen von Helsinki und Taipei und in der Clinical Trials Regulation festgehalten) fordern eine freiwillige und informierte Einwilligung von Teilnehmenden an medizinischen Studien oder Behandlungen. Im **medizinethischen Kontext** geht es bei der Einwilligung in eine Behandlung darum, Menschen informierte Entscheidungen zu ermöglichen, inklusive einer Erklärung, was im Rahmen einer Behandlung zu erwarten ist und welche Risiken oder nachteilige Auswirkungen daraus entstehen könnten. Im Datenschutzrecht geht es hingegen um die Verarbeitung der personenbezogenen Daten und die Risiken und nachteiligen Auswirkungen, die daraus entstehen können. In der Praxis wird Betroffenen oft ein Dokument vorgelegt, welches beide Aspekte der Einwilligung abdeckt.

Die Einwilligung der Betroffenen ist eine von sechs möglichen Rechtsgrundlagen der DSGVO, die eine Verarbeitung von personenbezogenen Daten datenschutzrechtlich legitimiert. Die Einwilligung erfolgt im Forschungsprojekt Smart FOX über ein sogenanntes Patient:innenportal. Doch wie muss eine rechtsgültige Einwilligung und der Einwilligungsprozess innerhalb von Smart FOX gestaltet sein? Erwägungsgrund 32 DSGVO führt diese Anforderungen aus: „Die Einwilligung sollte durch eine **eindeutige bestätigende Handlung** erfolgen, mit der **freiwillig**, für den **konkreten Fall**, in **informierter Weise** und **unmissverständlich** bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“.

Der Wortlaut der „**eindeutig bestätigenden Handlung**“ verweist darauf, dass eine Opt-Out-Handlung aus der Datenverarbeitung nicht als Einwilligung gelten kann. Es reicht also nicht aus, wenn die Datenspender:innen einer Verarbeitung *nicht widersprechen*, sondern es bedarf einer aktiv-bejahenden Einwilligung. Diese kann schriftlich wie auch mündlich erfolgen – allerdings muss der/die

Verantwortliche für die Verarbeitung nachweisen können (Art 7 Abs 1 DSGVO), dass die Einwilligung erteilt wurde, was in der Praxis meist zu einer schriftlichen Einwilligung führt.

Die Anforderung der **Freiwilligkeit** bedeutet, dass die Einwilligung als Rechtsgrundlage insbesondere in Situationen, wo ein Machtungleichgewicht zwischen Betroffenen und Verantwortlichen besteht, kritisch zu sehen ist. Hatten die Betroffenen tatsächlich eine freie Wahl bei der Einwilligung oder fühlten sie sich unter Druck gesetzt? Bei der Datenspende ist dies dann besonders relevant, wenn Patient:innen von sie behandelnden Ärzt:innen über die Möglichkeit, ihre Daten für Forschungszwecke zu spenden, informiert werden. Es muss sichergestellt werden, dass bei Patient:innen nicht der Eindruck erweckt wird, die Verweigerung der Datenspende hätte Auswirkungen auf ihre medizinische Versorgung und gesundheitliche Betreuung durch die behandelnde:n Ärzt:innen.

Zudem muss eine Einwilligung **informiert** und **unmissverständlich** erfolgen, was bedeutet, dass die Betroffenen über den Zweck und die Dauer der Datenverarbeitung sowie über ihre Rechte nach der DSGVO, und wie diese eingefordert werden können, informiert werden müssen. Die Informationsansprüche werden in Art 13 und Art 14 der DSGVO ausgeführt. Art 12 DSGVO besagt weiter, dass die Informationen in einer „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ bereitgestellt werden müssen, sowie dass diese in kindgerechter Sprache vermittelt werden müssen, wenn es sich bei den Betroffenen um Kinder handelt.[29] Innerhalb des Einwilligungsprozess für eine Datenspende müssen also die Informationen den Betroffenen über das Patient:innenportal zur Verfügung gestellt werden.

Weiter erklärt Erwägungsgrund 32 der DSGVO, dass die Einwilligung **für einen konkreten Fall** erfolgen muss. Dies bezieht sich auf den Grundsatz der „Zweckbindung“ nach Art 5 Abs 1 lit b, der besagt, dass personenbezogene Daten nur für „festgelegte, eindeutige und legitime Zwecke erhoben werden“ dürfen. Zum Zeitpunkt der Einwilligung muss also klar festgelegt sein, für welche Verarbeitungszwecke die Einwilligung erfolgt. Eine Verarbeitung über diesen Rahmen hinaus ist demnach rechtswidrig. Jedoch dürfen die Mitgliedsstaaten über Art 89 Abs 1 DSGVO Ausnahmen im nationalen Recht festlegen, durch die dem Zweckbindungsgrundsatz zum Wohle der Forschung eine gewisse Flexibilität eingeräumt wird. Österreich hat sowohl in § 7 DSG als auch in § 2d FOG solche Ausnahmen für die Forschung vorgesehen. Dies bedeutet, dass personenbezogene Daten im Kontext von Smart FOX als wissenschaftlichem Forschungsprojekt auf Grundlage eines sogenannten „Broad Consents“ verarbeitet werden können. Der Broad Consent erlaubt die Einwilligung in die

[29] *Milkaite/Lievens*, Child-friendly transparency of data processing in the EU: from legal requirements to platform policies, Journal of Children and Media 14, 5.

Datenverarbeitung nicht nur für ein spezifisches Forschungsprojekt, sondern in umfassenderer Form für einen festgelegten Forschungsbereich, z.B. für die Lungenkrebsforschung.[30] Wie breit der Zweck der Einwilligung aber tatsächlich formuliert sein darf, ist eine umstrittene Frage, insbesondere auch, da die Erwägungsgründe zwar wichtig für die Auslegung, aber nicht rechtlich bindend sind, im Gegensatz zu den Artikeln der DSGVO.[31] Klar ist hingegen, dass selbst bei umfangreicher Interpretation des Begriffs Forschungsbereich eine pauschale oder zu vage formulierte Einwilligung unwirksam wäre.[32]

Innerhalb von Smart FOX ist die Nutzung des Broad Consents im Datenspendeszenario der ungerichteten Datenspende vorgesehen. Bei der ungerichteten Datenspende spenden die Betroffenen – anders als bei der gerichteten Datenspende – ihre personenbezogenen Gesundheitsdaten nicht für ein konkretes und fest definiertes Forschungsprojekt, sondern stellen ihre Patient:innendaten für zukünftige Forschungsvorhaben innerhalb eines Forschungsbereichs zur Verfügung.[33] Innerhalb des Einwilligungsprozesses über das Patient:innenportals können die Betroffenen Einschränkungen vornehmen, wie beispielsweise eingrenzen, in welchen geografischen Regionen oder welchen Organisationen ihre Daten der Forschung zur Verfügung stehen.

Eine Herausforderung im Rahmen des Broad Consents ist, dass den Betroffenen zu jedem Zeitpunkt klar sein muss, wer die Verantwortlichen für die Datenverarbeitung sind, also an wen sie sich wenden können, um die Wahrnehmung ihrer Betroffenenrechte einzufordern. Anders als bei der gerichteten Datenspende ist bei der ungerichteten Datenspende zum Zeitpunkt der Einwilligung nicht klar, wer die Verantwortlichen für die Verarbeitung bei zukünftigen Forschungsprojekten sein werden. Um diese Herausforderung zu lösen, muss über das Patient:innenportal von Smart FOX diese Information für die Betroffenen abrufbar sein. Solange die Daten nach einer ungerichteten Datenspende in einer FoxBox „lagern“, müssen hier also die Kontaktdaten der Verantwortlichen der betreibenden Organisation hinterlegt sein. Diese Namen der Verantwortlichen für die personenbezogenen Datenverarbeitungen sowie ihre Kontaktdaten sind innerhalb jedes Profils der Datenspender:innen aktualisiert, sobald die personenbezogenen Daten über die FoxBox von anderen Organisationen abgerufen werden.

[30] *Hallinan*, Broad consent under the GDPR: an optimistic perspective on a bright future, Life Sciences, Society and Policy 16, 1.
[31] *Molnár-Gábor*, Ausgestaltung der Einwilligung in die Datenspende für die Gesundheitsforschung, DuD 45, 2021, 799 (802).
[32] *Molnár-Gábor,* Ausgestaltung der Einwilligung, 799 (802).
[33] Siehe Kapitel 7.1. für eine ausführliche Erklärung der gerichteten und ungerichteten Datenspende, die im Rahmen des Forschungsprojekts Smart FOX definiert wurden.

Der Broad Consent wird oft durch das Konzept des „Dynamic Consent“ ergänzt, durch das den Betroffenen ermöglicht werden soll, die Einwilligung dynamisch anzupassen – also beispielsweise im Nachhinein die Einwilligung zeitweise auszusetzen oder diese nur für weiter eingegrenzte Forschungsvorhaben bereitzustellen.[34] Auch im Fall des Forschungsprojekts Smart FOX ist vorgesehen, dass die Betroffenen ihre Einwilligung noch nachträglich über das Patient:innenportal bearbeiten und zurückziehen können.

Die Einwilligung im Patient:innenportal von Smart FOX

Im Rahmen des Workpackage 4 des Forschungsprojekts Smart FOX wurde bereits das Patient:innenportal als Demonstrator entwickelt und im Konsortialmeeting am 21. Mai 2025 präsentiert. Während im Fall einer gerichteten Datenspende die Forschungseinrichtung direkt die Daten erhält und die Einwilligung nicht bearbeitbar ist, kann bei einer ungerichteten Datenspende, die nachfolgend um zusätzliche Daten erweitert oder auch eingeschränkt werden kann, die Einwilligung durch die Patient:innen im Portal modifiziert werden. Als Patient:in können dabei verschiedene Workflows im Patient:innenportal vorgenommen und entsprechende Informationen für die rechtsgültige Einwilligung abgerufen werden:

- **Anzeige grundlegender Informationen**: Daten können für eine konkrete Studie gespendet werden, wobei vor der Datenspende grundlegende Informationen zur jeweiligen Studie angezeigt werden.
- **Anzeige zusätzlicher Informationen**: Bei Interesse zu einer bestimmten Studie können zusätzliche Informationen durch die Patient:innen sowie eingebundene externe Inhalte abgerufen werden (Bereitstellung bei Klicken auf „Mehr über die Forschungsstudie erfahren“).
- **Details zur Datenspende überprüfen**: Durch die Patient:innen können Modifikationen der Einwilligung vorgenommen werden, indem beispielsweise die konkrete Verwendung der zukünftig gespendeten Daten oder geographische Einschränkungen festgelegt werden.

Die Information der Patient:innen über den Zweck und die Dauer der Datenverarbeitung sowie über ihre Rechte nach der DSGVO kann somit unmittelbar bei der Datenspende erfolgen. Außerdem erlaubt der Einsatz des „Dynamic Consent“ die dynamische Anpassung der Einwilligung direkt durch die Betroffenen selbst.

[34] *Lee, A.R. et al*, Opportunities and challenges of a dynamic consent-based application: personalized options for personal health data sharing and utilization, BMC Medical Ethics 25, 92.

Die qualifizierte elektronische Signatur in Österreich bei der Einwilligung

Die eIDAS-Verordnung der EU (EU-Verordnung Nr. 910/2014, kurz eIDAS-VO) regelt die Bedingungen für die elektronische Identifizierung und enthält Vorschriften für die Vertrauensdienste. Außerdem wird der Rechtsrahmen für die elektronischen Signaturen, Siegel, Zeitstempel und Dokumente sowie Dienste für die Zustellung elektronischer Einschreiben und Zertifizierungsdienste für die Website-Authentifizierung definiert.[35] Diese Rechtsnorm gilt als unionsrechtliche Verordnung unmittelbar in den EU-Mitgliedsstaaten; sie bedarf also keiner Umsetzung in nationales Recht. Laut Art 25 Abs 2 eIDAS-VO ist die Rechtswirkung der qualifizierten elektronischen Signatur (QES) dieselbe wie einer handschriftlichen Signatur. In der eIDAS-VO finden sich außerdem in Art 3 Definitionen der folgenden Begriffe:

> **qualifizierte elektronische Signatur**: erstellt durch qualifizierte elektronische Signaturerstellungseinheit, beruhend auf qualifiziertem Zertifikat für elektronische Signaturen. Sie können den Unterzeichnenden klar zugeordnet werden und stehen unter deren alleiniger Kontrolle;[36]
> **qualifizierte elektronische Signaturerstellungseinheit**: konfigurierte Soft-/Hardware, Verwendung für die Erstellung von elektronischen Signaturen, erfüllt Anforderungen des Anhang II der eIDAS-VO;[37]
> **qualifiziertes Zertifikat für elektronische Signaturen**: wurde als elektronische Bescheinigung, dass die Signaturvalidierungsdaten mit einer natürlichen Person verknüpft sind sowie die Verknüpfung mit dieser Person (Name oder Pseudonym) bestätigt wird, von qualifizierten Vertrauensdiensteanbietenden ausgestellt, erfüllt Anforderungen des Anhang I der eIDAS-VO;[38]
> **qualifizierter Vertrauensdienst**: elektronischer Dienst, der (üblicherweise entgeltlich) elektronische Signaturen, Siegel, Zeitstempel, elektronische Einschreiben oder Webseiten-Authentifizierungszertifikate erstellt, prüft und validiert sowie die Anforderungen der eIDAS-VO erfüllt;[39]
> **qualifizierter Vertrauensdiensteanbietende**: natürliche oder juristische Person, die einen oder mehrere qualifizierte(n) Vertrauensdienst(e) erbringt und der der Status von qualifizierter Vertrauensdiensteanbietenden verliehen wurde.[40]

Im Signatur- und Vertrauensdienstegesetz (SVG), das 2016 in Kraft getreten ist, sind vor allem Aufsicht, Zertifizierung und Einbindung von Vertrauensdiensteanbietenden auf nationaler Ebene

[35] Art 1 eIDAS-VO.
[36] Art 3 Z12 eIDAS-VO.
[37] Art 3 Z23 eIDAS-VO.
[38] Art 3 Z15 eIDAS-VO.
[39] Art 3 Z17 eIDAS-VO.
[40] Art 3 Z20 eIDAS-VO.

rechtlich geregelt. Es legt fest, dass die QES das Erfordernis der Schriftlichkeit des § 886 ABGB erfüllt, jedoch nicht andere gesetzliche Formerfordernisse (z.B. die Einbindung von Notar:innen oder Rechtsanwält:innen).

Die Gleichstellung der QES mit der handschriftlichen Unterschrift bedeutet für die Gesundheitsdatenspende, dass Einwilligungen in die Verarbeitung von personenbezogenen Gesundheitsdaten ausdrücklich und dokumentiert gem. Art 9 Abs 2 lit a DSGVO rechtssicher abgegeben werden können. Eine QES ist also im Kontext von Smart FOX rechtlich zwar nicht erforderlich, wird allerdings in Hinblick auf die Rechtssicherheit durch den Europäischen Datenschutzausschuss empfohlen.[41] Durch die QES kann die datenspendende Person eindeutig authentifiziert sowie identifiziert werden[42] und somit eine hochqualitative und rechtssichere Datensammlung und -verwendung ermöglicht werden.

Alternativen zu der Einwilligung: die Forschungsausnahme als Rechtsgrundlage in Smart FOX

Die Einwilligung ist eine der Rechtsgrundlagen der DSGVO, mit welcher die rechtmäßige Verarbeitung von personenbezogenen Daten möglich ist (Art 6 Abs 1 lit a DGSVO). Die DSGVO gibt nicht direkt einer Rechtsgrundlage Vorrang über andere. Oft ist im Kontext von medizinischen Daten die Einwilligung am naheliegendsten, da diese gemeinsam mit der ethisch bzw. medizinrechtlich erforderlichen Einwilligung eingeholt werden kann. Dennoch gibt es einige Gründe, warum Forschungsprojekte sich auf andere Grundlagen für die Zulässigkeit der Verarbeitung, wie zum Beispiel das Forschungsprivileg anstelle der Einwilligung, stützen. Zunächst ist es häufig in der Praxis quasi unmöglich, für vorhandene Daten eine nachträgliche Einwilligung zur Verarbeitung zu Forschungszwecken einzuholen. Des Weiteren kann eine Einwilligung grundsätzlich jederzeit widerrufen werden. Außerdem ist die Einwilligung nicht etwa die unübertreffliche Maßnahme zur informationellen Selbstbestimmung, als welche sie oft präsentiert wird. Zu bedenken sind die eindeutigen Wissens- und Machtasymmetrien bei der Einholung der Einwilligung, insbesondere wenn es sich bei den Betroffenen um Patient:innen handelt.[43]

Nennenswert ist im Kontext von Smart FOX eine weitere Rechtsgrundlage, obwohl diese derzeit nicht anwendbar für die geplante Form der Datenspende ist und auch nicht konkret der Idee einer

[41] *European Data Protection Board,* Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und„Auftragsverarbeiter“ in der DSGVOVers. 2.0, Rz 101.
[42] *Kalss* in *Kletečka/Schauer,* ABGB-ON[1.06] § 886 Rz 10 (Stand 1.8.2022, rdb.at).
[43] Es ist mittlerweile weitgehend anerkannt, dass eine einmalige Einwilligung informationelle Selbstbestimmung nicht perfekt abdeckt (siehe z.B. *Molnár-Gábor,* Ausgestaltung der Einwilligung*; Hermstrüwer*, Informationelle Selbstgefährdung (2016), 93ff).

Daten*spende* entspricht, sondern die Sekundärdatennutzung ohne Einwilligung ermöglichen würde. In Art 9 Abs 2 lit g DSGVO ist folgender Erlaubnistatbestand für die Verarbeitung besonderer Datenkategorien enthalten:

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

Art 89 Abs 1 legt zusätzlich fest, dass die Verarbeitung geeigneten Garantien unterliegen muss. Abgesehen von der Umsetzung dieser Garantien enthält Art 9 Abs 2 lit j DSGVO jedoch die Möglichkeit der relativ breiten Erlaubnis zur Verarbeitung zu wissenschaftlichen Forschungszwecken. Dieser Absatz allein ist jedoch keine Rechtsgrundlage, die Ausnahme für Forschungszwecke muss in das jeweilige nationale Recht eingeführt werden, um gültig zu sein.

Grundsätzlich hat der österreichische Gesetzgeber ebendiese Gelegenheit genutzt, um eine Ausnahme für die Forschung einzuführen: Diese ist sowohl in § 7 DSG als auch § 2d FOG enthalten. Allerdings ist dies derzeit für Smart FOX kaum relevant, da es für ELGA-Daten eine speziellere Norm gibt, nämlich das GTelG, welches vorrangig zum FOG zur Anwendung kommt, wenn es um ELGA-Daten geht. Das GTelG schränkt, in der derzeitigen Fassung, die Nutzung von ELGA-Daten stark ein und macht die Sekundärnutzung von ELGA-Daten auf Grundlage der Forschungsausnahme praktisch unmöglich (siehe Kapitel 5.1.). Aus diesem Grund wurde die Datenspende im Kontext von Smart FOX so konzipiert, dass ELGA-standardisierte Daten mit der Einwilligung der Betroffenen als Rechtsgrundlage verarbeitet werden sollen.

Jedoch gibt es derzeit Veränderungen im Rechtsrahmen, sowohl auf europäischer als auch auf österreichischer Ebene. Es ist daher durchaus denkbar, dass die Einschränkungen im GTelG reduziert werden und die Sekundärnutzung auf Basis einer anderen Grundlage als der Einwilligung in Zukunft möglich sein wird. Kapitel 5.1. hebt hier die Novellierung des GTelG, welche im September 2024 in Kraft trat, hervor und evaluiert, wie diese Smart FOX betrifft. Zusätzlich untersucht Kapitel 8.4. die möglichen Veränderungen im Rechtsrahmen durch den EHDS. Es ist also möglich, dass einerseits die Sekundärdatennutzung von ELGA-Daten und andererseits dies ohne eine Einwilligung in Zukunft möglich wird, was jedoch außerhalb des (Zeit-)Rahmens des Forschungsprojekts Smart FOX fällt.

4.1.2.7. Rechte und Pflichten der Akteur:innen im Datenschutzrecht

Es gibt im Datenschutzrecht kein Eigentum an Daten im klassischen Sinne. Stattdessen definiert die DSGVO eine Reihe an Rollen im Kontext einer Datenverarbeitung, die mit bestimmten Rechten und Pflichten einhergehen. Nicht immer ist es leicht zu bestimmen, welche Akteur:innen welche Rollen einnehmen. Insbesondere die Differenzierung zwischen Verantwortlichen für die Datenverarbeitung und Auftragsverarbeiter:innen erzeugt in der Praxis häufig Unsicherheiten. Dieses Unterkapitel soll dabei helfen, eindeutig zu identifizieren, welche Akteur:innen im Forschungsprojekt Smart FOX welche Datenschutzrollen einnehmen und welche Pflichten ihnen somit obliegen.

Betroffene oder Datensubjekte

Als Betroffene werden nach Art 4 Abs 1 DSGVO jene Personen bezeichnet, die durch Daten direkt oder indirekt identifizierbar sind. Direkt identifizierbar ist eine Person zum Beispiel durch Name, Sozialversicherungsnummer, Telefonnummer, E-Mail-Adresse oder andere Kennnummern, durch die eine Person eindeutig zugeordnet werden kann. Eine indirekte Identifikation ist über Daten möglich, die weitere Informationen benötigen, um zu einer eindeutigen Identifikation zu führen –so der Fall für die meisten Gesundheitsdaten, z. B. Alter, Gewicht, Krankheitsgeschichte. Die DSGVO erteilt Betroffenen besondere Rechte hinsichtlich ihrer Daten, wie beispielsweise ein Recht auf Auskunft, Löschung oder Widerruf. Diese sogenannten Betroffenenrechte finden sich in Art 12 bis 23 DSGVO.

Verantwortlicher für die Datenverarbeitung

Nach Art 4 Abs 7 DSGVO ist der/die Verantwortliche für die Datenverarbeitung eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die über den Zweck und die Mittel der Verarbeitung bestimmt. Der/die Verantwortliche legt also fest, für welche Ziele, in welchem Umfang und auf welche Weise Daten verarbeitet werden. Diese Rolle nehmen regelmäßig mehrere Akteur:innen innerhalb eines Forschungsprojektes wahr, wenn sie gemeinsam essentielle Fragen der Datenerhebung und/oder Verarbeitung festlegen. In diesem Fall sind sie gemeinsam Verantwortliche und müssen nach Art 26 DSGVO vereinbaren, wer welche Pflichten als Verantwortliche:r übernimmt. Die Verantwortlichen tragen die Verantwortung sicherzustellen, dass die Verarbeitung nach den Vorgaben der DSGVO erfolgt und alle geeigneten technischen und organisatorischen Maßnahmen getroffen wurden, um die Integrität und Sicherheit der Daten zu gewährleisten (Art 24 DSGVO). Zu diesen Pflichten gehört insbesondere die Sicherstellung einer Rechtsgrundlage für die Verarbeitung der Daten, die Einhaltung der Prinzipien nach Art 5 („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“; „Zweckbindung“;

„Datenminimierung“; „Richtigkeit“; „Speicherbegrenzung“; „Integrität und Vertraulichkeit“) und die Gewährleistung der Betroffenenrechte.

Auftragsverabeiter:in

Als Auftragsverarbeiter:in wird nach Art 4 Abs 8 DSGVO jene natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle bezeichnet, die Daten im Auftrag des/der Verantwortlichen verarbeitet. Ein:e Auftragsverarbeiter:in darf also keine Tätigkeiten ausführen, durch die der Zweck und die Mittel der Datenverarbeitung festgelegt werden, sondern ausschließlich mit der Ausführung bereits definierter Verarbeitungsschritte betraut sein. Der Umfang und Zweck der Auftragsverarbeitung muss in einem Vertrag genau geregelt sein (Art 28 DSGVO). Ein:e Auftragsverarbeiter:in haftet nur für Verstöße gegen die DSGVO, wenn er/sie außerhalb der vertraglich festgelegten Pflichten handelt oder diese nicht wahrnimmt (Art 82 Abs 2 DSGVO).

Datenschutzrollen in Forschungsprojekten

Im Rahmen eines Forschungsprojekts ist zusammenfassend wichtig, möglichst früh im Projektverlauf zu prüfen, welche Partner:innen welche Datenschutzrollen einnehmen, wer also (gemeinsame) Verantwortliche und/oder Auftragsverarbeiter:inen sind – dafür kann auch ein Datenmanagementplan verwendet werden. Folglich muss bei gemeinsamer Verantwortlichkeit eine Vereinbarung über die gemeinsame Verantwortlichkeit (auch „Joint Controllership Agreement“) abgeschlossen werden. Im Falle von Auftragsverarbeitung ist ein entsprechender schriftlicher Auftragsverarbeitungsvertrag abzuschließen. Für die Sicherstellung und Dokumentation der technischen und organisatorischen Maßnahmen gem. Art 32 DSGVO ist durch Verantwortliche sowie Auftragsverarbeiter:innen zu sorgen.

Der Europäische Datenschutzausschuss hat 2021 „Leitlinien zu den Begriffen ‚Verantwortlicher‘ und ‚Auftragsverarbeiter‘ in der DSGVO“ veröffentlicht, die zwei Diagramme beinhalten, die bei der Ermittlung der verschiedenen Rollen Hilfe leisten sollen (siehe folgende Seiten):

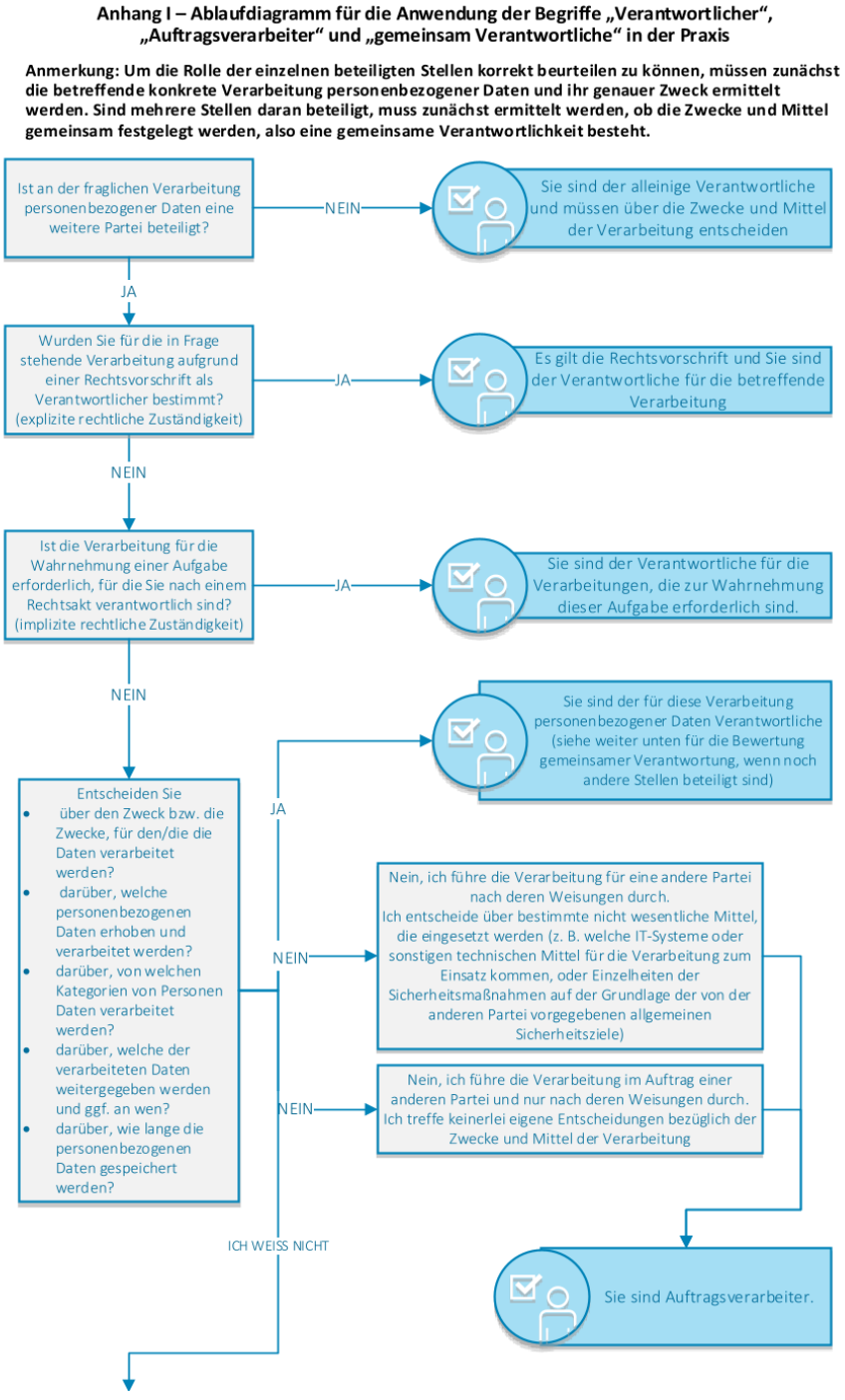

Abbildung 1: Diagramm zu Datenschutzrollen aus den „Leitlinien zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO“ des Europäischen Datenschutzausschusses

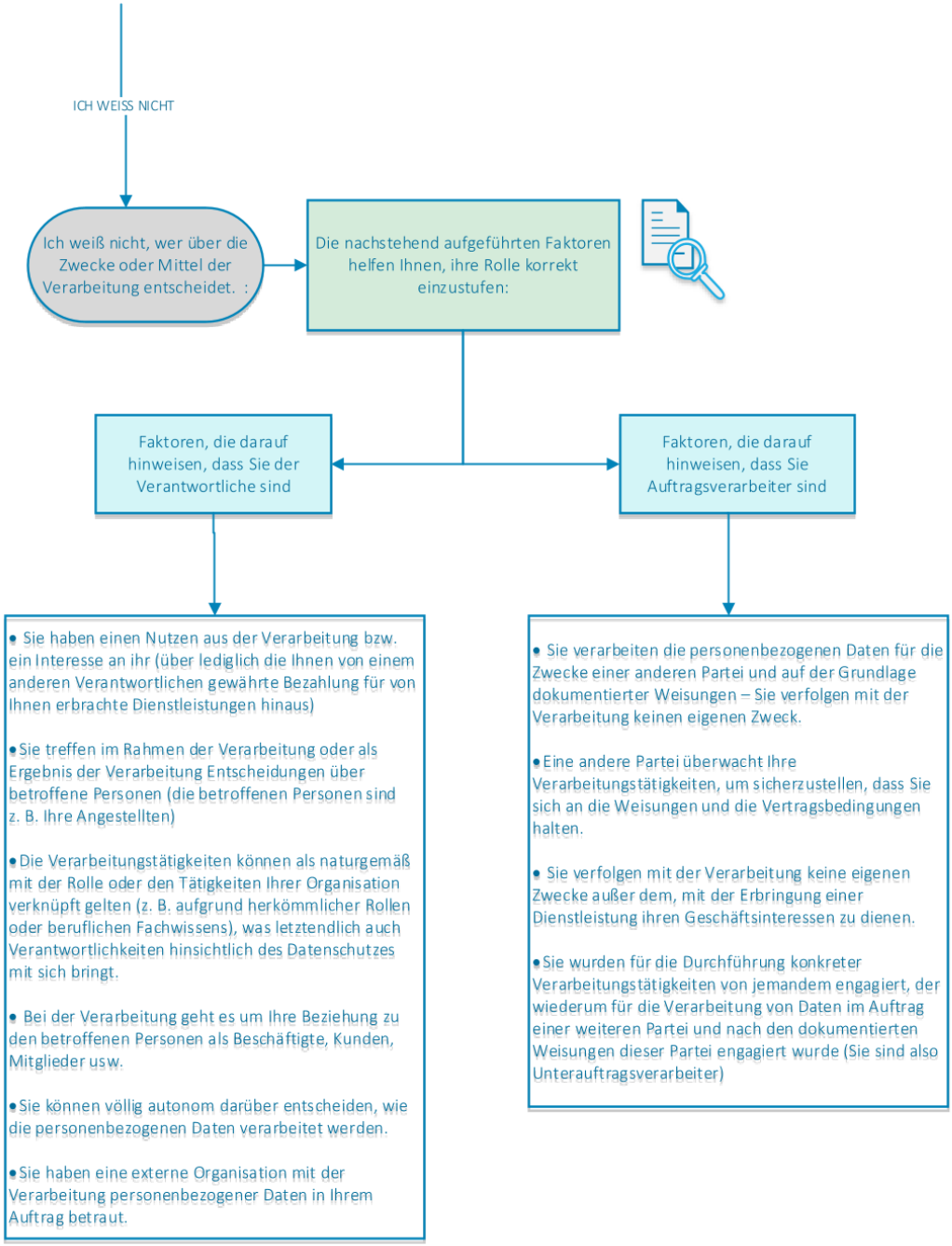

Abbildung 2: Diagramm zu Datenschutzrollen aus den „Leitlinien zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO“ des Europäischen Datenschutzausschusses

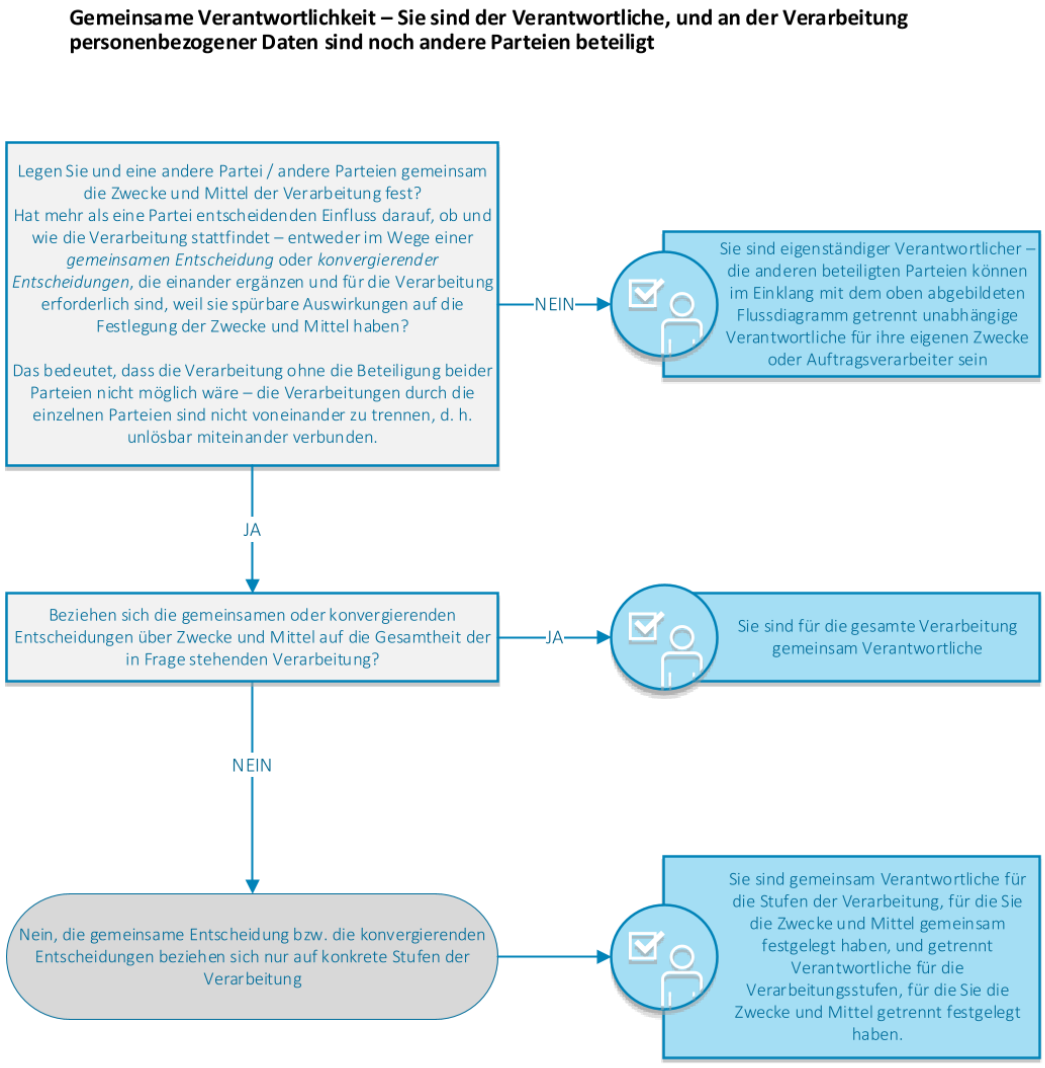

Abbildung 3: Diagramm zu Datenschutzrollen aus den „Leitlinien zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO“ des Europäischen Datenschutzausschusses/ European Data Protection Board

4.1.2.8. Datenschutzrollen in Smart FOX

Im Rahmen des Forschungsprojekts Smart FOX werden Anforderungen für die Datenspende in Österreich erprobt, noch ohne eine vollendete Struktur für einen AHDDS zu haben, für den die Datenschutzrollen konkret definiert werden können. Langfristig sind die Datenschutzrollen in Smart FOX komplex und abhängig von der finalen Form, die Smart FOX annimmt. Unterschiedliche

Szenarien wurden im Rahmen des Projekts mit Partner:innen ausgearbeitet und eine wahrscheinliche Struktur sieht folgendermaßen aus:

Eine natürliche oder juristische Person, z.B. eine Universität, führt Forschung durch, für die Smart FOX (entweder als neu gegründete juristische Person oder ein oder mehrere Smart-FOX-Partner:innen) Daten zur Verfügung stellt. Die Universität bereitet das Protokoll für die Studie vor und nutzt die Dienste von Smart FOX, um Zugriff auf strukturierte, pseudonymisierte Daten zu erhalten. Relativ eindeutig ist hier, dass die Universität die Zwecke und Mittel der Datenverabreitung bestimmt und somit eine Verantwortliche nach Art 4 Abs 7 DSGVO ist. Fraglich ist jedoch, ob Smart FOX als Auftragsverarbeiter agiert oder als gemeinsamer Verantwortlicher. Nach Rechtssprechung des EuGH [44] ist der Begriff des Verantwortlichen recht breit zu interpretieren und kollektive Aktivitäten schnell als gemeinsame Verarbeitung einzustufen, weshalb auch z.B. bei gemeinsamen Aktivitäten im Rahmen von Forschungsprojekten Partner:innen oft als gemeinsame Verantwortliche eingestuft werden. [45] Ausschlaggebend ist jedoch letztendlich die Bestimmung der Zwecke und Mittel der Verarbeitung und wenn, wie derzeit von Partner:innen vorgesehen, Smart FOX diese nicht mitbestimmt, wäre Smart FOX als Auftragsverarbeiter einzustufen. Dies kann analog zu Szenarien gesehen werden, in welchen Sponsor:innen eine klinische Studie durchführen wollen und ein:e Investigator:in die praktische Durchführung übernimmt. Der Europäische Datenschutzausschuss schreibt hier, dass der/die Investigator:in ein:e gemeinsame:r Verantwortliche:r ist, wenn sie/er das Studienprotokoll mitbestimmt. Wenn sie/er jedoch keinen Einfluss auf die Gestaltung der Studie hat (insb. das Protokoll nicht migestaltet), so ist sie/er als Auftragsverarbeiter:in anzusehen.[46]

Die Rolle und damit einhergehenden Verantwortungen von Smart FOX (oder einzelnen Partner:innen) ist also abhängig von der finalen Form von Smart FOX nach Ablauf der Projektphase. Es ist jedoch in der hier beschriebenen Struktur denkbar, dass Smart FOX nicht als gemeinsamer Verantwortlicher, sondern als Auftragsverarbeiter agiert. In jedem Fall ist eine schriftliche Vereinbarung über die Rollen und Verantwortung der involvierten Akteur:innen gem. Art 26 Abs 1 und Art 28 Abs 3 DSGVO notwendig, für welche Smart FOX zur einfacheren Abwicklung entsprechende Vorlagen zur Verfügung stellen könnte. Besonders zu beachten ist, dass für die Festlegung der datenschutzrechtlichen Rollen die Praxis viel relevanter ist als die vertragliche

[44] *Jehovan todistajat (Jehovah's Witnesses) v Finland* – C-25/17 (2018).
[45] *Van Veen/Boeckhout/Schlünder/Boiten/Dias*, Joint controllers in large research consortia: a funnel model to distinguisch controllers in the sense of the GDPR from other partners in the consortium, Open Research Europe 9(2), 2024, 80.
[46] *EDPB*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2020, 20-21.

Vereinbarung. Wenn eine Partei faktisch als Verantwortliche:r agiert, so ist sie die/der Verantwortliche – auch wenn ein Vertrag das Gegenteil festhält.

Zusätzliche Komplexität birgt das Szenario der ungerichteten Datenspende in Smart FOX. Bei der gerichteten Spende werden Zwecke und Mittel der Datenverarbeitung nach derzeitigem Plan von der jeweiligen Studienleitung festgelegt. Bei der ungerichteten Datenspende gibt es zum Zeitpunkt der Einholung der Einwilligung noch keine definierte Studienleitung. Die Rolle von Smart FOX ist also in diesem Fall von der Frage abhängig, ob im Moment der Einholung der Einwilligung bereits die Datenverarbeitung beginnt. Sollte in diesem Moment bereits eine Form der Datenverarbeitung stattfinden, z.B. die Erstellung einer von Smart FOX administrierten FoxBox mit Daten zu einer bestimmten Erkrankung, so passiert dies unter der Verantwortung von Smart FOX (wieder ggfs eine neu gegründete juristische Person oder ein oder mehrere Partner:innen). Smart FOX bestimmt in diesem Fall Zwecke und Mittel der Verarbeitung und ist auch in der Position, die Gewährleistung der Betroffenenrechte zu garantieren. Sollte dies von mehreren Smart FOX Partner:innen durchgeführt werden, so wäre ein Vertrag zur gemeinsamen Verantwortlichkeit notwendig.

Diese letztere Situation wurde in den Smart FOX Learning Clubs besprochen und reflektiert einige der noch offenen Fragen bei der ungerichteten Datenspende. Das Szenario, in welchem Smart FOX gewisse FoxBoxen selber administriert und Datenverarbeitung beginnt, bevor eine Studienleitung einen konkreten Zweck dafür festgelegt hat, entspricht jedoch nicht dem derzeitigen Plan. Zum derzeitigen Zeitpunkt (Jänner 2026) erhebt Smart FOX zwar bereits die Einwilligung zu gewissen Zwecken (broad consent), die Datenverarbeitung beginnt jedoch auch bei der ungerichteten Datenspende erst mit einem konkreten Protokoll und dem Start einer Studie, für welche die Studienleitung die Verantwortung trägt. Es scheint jedoch wahrscheinlich, dass Smart FOX für eine gewisse Datensammlung, etwa für Metadaten über den Inhalt existierender FoxBoxen, die Mittel und Zwecke der Verarbeitung definiert. Für die abschließende Klärung dieser Strukturen in einem zukünftigen AHDDS muss die endgültige Rechtsform der Datenspende und der Prozess für die ungerichtete Datenspende feststehen.

4.1.3. Urheberrecht

Auch aus urheberrechtlicher Perspektive ist die Frage des „Eigentums“ aus unterschiedlichen Perspektiven zu untersuchen – je nachdem, ob es sich bei den zu spendenden Gesundheitsdaten um reine Tatsachen, ausformulierte Gutachten oder z.B. Röntgenbilder handelt, kommt die Anwendung von urheberrechtlichen Rechtsvorschriften in Frage.

Nach § 1 des österreichischen Urheberrechtsgesetzes (UrhG) besteht an Werken der Literatur (dazu zählen auch Computerprogramme, nicht aber Rohdaten), der Tonkunst, der bildenden Künste und der Filmkunst, die eigentümlich (also individuell, originell und persönlich geprägt) sind, **Urheberrechtsschutz** zugunsten der Urheber:innen.[47] Es besteht außerdem die Möglichkeit der gemeinschaftlichen Miturheber:innenschaft, wenn mehrere natürliche Personen gemeinsam ein einheitliches, untrennbares Werk geschafften haben (§ 11 UrhG).

Zu beachten ist, dass wegen des **Schöpfungsprinzips im Urheberrecht** nur natürliche Personen Urheber:innen sein können, im Rahmen einer Krankenbehandlung also beispielsweise Ärzt:innen oder Krankenpflegerinnen, sofern sie ein Werk schaffen. Dienstgeber:innen und Auftraggeber:innen können nur Werknutzungsrechte oder -bewilligungen ableiten, nicht aber selbst die Urheber:innenstellung erlangen – der Oberste Gerichtshof (OGH) geht in der Entscheidung OGH 4 Ob 226/19t sogar vom möglichen konkludenten, also nicht expliziten Einräumen der Werknutzungsrechte aus. Dies gilt auch für Werkschöpfungen im Rahmen eines Auftrags, einer Bestellung oder eines Werkvertrags (z.B. die Anfertigung von Röntgenbildern oder medizinischen Gutachten).[48]

Das Urheberrecht räumt den Urheber:innen das allein ihnen zustehende Recht ein, ein Werk gem. § 15 bis 18c UrhG zu **verwerten** (§ 14 Abs 1 UrhG) – dazu zählen unter anderem die Bearbeitung (§ 14 Abs 2 UrhG), Vervielfältigung (§ 15 UrhG), Verbreitung (§ 16 UrhG) oder Vorführung (§ 18) UrhG) des Werks. Dieses Urheberrecht besteht für 70 Jahre nach dem Tod der Urheberin (§ 60 UrhG) und ist nicht übertragbar, außer im Erbfall (§ 23 Abs 1 und Abs 3 UrhG).

4.1.3.1. Urheberrecht an Resultaten von Krankenbehandlungen

Rohe erhobene/gesammelte **Gesundheitsdaten** stellen keine Schöpfung im Sinne des Urheberrechts dar, sind also nicht als Werke der Literatur, der Tonkunst, der bildenden Künste oder der Filmkunst urheberrechtlich geschützt. **Gesundheitsdatenbanken** hingegen können als Datenbankwerke urheberrechtlichen Schutz genießen, sofern sie systematisch geordnet und Sammlungen von Werken, Daten oder anderen unabhängigen Elementen gem. § 6 UrhG sind. Voraussetzung ist, dass es sich beim Datenbankwerk aufgrund der Auswahl und/oder Anordnung um eine eigentümliche

[47] Kucsko in Handig/Hofmarcher/Kucsko, urheber.recht[3] § 1 UrhG (Stand 1.8.2023, rdb.at).
[48] Kusznier in Handig/Hofmarcher/Kucsko, urheber.recht[3] § 10 UrhG (Stand 1.8.2023, rdb.at).

geistige Schöpfung handelt; die Struktur des Werks ist Gegenstand des urheberrechtlichen Schutzes.[49]

Medizinische Befunde qualifizieren sich – sofern es sich um reine Tatsachenberichte handelt, die nicht kommentiert werden – nicht als Sprachwerke, denen urheberrechtlicher Schutz zusteht. Sachverständigen-Gutachten sowie wissenschaftliche Texte genießen allerdings in der Regel als geistige eigentümliche Sprachwerke Urheberrechtsschutz.

Patient:innenbilder, die im Zuge einer Behandlung in einer Krankenanstalt hergestellt werden, können unter Umständen Lichtbildwerke darstellen und somit urheberrechtlich geschützt sein – dafür muss sogenannte reduzierte Originalität vorliegen, also Unterscheidbarkeit des Bildes ohne besondere Originalität oder Individualität:

Das UrhG unterscheidet zwischen Lichtbildwerken und Lichtbildern. **Lichtbildwerke** werden durch fotographische oder ähnliche Verfahren hergestellt und weisen die Persönlichkeit der Urheber:innen anhand der Gestaltung auf, die eine Unterscheidbarkeit ausdrückt(§ 3 UrhG). An Lichtbildwerken also bestehen der umfassende Urheberrechtsschutz und somit auch die absoluten Verwertungsrechte, die bereits angeführt wurden (siehe oben). Hingegen ist ein **Lichtbild** eine „mit technischen Mitteln bewirkte, bildliche Festlegung eines Ausschnitts der Außenwelt“[50], das keine eigentümliche geistige Schöpfung darstellen muss und mittels eines fotographischen (oder diesem ähnlichen Verfahren) hergestellt wurde (vgl. § 73 UrhG). Die Aufnahme geschieht im Interesse der detaillierten Dokumentation und „einwandfreien Wiedergabe“[51] des Motivs“.[52] [53] Als Lichtbilder sind auch Röntgen-, Ultraschall- oder MRT-Bilder zu qualifizieren.[54] Den Hersteller:innen eines Lichtbildes kommen die Leistungsschutzrechte nach § 74 UrhG zu, u.a. das ausschließliche Recht auf Vervielfältigung, Verbreitung, Vorführen und Veröffentlichung, die geringere Schutzvoraussetzungen und -umfang als der Urheberrechtsschutz aufweisen[55]. Die Rechte der Lichtbildhersteller:innen sind veräußerlich (§ 74 Abs 2), können also übertragen werden. Die Schutzdauer beträgt 50 Jahre nach Tod oder Veröffentlichung (§ 74 Abs 6 UrhG) und kann natürlichen und juristischen Personen zukommen. Gem. § 74 Abs 1 S 2 UrhG gelten nämlich bei

[49] Zemann in Dokalik/Zemann, Urheberrecht8 § 40f UrhG (Stand 1.10.2022, rdb.at)
[50] Tonninger in Handig/Hofmarcher/Kucsko, urheber.recht[3] § 73 UrhG Rz 5 (Stand 1.8.2023, rdb.at).
[51] Helene Herda, Die Verwendung von Patientenbildern durch die Krankenanstalt: Zustimmungserfordernis für Patienten?, RdM 2024/27.
[52] OGH 4 Ob 226/19z.
[53] Tonninger in Handig/Hofmarcher/Kucsko, urheber.recht[3] § 3 UrhG Rz 13 (Stand 1.8.2023, rdb.at).
[54] Christian Handig, Fotomotiv- Schutz oder Freiheit?, ipCompetence 2011 H 6, 54.
[55] Helene Herda, Die Verwendung von Patientenbildern durch die Krankenanstalt: Zustimmungserfordernis für Patienten?, RdM 2024/27.

gewerbsmäßig von unselbstständigen Beschäftigten hergestellten Lichtbildern die Unternehmensinhabenden als Hersteller:innen – somit kommt bei Lichtbildern der Leistungsschutzrecht nicht etwa Ärzt:innen oder Krankenpfleger:innen, sondern der Krankenanstaltenträgerin zu.

Während ein Lichtbild kein Lichtbildwerk darstellt, ist jedes Lichtbildwerk automatisch ein Lichtbild. Dadurch werden Lichtbildwerke durch den Urheberrechtsschutz sowie durch die Leistungsschutzrechte geschützt – wie im Fall von gegensätzlichen Regelungen vorzugehen ist, hat der OGH in der Entscheidung OGH 4 Ob 226/19z offengelassen.

4.1.3.2. Urheberrechtlicher Schutz der ELGA

Abschließend ist hinsichtlich der Sekundärnutzung von Gesundheitsdaten zu sagen, dass diese singulär als rein faktische Informationen nicht urheberrechtlich geschützt sind. Allerdings kann hinsichtlich der Sammlung von Gesundheitsdaten im Rahmen der ELGA urheberrechtlicher Schutz bestehen, sofern es sich dabei um ein Datenbankwerk handelt. Nach § 40f UrhG können **Datenbanken** als Sammel-/Datenbankwerke von Gesundheitsdaten urheberrechtlich geschützt sein. Dazu ist notwendig, dass aufgrund der Auswahl, Sortierung, Systematisierung und Struktur der Daten Eigentümlichkeit einer geistigen Schöpfung besteht. Eine solche Eigentümlichkeit ist nicht durch allumfassende, vollständige Sammlungen gegeben. Computerprogramme zählen nicht zu Datenbankwerken, können aber separat Urheberrechtsschutz genießen (§ 40a UrhG). Die Inhalte der Datenbanken werden in ihren Rechten durch ihre Zugehörigkeit zu einer Datenbank nicht berührt (Art 3 Abs 2 DatenbankRL).[56]

Wenn man von **weitgehendem Urheberrechtsschutz** ausgeht, kann argumentiert werden, dass zwar einerseits keine Selektion der erfassten Daten nach bestimmten Kriterien (außer den erfüllten Voraussetzungen des § 15 GTelG 2012, nämlich im Patientenindex erfasste natürliche Personen, die nicht von der Opt-Out-Option bezüglich der Teilnahme an ELGA Gebrauch gemacht haben), andererseits aber aufgrund der besonderen Struktur und der dahinterstehenden umfassenden Systematik und Sortierung der Sammlung. Diese Einschätzung bedeutet dementsprechend, dass an dem Datenbankwerk der ELGA-Daten als Sammelwerk gem. § 40f sowie § 6 UrhG ein Urheberrecht besteht, also die Verwertungsrechte gemäß dem III. Abschnitt UrhG der Urheberin vorbehalten sind.

[56] Woller in Handig/Hofmarcher/Kucsko, urheber.recht[3] § 40f UrhG (Stand 1.8.2023, rdb.at).

Bei der Beurteilung der eigentümlichen, geistigen Schöpfung der ELGA-Daten als Sammelwerk ist allerdings zu beachten, dass ELGA-Gesundheitsdaten iSd § 2 Z 9 lit a und lit b GTelG 2012 gem. § 16 Abs 1 ELGA-VO nach vom Bundesministerium für Gesundheit zu veröffentlichenden Implementierungsleitfäden in Inhalt, Struktur, Format und Codierung dargestellt werden. Im Fall einer **engeren Betrachtung des Urheberschutzes** ist also festzuhalten, dass weder hinsichtlich der Auswahl der enthaltenen Daten noch hinsichtlich der Struktur eine eigentümliche oder geistige Schöpfung vorliegt, somit auch kein Urheberrechtsschutz für die gesammelten ELGA-Daten besteht. Dieser Meinung folgend ist aus Perspektive des Urheberrechts problemlos die Verwertung der Datensammlung möglich, da diese Verwertungsrechte des III. Abschnitt UrhG nicht einer Urheberin vorbehalten sind.

4.1.4. Weitere EU-Rechtsgrundlagen

Neben der bisher geschilderten Rechtslage (datenschutzrechtliche und urheberrechtliche Erwägungen) spielen kürzliche europäische Entwicklungen (Rechtsakte im Bereich der Daten und Digitalisierung, welche nicht eindeutig dem einen oder anderen Bereich zuordenbar sind) eine immer wichtigere Rolle bei der Gestaltung der Nutzung von Gesundheitsdaten. Die **Europäische Datenstrategie** ist eine treibende Kraft hinter der Schaffung eines EU-weiten Datenbinnenmarkts, der auf eine bessere Nutzung und Verfügbarkeit von Daten abzielt. Ziel dieser Strategie ist es, eine datenbasierte Wirtschaft zu fördern, die sowohl der europäischen Gesellschaft als auch der Wirtschaft zugutekommt.[57]

Zentrale Elemente der europäischen Datenstrategie sind der **DA, die Open Data-Richtlinie** und der **DGA**. Der DA zielt darauf ab, Hindernisse für den Zugang zu Daten zu beseitigen und ihre gemeinsame Nutzung zu erleichtern, wobei der Schutz sensibler Daten, wie Gesundheitsdaten, weiterhin gewährleistet bleiben soll. Die Open Data-Richtlinie fördert die Veröffentlichung der Daten von öffentlichen Einrichtungen und kann daher natürlich auch Gesundheitsdaten betreffen. Der DGA schafft einen rechtlichen Rahmen für die Datenverwaltung in der EU und fördert die freiwillige Bereitstellung von Daten für gemeinwohlorientierte Zwecke.

4.1.4.1. Data Act

Die Datenverordnung (Verordnung (EU) 2023/2854), auch Data Act und abgekürzt DA genannt, die am 12. September 2025 in Kraft trat, schafft rechtliche Klarheit hinsichtlich des Zugriffs auf Daten und deren Nutzung und zielt darauf ab, die Zugänglichkeit, Nutzbarkeit und Verfügbarkeit von Daten

[57] https://digital-strategy.ec.europa.eu/en/policies/digital-decade-policy-programme.

zu erhöhen, um Innovationen zu fördern. Im Zusammenhang mit Gesundheitsdaten, insbesondere jenen, die in der ELGA gespeichert sind, wird der DA weitreichende Auswirkungen auf die Art und Weise haben, wie diese Gesundheitsdaten verwendet und geteilt werden können.

Ein zentraler Aspekt des DA ist die **Stärkung der Kontrolle über generierte Daten für Nutzende und Unternehmen**. Im Kontext des Internet of Things (IoT), das als Netzwerk vernetzter Produkte verstanden wird, könnten Gesundheitsdaten zunehmend aus verschiedenen Quellen stammen, die nicht nur klinische, sondern auch alltagsbezogene Gesundheitsinformationen umfassen. Der DA legt Maßnahmen fest, die sicherstellen sollen, dass die Datenkontrolle bei denjenigen verbleibt, die die Daten generieren, und soll den Missbrauch markbeherrschender Stellungen durch Unternehmen verhindern. Dies ist besonders wichtig, um eine faire Nutzung von Gesundheitsdaten zu gewährleisten und zu verhindern, dass bestimmte Akteur:innen bevorzugten Zugang zu diesen Daten erhalten.

Ein weiterer Schutzmechanismus, den der DA beinhaltet, betrifft den **Zugriff auf nicht-personenbezogene Daten durch Drittländer-Regierungen**. Dies ist besonders relevant im globalisierten Gesundheitssektor, wo die Kontrolle über Daten auch eine Frage der nationalen und wirtschaftlichen Sicherheit darstellt. Beispielsweise dürfen Daten nur dann an Drittländer übermittelt werden, wenn diese Länder ein angemessenes Schutzniveau garantieren und eine Überprüfung durch ein unabhängiges Gericht vorsehen. Dieser Mechanismus soll sicherstellen, dass EU-Unternehmen vor unberechtigten Zugriffen und potenzieller Industriespionage geschützt sind.[58]

Der DA fördert die **Interoperabilität** sowohl zwischen verschiedenen Sektoren als auch zwischen den Mitgliedstaaten der EU. Für die Gesundheitsdaten in ELGA bedeutet dies, dass eine effektivere und sichere sektorenübergreifende Nutzung möglich wird, die sowohl den Patienten als auch dem Gesundheitssystem zugutekommt. Durch standardisierte Formate und Protokolle können Gesundheitsdaten einfacher zwischen verschiedenen Akteuren, wie Krankenhäusern, Forschungseinrichtungen und staatlichen Stellen, ausgetauscht werden. Dies kann nicht nur die Qualität der medizinischen Versorgung verbessern, sondern auch die Effizienz und Innovationskraft im Gesundheitswesen steigern. [59] [60]

Ein bedeutender Aspekt des DA ist die Möglichkeit für öffentliche Stellen, Daten von Unternehmen anzufordern, wenn ein außergewöhnlicher Bedarf am Zugang zu diesen Daten besteht, wie es in

[58] https://europeanlawblog.eu/2022/06/14/the-data-act-or-the-final-piece-to-create-a-comprehensive-legal-framework-for-international-transfers-of-data/.
[59] https://digitalisierungsrecht.eu/interoperabilitaet-im-data-act/.
[60] https://digital-strategy.ec.europa.eu/de/policies/data-act.

Kapitel V des DA geregelt ist. Diese Regelung sieht vor, dass eine **Datenanforderung im öffentlichen Interesse** liegen muss, etwa zur Bewältigung von Gesundheitskrisen oder zur Erfüllung spezifischer rechtlicher Aufgaben. Laut Art 14 DA muss dabei nachgewiesen werden, dass eine außergewöhnliche Notwendigkeit besteht. Diese außergewöhnliche Notwendigkeit ist jedoch zeitlich befristet und darf nur unter bestimmten Bedingungen, wie in Art 15 beschrieben, geltend gemacht werden. Darüber hinaus regelt Art 21 DA die Weitergabe der angeforderten Daten und stellt sicher, dass diese nur für gemeinnützige Zwecke oder zur Erfüllung öffentlicher Aufgaben genutzt werden und nicht von gewerblichen Unternehmen beeinflusst werden dürfen, um eine faire und unvoreingenommene Nutzung der Forschungsergebnisse zu gewährleisten.

Der DA sieht zudem vor, dass Dateninhabende, insbesondere Kleinst- und Kleinunternehmen, eine **Gegenleistung für die Bereitstellung von Daten** erhalten können. Dies schließt auch die Kosten für organisatorische und technische Maßnahmen wie Anonymisierung, Pseudonymisierung und Datenaggregation ein. Damit sollen kleinere Akteure in die Lage versetzt werden, am Datenökosystem teilzuhaben, ohne unverhältnismäßig belastet zu werden.

Außerdem stärkt der DA die **Datenportabilität**, indem er klare Regeln für den Datentransfer zwischen verschiedenen Diensten und Plattformen festlegt. Dies erleichtert den Wechsel von Dienstanbietenden zu anderen – insbesondere in Bereichen wie Cloud-Diensten und IoT-Systemen. Die Portabilität von Daten ist entscheidend für die Förderung von Wettbewerb und Innovation, da sie es den Nutzenden ermöglicht, ihre Daten in einem strukturierten, gängigen und maschinenlesbaren Format mitzunehmen und an andere Anbietende zu übertragen. Diese Regelungen sollen verhindern, dass Daten durch Lock-in-Effekte bei Anbietenden festgehalten werden, was sowohl den Verbraucherschutz als auch die Marktdynamik stärkt.

Im Kontext der Gesundheitsdaten bedeutet dies, dass Patient:innen leichter zwischen verschiedenen Gesundheitsdiensten wechseln können, ohne den Zugriff auf ihre historischen Gesundheitsdaten zu verlieren. Dies kann insbesondere die Entwicklung von personalisierten Gesundheitsdiensten fördern, da die nahtlose Übertragung von Daten über verschiedene Plattformen hinweg die Nutzung und Analyse dieser Daten für innovative Anwendungen ermöglicht. Zudem verpflichtet der DA die Anbietenden, klare und transparente Bedingungen für die Datenportabilität zu schaffen und sicherzustellen, dass die Nutzenden nicht durch hohe Wechselkosten oder technische Barrieren daran gehindert werden, ihre Daten mitzunehmen.

Die Umsetzung dieser Portabilitätsregelungen soll durch die Einführung gemeinsamer technischer Standards und Spezifikationen erleichtert werden, um die Interoperabilität zwischen verschiedenen

Diensten und Plattformen zu gewährleisten. Diese Standards werden von der Europäischen Kommission in Zusammenarbeit mit den entsprechenden europäischen Normungsorganisationen entwickelt und sind entscheidend, um eine breite Akzeptanz und Anwendung der Portabilitätsanforderungen zu gewährleisten.

4.1.4.2. Open Data-Richtlinie[61]

Die Richtlinie (EU) 2019/1024 des europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors, auch bekannt als die Open Data-Richtlinie, spielt eine entscheidende Rolle bei der Regulierung der **Weiterverwendung öffentlich verfügbarer Informationen**, die im Besitz des öffentlichen Sektors sind. Diese Richtlinie zielt darauf ab, den Zugang zu und die Nutzung von öffentlichen Daten zu erleichtern, um die Transparenz zu erhöhen und die Innovation in der EU zu fördern.

In Bezug auf Public Service Data bedeutet dies, dass alle Daten, die von öffentlichen Einrichtungen bereitgestellt werden, **grundsätzlich offen und zugänglich** sein sollten, sofern keine spezifischen Einschränkungen bestehen, wie z. B. Datenschutzbestimmungen oder Fragen der nationalen Sicherheit. Dies betrifft auch Gesundheitsdaten, die von öffentlichen Gesundheitseinrichtungen generiert oder verwaltet werden. Diese Daten können somit unter den Bedingungen der Richtlinie für Forschung, Innovation und andere gemeinnützige Zwecke weiterverwendet werden.

Durch die Open Data-Richtlinie wird auch die **Interoperabilität und Vergleichbarkeit** von öffentlichen Daten gestärkt, was es ermöglicht, diese Daten über nationale Grenzen hinweg zu nutzen. Dies ist besonders relevant für die Entwicklung grenzüberschreitender Gesundheitsdienste und die Förderung von Forschungsprojekten, die auf europäischer Ebene durchgeführt werden. Die Richtlinie trägt somit ebenso dazu bei, einen gemeinsamen europäischen Datenraum zu schaffen, der Innovationen in verschiedenen Sektoren, einschließlich des Gesundheitswesens, fördert.

4.1.4.3. Data Governance Act

Der Data Governance Act (Verordnung (EU) 2022/868, kurz DGA), der seit Juni 2021 in Kraft ist und seit September 2023 vollständig anwendbar ist, zielt darauf ab, die Nutzung und Wiederverwendung von Daten in der EU zu fördern, insbesondere Daten aus öffentlicher Hand und geschützten Daten, die nicht unter die Open-Data-Richtlinie fallen. Somit legt der DGA einen **regulatorischen Rahmen**

[61] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L1024.

für den Sekundärnutzung von öffentlichen Daten in der EU, auf den sektorspezifische Gesetze, wie die Verordnung zum EHDS, aufbauen.

Der DGA ist eine Verordnung, was bedeutet, dass Nationalstaaten das Gesetz nicht erst in nationales Recht umsetzen müssen, sondern der DGA sofortige Rechtsgültigkeit hat. Die Hauptziele des DGAs sind gem. Art 1 Abs 1 DGA:

- die Nutzung von Daten zu ermöglichen, die in öffentlicher Hand sind;
- die Aktivitäten sogenannter Daten-Vermittlungsdienste zu regeln, die den Datenaustausch zwischen verschiedenen Akteuren unterstützen;
- das Konzept des Datenaltruismus zu etablieren, um freiwilligen Datenaustausch zu fördern.

Ein zentrales Anliegen des DGA ist es, den Zugang zu Daten aus öffentlichen Stellen zu ermöglichen, insbesondere in Bereichen, in denen sensible Daten aus Gründen wie geschäftlicher und statistischer Geheimhaltung, Schutz geistigen Eigentums oder personenbezogener Daten besonders geschützt sind (Art 3 Abs 1 DGA). Der DGA legt klare Regeln und Sicherheitsmechanismen fest, um den Schutz von personenbezogenen und vertraulichen Daten zu gewährleisten. Nach Art 3 DGA bestehen für die Herausgabe von öffentlichen Daten je nach Datentyp differenzierte Bedingungen. So müssen öffentliche Stellen etwa Anonymisierungs- und Pseudonymisierungstechniken sowie sichere Zugriffsmethoden einsetzen, um den Schutz der Privatsphäre zu wahren. Die Weiterverwendung solcher Daten kann jedoch nur mit der ausdrücklichen Zustimmung der betroffenen Personen oder Dateninhabenden erfolgen, wobei die strengen Vorgaben der DSGVO einzuhalten sind.

Um diese Bedingungen zu erfüllen, soll jeder EU-Mitgliedstaat laut Art 7 DGA zuständige Stellen zu bestimmen, die insbesondere bei technischen Fragen hinsichtlich der Datenweitergabe und bei der Einholung von Einverständniserklärungen unterstützen sollen. Grundsätzlich müssen die Bedingungen der Datenweitergabe nichtdiskriminierend, transparent und verhältnismäßig sein (Art 4 Abs 2 DGA).

Für die Herausgabe von Daten aus öffentlicher Hand gilt laut Art 4 DGA ein Verbot von Ausschließlichkeitsvereinbarungen, durch die die Daten nur für einen oder einige wenige Akteur:innen verfügbar sind. Dieses sollen verhindern, dass einzelne Unternehmen exklusiven Zugriff auf bestimmte Datensätze erhalten, um eine breitere Verfügbarkeit der Daten zu fördern und so Innovationen und die gemeinnützige Forschung zu unterstützen. Dieses Verbot gilt nicht, wenn die Vereinbarung dem allgemeinen Interesse dient (Art 4 Abs 2 DGA). Ein ausschließliches Recht auf Datenweiterverwendung muss „im Einklang mit den Grundsätzen der Transparenz, der

Gleichbehandlung und der Nichtdiskriminierung“ sein und kann für maximal zwölf Monate gewährt werden (Art 4 Abs 3 DGA). Öffentliche Stellen können Gebühren für die Erlaubnis zur Datenweiterverwendung erheben: Diese müssen ebenfalls transparent, nichtdiskriminierend und verhältnismäßig sein (Art 5 Abs 1 und 2 DGA). Laut Art 9 Abs 1 DGA müssen Entscheidungen über Anträge auf Datenweiterverwendung innerhalb von zwei Monaten getroffen werden. Diese können jedoch um bis zu 30 Tage verlängert werden (Art 9 Abs 1 DGA). Die Antragsteller:innen haben das Recht auf einen wirksamen Rechtsbehelf bei Ablehnung (Art 9 Abs 2 DGA).

Öffentliche Stellen dürfen zudem **angemessene Gebühren für den Zugang** zu den Daten erheben, wobei diese Gebühren für wissenschaftliche oder nichtkommerzielle Zwecke reduziert oder ganz entfallen können. Eine zentrale Informationsstelle soll potenzielle Datenwiederverwendende über verfügbare Datensätze informieren.

Der DGA regelt auch die Rolle sogenannter **Datenvermittlungsdienste**. Datenvermittlungsdienste werde als neutrale Akteure beschrieben, die zwischen Dateninhabenden und potenziellen Datennutzenden vermitteln und technische, rechtliche oder sonstigen Dienste bereitstellen, um den Datenaustausch zu ermöglichen.[62] Diese Akteure unterstützen den Datenaustausch zwischen Dateninhabenden und Datennutzenden, ohne selbst die Daten zu monetarisieren. Es gibt verschiedene Arten von Datenvermittlungsdiensten nach Art 2 Abs 15 DGA:

- Dienste, die personenbezogenen Daten von Betroffenen an mögliche Datennutzernde vermitteln;
- Dienste, die Daten zwischen Dateninhabenden, wie öffentlichen Stellen, Forschungseinrichtungen oder Unternehmen, und möglichen Datennutzende ermöglichen; und
- Datengenossenschaften, „deren Hauptzwecke in der Unterstützung ihrer Mitglieder bei der Ausübung ihrer Rechte in Bezug auf bestimmte Daten bestehen“.

Diese Datenvermittlungsdienste müssen strenge **Anforderungen** erfüllen, darunter die Verpflichtung, den Datenaustausch zu fördern, ohne dabei selbst wirtschaftliche Vorteile aus den Daten zu ziehen (Art 11 und 12 DGA). Zunächst muss ein Datenvermittlungsdienst nach dem in Art 11 DGA erläuterten Prozess bei den zuständigen Behörden angemeldet werden. Außerdem müssen sich die Dienste laut Art 11 Abs 1 DGG auf den Datenaustausch beschränken. Der Datenvermittlungsdienst darf die Daten selbst also nicht monetisieren, zum Beispiel durch Analyse

[62] *Carovano/Finck*, Regulating data intermediaries: The impact of the Data Governance Act on the EU’s data economy, Computer Law & Security Review 50, 105830.

der Daten und Bereitstellung von Meta-Daten.[63] Eine Pseudonymisierung oder Anonymisierung oder eine sonstige Aufarbeitung der Daten, die dem Datenaustausch zwischen den Akteur:innen dienen, sind allerdings Services, die im Rahmen des Datenvermittlungsdienst erlaubt sind.[64] Wenn der Datenvermittlungsdienst zwischen Privatpersonen, die ihre personenbezogenen Daten weitergeben möchten, und Datennutzenden vermittelt, hat der Datenvermittlungsdienst besondere Pflichten gegenüber der Privatperson (Art 12 lit m DGA). Er informiert und berät die Betroffenen hinsichtlich der Datenweitergabe und handelt dabei im besten Interesse der Person. Eine ausführliche Analyse hinsichtlich der Frage, ob Smart FOX als Datenvermittlungsdienst gelten kann, findet sich in Kapitel 8.3.

Zentral ist auch das Konzept des Datenaltruismus, bei dem Einzelpersonen und Organisationen freiwillig ihre Daten für gesellschaftlich relevante Zwecke bereitstellen. Dies wird besonders im Gesundheitssektor relevant, wo Datenaltruismus eine entscheidende Rolle dabei spielen kann, Forschenden den Zugang zu umfangreichen Datensätzen zu ermöglichen, um neue medizinische Erkenntnisse zu gewinnen. Gleichzeitig müssen jedoch die Rechte und Interessen der Dateninhabenden geschützt werden, um sicherzustellen, dass der Datenaustausch sicher und transparent erfolgt. Eine ausführliche Analyse hinsichtlich des Datenaltruismus findet sich allerdings in Kapitel 5.3.

Der DGA bietet somit einen umfassenden Rahmen für den sicheren und geregelten Austausch von Daten, insbesondere in Bereichen, die strengen rechtlichen und datenschutzrechtlichen Anforderungen unterliegen.

[63] *Micheli et al*, Mapping the landscape of data intermediaries, 24.08.2023.
[64] Ibid.

4.2. Wie werden Datenspendende geschützt?

Datenspendende werden auf verschiedene Weisen geschützt. Dabei müssen Grundrechte, Persönlichkeitsrechte sowie Betroffenenrechte bedacht werden.

4.2.1. Grundrechte

Datenschutz ist nicht nur Gegenstand von einfachen Gesetzen, sondern ebenfalls durch Grundrechte geschützt. Der Begriff der Menschen- oder Grundrechte hat in Österreich keine lange rechtshistorische Tradition, sondern erst in jüngerer Zeit, insbesondere durch den Beitritt in die EU, Eingang in die nationale Rechtsordnung gefunden.[65] Die GRC trat 2009 mit dem Vertrag von Lissabon in Kraft. Die Mitgliedsstaaten sind verpflichtet, die Charta zu befolgen, wenn sie EU-Recht anwenden – wie beispielsweise die DSGVO.[66] Relevant für die Verarbeitung von Daten zum Zwecke einer Datenspende sind Art 7 und Art 8 der GRC.

Art 7 GRC schützt das **Recht auf Achtung des Privat- und Familienlebens, der Wohnung und des Briefverkehrs**. Dieser Artikel verkörpert die klassische Idee des Privatsphärenschutz als Abwehrrecht gegen den Staat. Art 7 GRC schützt Gesundheitsdaten, da diese in der Regel geeignet sind, tiefe Einblicke in das private Leben einer Person zu geben. Die Rechtsvorschrift wurde wortgleich von Art 8 EMRK übernommen, die als Inspiration für die GRC gilt.[67] Da die Mitgliedsstaaten der EU ebenfalls Mitglieder der EMRK sind, ist in Österreich ebenfalls die EMRK anwendbar – es besteht somit eine zweifache Schutzregelung, die allerdings als Teil verschiedenen Institutionen und somit auch Anwendungsbereichen und Rechtsdurchsetzungswegen bestehen. In Österreich steht die EMRK seit 1964 im Verfassungsrang, wodurch die in der EMRK festgelegten Rechte unmittelbar von Behörden und Gerichten in Österreich angewendet und vor ihnen durchgesetzt werden .

Neben Art 7 GRC besteht auch noch Art 8 GRC, der ein **Recht auf Datenschutz** explizit als Grundrecht in der GRC verankert. Art 8 GRC schützt alle personenbezogenen Daten und hat somit einen weiteren Schutzbereich als Art 7 GRC, in den auch Daten fallen, die klassisch nicht als privat angesehen werden. Ebenfalls genannt werden in Art 8 Abs 2 GRC die Grundsätze, bei deren Einhaltung eine Verarbeitung rechtmäßig ist, nämlich auf Grundlage einer Einwilligung oder einer sonstigen rechtlichen Grundlage. Art 8 GRC besitzt ebenso wie Art 7 GRC einen Zwilling, nämlich in

[65] *Berka/Binder/Kneihs*, Die Grundrechte: Grund- und Menschenrechte in Österreich: Handbuch[2.] (2019) 8.
[66] *European Union Agency of Fundamental Rights*, Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level: guidance (2020).
[67] Berka, 391.

Art 16 Abs 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der ebenfalls das Grundrecht auf Datenschutz sichert. Auch § 1 DSG auf österreichischer Ebene sichert jedermann das Recht auf Schutz seiner personenbezogenen Daten zu. Auch diese Bestimmung hat Verfassungsrang.

Zusammenfassend ergänzen sich die verschiedenen Rechtsquellen, die gemeinsam das Ziel haben zu begrenzen, wie (sensible) Informationen verwendet werden können. Die **Durchsetzung des Rechts auf Datenschutz** konkretisiert insbesondere Art 8 GRC in Abs 3, der festlegt, dass „unabhängige Stellen" die Überwachung seiner Einhaltung übernehmen sollen. In der Praxis ist diese Stelle also die österreichische Datenschutzbehörde, die für die Wahrung der Grundrechte von Betroffenen Verantwortung trägt und an die sich Einzelne bei Verstößen wenden können.[68]

4.2.2. Persönlichkeitsschutz

Gem. § 15 ABGB können **Personenrechte** einerseits für jedermann aufgrund bestimmter Eigenschaften und Verhältnisse (damit sind vor allem §§ 16 bis 43 ABGB gemeint) und andererseits durch Familienverhältnisse (hinsichtlich Smart FOX sind vor allem die Obsorgerechte von Interesse) begründet werden.[69]

In § 16 ABGB wird festgelegt, dass die **Persönlichkeit des Menschen** einen Grundwert darstellt. Diese Persönlichkeit wird durch absolute Persönlichkeitsrechte geschützt, die gegenüber allen gelten. Insbesondere geht es um die Wahrung der Menschenwürde im sozialen Umfeld des Menschens.[70] Nach § 16 sind Menschen als natürliche Personen geschützt, die angeborenen Rechte fallen ihnen ab der vollendeten Geburt zu (Rechtsfähigkeit, die auch die Parteifähigkeit, also die Möglichkeit zu klagen bzw. geklagt zu werden, bedeutet). Als Kernbereich der Persönlichkeit gilt u.a. die Privatsphäre, die die gesundheitliche Situation erfasst – ein Eingriff in "diesen intimsten Lebensbereich" [71] indiziert bereits die Rechtswidrigkeit des Verhaltens, da die offensichtliche unmittelbare Nähe zur Persönlichkeit Enthaltungspflichten begründet, die jedermann verpflichten.[72] Im höchstpersönlichen Lebensbereich, der die Gesundheit, das Familienleben, das Sexualleben, die Religion und den Umgang mit Nahestehenden umfasst, kann ein Eingriff nicht durch eine Interessenabwägung gerechtfertigt werden.[73]

[68] *Berka/Binder/Kneihs*, Die Grundrechte, 401.
[69] Schauer in Kletečka/Schauer, ABGB-ON[1.02] § 15 (Stand 1.3.2017, rdb.at).
[70] Aicher in Rummel/Lukas, ABGB[4] § 16, RZ 8 (Stand 1.7.2015, rdb.at).
[71] Aicher in Rummel/Lukas, ABGB[4] § 16, RZ 9 (Stand 1.7.2015, rdb.at).
[72] Aicher in Rummel/Lukas, ABGB[4] § 16, RZ 9 (Stand 1.7.2015, rdb.at).
[73] Aicher in Rummel/Lukas, ABGB[4] § 16, RZ 14 (Stand 1.7.2015, rdb.at).

Aus dem § 16 ABGB können verschiedene Rechte abgeleitet werden – für das Forschungsprojekt Smart FOX kann das Recht auf Wahrung der Geheimsphäre von Relevanz sein.

4.2.2.1. Das Recht auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung ist ein Rechtsbegriff, der ursprünglich aus dem deutschen Verfassungsrecht stammt. 1983 leitete das Deutsche Bundesverfassungsgericht (dBVerfG) das Recht von Art 2 Abs 1 des deutschen Grundgesetzes (dGG) (allgemeines Persönlichkeitsrecht) in Verbindung mit Art 1 Abs 1 dGG (Menschenwürde) ab. Hintergrund war ein im März 1982 durch den Deutschen Bundestag verabschiedetes Volkszählungsgesetz, durch das eine umfassende Datenerhebung mit mehr als 160 Fragen zu den Lebens- und Arbeitsverhältnissen der Bürger:innen ermöglicht wurde.[74] Es folgten Proteste innerhalb der Bevölkerung, die staatliche Überwachung fürchtete.[75] Das dBVerG beschäftigte sich folglich 1983 mit dem Volkszählungsgesetz und befand das Ziel des Gesetzes für rechtskonform. Aufgrund fehlender organisatorischer und verfahrensrechtlicher Garantien zum Schutz der Rechte der Bürger:innen erklärte das dBVerfG das Gesetz allerdings für verfassungswidrig.

Im Zuge seiner Argumentation rechtfertigt das dBVerfG erstmals eine neue Ausprägung des allgemeinen Persönlichkeitsrechts in Form des Rechts auf informationelle Selbstbestimmung. Das allgemeine Persönlichkeitsrecht, so der Gerichtshof, schützt den „Wert und die Würde der Person, die in freier Selbstbestimmung als Mitglied einer freien Gesellschaft wirkt".[76] Dieses Recht umfasst den „Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten". [77] Denn „[w]er nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner:innen nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden". [78] Das Recht auf informationelle Selbstbestimmung gibt den Einzelnen grundsätzlich die Befugnis, über die Preisgabe und Verwendung ihrer persönlichen Daten zu verfügen. Der Schutz der Offenheit der individuellen

[74] *Hornung/Schnabel*, Data protection in Germany I: The population census decision and the right to informational self-determination, Computer Law & Security Review 25, 84.
[75] *Hornung/Schnabel*, Computer Law & Security Review 25, 84.
[76] BVerfGE 65, 1 (144).
[77] BVerfGE 65, 1 (Leitsätze).
[78] BVerfGE 65, 1 (146).

Selbstentfaltung dient dabei nicht nur den Einzelnen, sondern ist ebenfalls eine Vorrausetzung eines demokratischen politischen Systems, in das Bürger:innen sich frei einbringen. [79]

Die Verfügungsmacht des Menschen über seine Daten ist jedoch nicht allumfassend. Da Daten ein Abbild sozialer Realität darstellen, könnten diese nicht ausschließlich in den Herrschaftsbereich eines Menschen fallen.[80] Das dBVerfG betont, dass Einschränkungen des Rechts auf informationelle Selbstbestimmung für Zwecke im überwiegenden Allgemeininteresse prinzipiell möglich sind, wie auch im Falle der Volkszählung [81] – allerdings bedarf es in diesem Fall umfassende Schutzmaßnahmen. Um die Bürger:innen vor unverhältnismäßiger Datensammlung zu schützen, greifen die Datenschutzprinzipien, von denen das dBVerfG insbesondere das Transparenz- und Zweckbindungsprinzip hervorhebt, um die informationelle Selbstbestimmung zu wahren.[82]

Wie dargelegt ist das Grundrecht auf informationelle Selbstbestimmung Ausfluss des deutschen Verfassungsrechts und findet keine wortgleiche Übereinstimmung im österreichischen Verfassungsrecht. Allerdings ist das Recht auf informationelle Selbstbestimmung inzwischen nach hM auch im österreichischen Recht als Teil des Persönlichkeitsrecht iSd § 16 ABGB anerkannt.[83] 2011 bemerkte der OGH jedoch noch, dass das Recht auf informationelle Selbstbestimmung im vorliegenden Fall zu den Offenlegungsverpflichtung nach den §§ 277 ff UGB nicht zu prüfen sei, da es sich um ein *deutsches* Grundrecht handele. § 16 Satz 1 ABGB besagt, dass jeder Mensch ihm angeborene Rechte besitzt und daher als eine Person zu betrachten ist. Ähnlich wie aus Art 2 Abs 1 dGG, wird auch aus § 16 Satz 1 ABGB eine Vielzahl an Persönlichkeitsrechten abgeleitet, wie der Schutz der körperlichen Integrität oder der Ehre und des Ansehens. [84] Ebenfalls das Recht auf Achtung der Privats- und Geheimnissphäre wird von § 16 ABGB abgeleitet. Beispielsweise entschied mehrmals der OGH, dass Videoüberwachung durch Private unzulässig sei auf Grundlage von § 16 ABGB.[85] Auch wenn § 16 ABGB ein Recht auf informationelle Selbstbestimmung prinzipiell gewährt, ist jedoch noch offen wie dies im österreichischen Kontext auszulegen ist und ob der Verweis auf die deutsche Rechtsprechung hierfür geeignet ist. Eine weitere Quelle für das Recht auf informationelle Selbstbestimmung ist Art 8 Abs 1 GRC, das das Grundrecht auf Datenschutz sichert und aus dem laut

[79] BVerfGE 65, 1 (146).
[80] BVerfGE 65, 1 (148).
[81] BVerfGE 65, 1 (148, 166).
[82] *Mahieu*, The right of access to personal data: A genealogy, Technology and Regulation 2021, 62 (68).
[83] *Jaksch*, Zusammenfassung und Ausblick, in *Jaksch* (Hrsg), Datenschutzrechtliche Fragen des IT-gestützten Arbeitsplatzes (2020) 277 (136 f.); *Schwimann/Neumayr*, § 16 ABGB, in *Egger* (Hrsg), ABGB Taschenkommentar: mit EheG, EPG, KSchG, ASVG, EKHG und IPRG 6., neu bearbeitete Auflage(2024) Rn 15.
[84] *Fenyves/Kerschner/Vonkilch*, zu § 16 ABGB, in *Meissel* (Hrsg), Großkommentar zum ABGB - Klang (2008), .
[85] OGH 24.05.2018, 6 Ob 16/18y, Rz 8.

EuGH ein Anspruch auf Herrschaft über die eigenen Daten entspringt (siehe Kapitel 5.2 Lösungsweg 1).[86]

Grundsätzlich ist eine Datenspende ein Akt der informationellen Selbstbestimmung, wenn diese auf Basis der Einwilligung erfolgt. Das GTelG begrenzt in § 14 Abs 2, für welche Zwecke die Gesundheitsdaten, die innerhalb der ELGA gespeichert sind, verwendet werden dürfen. Erlaubt ist die Verarbeitung nach Punkt 3 des § 14 Abs 2 zur Wahrnehmung der Betroffenenrechte nach Kapitel III der DSGVO. Patient:innen dürfen also selbst – wie auch nach den Teilnehmer:innenrechten des Gesundheitstelematikgesetz (§ 16) – auf ihre Gesundheitsdaten zugreifen. Diese Ausnahmen spiegelt die Idee des Rechts auf informationelle Selbstbestimmung wider.

4.2.2.2. Recht auf Wahrung der Geheimsphäre

Das Recht auf Wahrung der Geheimsphäre schützt einerseits die Privatsphäre von natürlichen Personen und andererseits auch gegen die Verbreitung von (rechtmäßig erlangten) Informationen, die die Geheimsphäre betreffen.[87] Es umfasst unter anderem auch die **Geheimhaltung von Gesundheitsdaten**.[88] Referenzpunkt könnte die deutsche Rechtsprechung sein, laut der gem. des Urteils BGH VI ZR 9/56 BGHZ 24, 72 durch den deutschen Bundesgerichtshof bereits die Geheimsphäre bei der Preisgabe von Gesundheitszeugnissen an unberechtigte Dritte verletzt wird – dabei kommt es nicht auf den Inhalt der Gesundheitszeugnisse, sondern auf die Missachtung des persönlichen Willens beim Zugänglichmachen von höchstpersönlichen Umständen an. Der deutsche Bundesgerichtshof weist allerdings darauf hin, dass alltägliche oder minimale Gesundheitsveränderungen keinen schützenswerten Charakter haben, da diese "den körperlichen und geistigen Habitus nicht weiter berühren und an deren Geheimhaltung vernünftigerweise kein Interesse besteht"[89].

In **§ 1 DSG** findet sich allerdings auch die Bestimmung, dass das Grundrecht auf Geheimhaltung personenbezogener Daten besteht – auch bei nicht-automationsunterstützter Anwendung von Daten.[90] Dieses ist allerdings durch das jeweilige Interesse der Verarbeitenden beschränkt: Bei einem Eingriff durch Private in § 6 hat eine Interessenabwägung nach mit § 7 bis § 9 DSG zu geschehen, bei hoheitlichen Eingriffen sind die Voraussetzungen des § 1 Abs 2 DSG für die

[86] *Calliess et al*, EUV/AEUV: das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta: Kommentar[6. Auflage] (2022) Art. 8 Rn. 5,10.
[87] Aicher in Rummel/Lukas, ABGB[4] § 16, RZ 36 (Stand 1.7.2015, rdb.at).
[88] Aicher in Rummel/Lukas, ABGB[4] § 16, RZ 37 (Stand 1.7.2015, rdb.at).
[89] BGH VI ZR 9/56 BGHZ 24, 72, RZ 20.
[90] Aicher in Rummel/Lukas, ABGB[4] § 16, RZ 40 (Stand 1.7.2015, rdb.at).

Beurteilung der Rechtswidrigkeit heranzuziehen. Es ist davon auszugehen, dass bezüglich der Sekundärnutzung von ELGA-Daten unter den Gesichtspunkten des Forschungsprojekts Smart FOX keine unrechtmäßigen Eingriffe in das Grundrecht auf Datenschutz entstehen, wenn die oben angeführten Voraussetzungen für eine Datenverarbeitung eingehalten werden.

Aus § 1 DSG und die DSGVO sowie den darin enthaltenen Rechten der betroffenen Personen kann außerdem die **informationelle Selbstbestimmung** als ein besonderes Persönlichkeitsrecht iSd § 16 ABGB abgeleitet werden.[91]

Im Falle einer rechtswidrigen und schuldhaften tatsächlichen Verletzung des Rechts der Wahrung der Geheimsphäre besteht gem. § 1328a ABGB ein **Anspruch auf Schadenersatz** bei Verletzung der Privatsphäre. Wenn es sich dabei um erhebliche Verletzungen handelt, die Bloßstellungspotenzial in der Öffentlichkeit aufweisen, ist eine **Entschädigung für erlittene persönliche Beeinträchtigungen** möglich.

4.2.2.3. Recht am eigenen Bild

§ 78 UrhG bestimmt, dass Bildnisse von Menschen nicht veröffentlicht oder verbreitet werden dürfen, wenn dadurch berechtigte Interessen der betroffenen Person (oder im Fall einer verstorbenen Person die Interessen von Nahestehenden) verletzt würden. Dabei handelt es sich um einen Ausfluss des allgemeinen Persönlichkeitsrechts des § 16 ABGB.[92] Das **Sichtbarmachen** gegenüber mehreren Personen reicht bereits aus, um eine Verbreitung oder Veröffentlichung zu begründen – dabei ist nicht erheblich, ob das Bild tatsächlich auch wahrgenommen wurde.

Sämtliche **bildliche Abbildungen** sind vom Recht am eigenen Bild erfasst: Im medizinischen Bereich sind beispielsweise Bildnisse, die durch Röntgen-, Ultraschall- oder MRT-Untersuchungen entstanden sind, betroffen. Allerdings ist besteht nur ein Recht am eigenen Bild, sofern die Person darauf auch erkennbar ist. Die **Erkennbarkeit** wird üblicherweise nicht durch etwa das Einfügen eines schwarzen Balkens über der Augenpartie ausgeschlossen. Das Gesicht stellt nicht das einzige Merkmal für die Erkennbarkeit dar: sämtliche Umstände, die charakteristisch für die betroffene Person sind (etwa Tattoos, Frisur oder Bart, Körperstatur oder beschreibender Begleittext des

[91] Posch in Schwimann/Kodek (Hrsg), ABGB Praxiskommentar[5] (2018), § 16 ABGB, RZ 42.
[92] Helene Herda, Die Verwendung von Patientenbildern durch die Krankenanstalt: Zustimmungserfordernis für Patienten?, RdM 2024/27.

Bildes), sind ebenso beachtlich.[93] Als Maßstab für die Erkennbarkeit sind Personen heranzuziehen, die die betroffene Person bereits mehrfach betrachtet haben.[94]

Der Schutz des Rechts am eigenen Bild erfasst die **berechtigten Interessen von natürlichen Personen** – dabei handelt es sich um nach der allgemeinen Betrachtung und objektivierte anerkannte Interessen. Diese sind jedenfalls als verletzt zu werten, wenn eine Veröffentlichung herabwürdigende, entwürdigende oder entstellende Konsequenzen nach sich zieht. Geschützt sind nach der österreichischen Rechtsordnung definitiv die persönliche Gesundheit als Teil des höchstpersönlichen Lebensbereichs, in diesem Fall wird der Kernbereich des höchstpersönlichen Lebensbereichs berührt und ein Eingriff nicht durch eine Interessenabwägung rechtfertigbar.[95] Auch Röntgenaufnahmen, MRTs, Ultraschallbilder, etc. sind demnach besonders sensibel, wenn darauf Personen erkennbar sind.

Nach § 81 UrhG steht den betroffenen Personen unabhängig vom tatsächlichen Verschulden ein **Anspruch auf Unterlassung** zu, wenn das Recht am eigenen Bild verletzt wird oder eine Verletzung zu befürchten ist. In § 82 UrhG wird der Beseitigungsanspruch seitens der verletzten Person geregelt. Dieser besagt, dass entgegen dem Recht am eigenen Bild hergestellte oder verbreitete Vervielfältigungen auf Verlangen zu beseitigen sind. Außerdem kann gem. § 85 UrhG durch das Gericht aufgetragen werden, dass die verletzende Partei das **Urteil** auf Unterlassung, Beseitigung oder (Nicht-)Bestehens eines Ausschließungs- oder Urheberrechts zu veröffentlichen hat. Gem. § 87 UrhG steht außerdem bei einer schuldhaften Schädigung ein **Ersatz des entgangenen Gewinns** zu, bei der Verletzung der Bildnisschutzrechte sowohl für materielle als auch für immaterielle Schäden. Dafür muss von den Geschädigten der Schaden behauptet und nachgewiesen werden. Der entgangene Gewinn ist unabhängig vom Verschuldensgrad zu ersetzen.[96] Die leichte Fahrlässigkeit genügt bereits hinsichtlich des Verschuldens der verletzenden Person.[97] Nach § 88 UrhG ist außerdem zu beachten, dass im Falle eines Verstoßes gegen das Recht am eigenen Bild durch bedienstete oder beauftragte Personen im Rahmen des Betriebs eines **Unternehmens** die Inhabenden des Unternehmens haften – beispielsweise haften im Fall von Krankenanstalten die

[93] Helene Herda, Die Verwendung von Patientenbildern durch die Krankenanstalt: Zustimmungserfordernis für Patienten?, RdM 2024/27.
[94] Thurner in Thiele/Burgstaller, UrhG[4] § 78 Rz 21.
[95] Helene Herda, Die Verwendung von Patientenbildern durch die Krankenanstalt: Zustimmungserfordernis für Patienten?, RdM 2024/27.
[96] Zemann in Dokalik/Zemann, Urheberrecht[8] § 87 UrhG (Stand 1.10.2022, rdb.at).
[97] Nageler-Petritz in Handig/Hofmarcher/Kucsko, urheber.recht[3] § 87 UrhG (Stand 1.8.2023, rdb.at).

jeweilige Trägerin, wenn es sich dabei nicht um private Handlungen von Bediensteten/Beauftragten handelt.

Soweit im Rahmen der Sekundärdatennutzung keine MRT-, Röntgen-, Ultraschall- oder fotografische Bilder gespendet und verarbeitet werden, auf denen eine natürliche Person erkennbar oder identifizierbar ist, stellt das Recht am eigenen Bild im Rahmen des Forschungsprojekts Smart FOX kein Hindernis für die Sekundärnutzung von gespendeten Gesundheitsdaten dar.

4.2.3. Betroffenenrechte

Wenn in eine Datenspende eingewilligt wird, haben die Datenspender:innen in der Regel auch danach noch verschiedene Recht an ihren personenbezogenen Daten, wie Auskunfts-, Berichtigungs- und Löschungsrechte. Diese Rechte werden im zweiten Kapitel der DSGVO festgelegt. Für die Wahrung und Umsetzung der Betroffenenrechte sind die Verantwortlichen für die Datenverarbeitung zuständig. Allerdings können Betroffenenrechte auch eingeschränkt werden. Art 89 Abs 1 DSGVO stellt eine sogenannte **Öffnungsklausel** dar, durch die den Mitgliedsstaaten ermöglicht wird, im nationalen Recht zu regeln, unter welchen Umständen die Betroffenenrechte gegenüber anderen Anliegen zurückstehen müssen. Österreich hat dies im § 2d Abs 6 FOG geregelt. Diese Rechtsvorschrift besagt, dass manche der Rechte keine Anwendung finden, wenn dadurch die Erreichung der Zwecke des FOGs unmöglich oder ernsthaft beeinträchtigt sind (siehe Kapitel 4.2.3.9.).

Im Folgenden werden die Betroffenenrechte nach Art 12 bis 22 DSGVO dargestellt. Darauf folgt eine Erläuterung, welche der Rechte auf Grundlage von § 2d Abs 6 FOG eingeschränkt werden können und unter welchen Bedingungen dies zulässig ist.

4.2.3.1. Transparenzpflichten

Art 12, 13 und 14 führt das Transparenzprinzip des Art 5 DSGVO weiter aus und verpflichtet Datenverantwortliche dazu, betroffenen Personen **Informationen über die Verarbeitung** ihrer personenbezogenen Daten bereitzustellen. Art 13 und Art 14 differenzieren hinsichtlich der Art der Datenerhebung: Werden Daten direkt bei der betroffenen Person erhoben, ist Art 13 einschlägig, andernfalls Art 14 DSGVO. Im Falle einer Datenspende werden die Daten durch die Betroffenen selbst zur Verfügung gestellt und somit ist Ersteres der Fall. Zum Zeitpunkt der „Erhebung“ personenbezogener Daten müssen folgende Informationen durch die Verantwortlichen zur Verfügung gestellt werden:

- die Identität und Kontaktdaten der Verantwortlichen sowie gegebenenfalls deren Vertreter:innen;
- Kontaktdaten der Datenschutzbeauftragten;
- Rechtsgrundlage und Zwecke der Verarbeitung personenbezogener Daten;
- Empfänger:innen oder Kategorien von Empfänger:innen der personenbezogenen Daten;
- Informationen über die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen;
- Dauer der Datenspeicherung;
- das Bestehen von Rechten der betroffenen Personen sowie die notwendigen Schritte zur Ausübung dieser Rechte.

Art 12 DGSVO erläutert zudem die Art und Weise, wie diese Informationen bereitgestellt werden müssen. So müssen die Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ übermittelt werden, sowie in kindgerechter Sprache, wenn es sich um eine Verarbeitung von Daten von Minderjährigen handelt.

Die Transparenzpflichten können nicht durch § 2d Abs 6 FOG beschränkt werden.

4.2.3.2. Das Recht auf Auskunft

Während die Transparenzpflichten proaktives Handeln der Verantwortlichen verlangen, kann die Herausgabe von Informationen zusätzlich auch von Betroffenen verlangt werden, zum Beispiel Jahre nach der Datenspende. Das Auskunftsrecht in Art 15 ermöglicht betroffenen Personen, vom Verantwortlichen eine Bestätigung darüber zu erhalten, ob personenbezogene Daten, die sie betreffen, verarbeitet werden. Wenn dies der Fall ist, haben die Verantwortlichen die Pflicht, der betroffenen Person Zugang zu folgenden Informationen zu gewähren:

- Zweck(e) der Verarbeitung personenbezogener Daten;
- Kategorien der verarbeiteten Daten;
- Empfänger:innen, an die personenbezogene Daten weitergegeben wurden oder weitergegeben werden;
- Dauer der Datenspeicherung;
- bestehende Rechte der betroffenen Personen, einschließlich des Rechts, eine Beschwerde bei der Aufsichtsbehörde einzureichen;
- Datenquelle, wenn die personenbezogenen Daten nicht direkt bei der betroffenen Person erhoben wurden;

- geplante **Datenübermittlungen** an Drittländer oder internationale Organisationen gem. Artikel 46;
- das Vorhandensein von **automatisierten Entscheidungsfindungen und Profiling** gem. Art 22 DSGVO.

Das Recht auf Auskunft kann nach § 2d Abs 6 FOG eingeschränkt werden, wenn dadurch die Durchführung des Forschungsvorhabens nicht möglich ist. Dies könnte zum Beispiel der Fall sein, wenn die Verantwortlichen durch die fortgeschrittene Weiterverarbeitung der Daten sowie durch Pseudonymisierung oder Aggregation der Daten nicht sicher wissen, ob noch personenbezogene Daten der Betroffenen vorhanden sind und somit keine Auskunft gegeben werden kann.

4.2.3.3. Das Recht auf Berichtigung

Gelangt die betroffene Personen Kenntnis darüber, dass personenbezogene Daten über sie **falsch oder unvollständig** sind, hat diese nach Art 16 DGSVO das Recht, von den Verantwortlichen die Berichtigung dieser Daten zu verlangen. Die Verantwortlichen sind verpflichtet, dieses Anliegen unverzüglich zu bearbeiten.

Das Recht auf Berichtigung kann nach § 2d Abs 6 FOG eingeschränkt werden.

4.2.3.4. Das Recht auf Löschung (Recht auf Vergessenwerden)

Laut Art 17 DSGVO gibt das Recht auf Löschung betroffenen Personen unter bestimmten Umständen das Recht, von Verantwortlichen die Löschung ihrer personenbezogenen Daten einschließlich Sicherungskopien zu verlangen. Dieses Recht besteht, wenn eine der folgenden Bedingungen vorliegt:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder verarbeitet wurden, **nicht mehr erforderlich**;
- Die betroffene Person **widerruft** ihre Einwilligung, und es gibt keine andere Rechtsgrundlage für die Verarbeitung;
- Die betroffene Person legt **Widerspruch** gegen die Verarbeitung nach Art 21 Abs 1 DSGVO ein, und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor;
- Die betroffene Person **widerspricht** der Verarbeitung für Zwecke der **Direktwerbung** nach Art 21 Abs 2 DSGVO;
- Die Verarbeitung erfolgte **unrechtmäßig**;

- Eine **gesetzliche Verpflichtung** zur Löschung besteht nach EU-Recht oder nationalem Recht;
- Die Daten betreffen ein **Kind** und wurden im Rahmen eines Dienstes der Informationsgesellschaft gemäß Artikel 8 Abs 1 DSGVO erhoben.

Das Recht auf Löschung ist nicht absolut und kann, wie in Art 17 Abs 3 DSGVO ausgeführt, **eingeschränkt** werden. Eine Einschränkung kann beispielsweise durch das Recht auf freie Meinungsäußerung und Informationsfreiheit, zum Schutz der öffentlichen Gesundheit oder zur Verwirklichung von Zielen im öffentlichen Interesse gem. Art 89 Abs 1 DSGVO gerechtfertigt sein. Unter letzteres können ebenfalls wissenschaftliche oder historische Forschungszwecke fallen.

Das Recht auf Löschung kann nach § 2d Abs 6 FOG eingeschränkt werden.

4.2.3.5. Das Recht auf Einschränkung der Verarbeitung

Laut Art 18 DSGVO haben betroffene Personen das Recht, die Einschränkung der Verarbeitung ihrer Daten durch den Verantwortlichen zu verlangen, wenn eine der folgenden Umstände vorliegt:

- Die **Richtigkeit** der Daten wird von der betroffenen Person angefochten (die Verarbeitung wird für die Dauer der Überprüfung eingeschränkt);
- Die Verarbeitung erfolgte **unrechtmäßig** und die betroffene Person fordert anstelle der Löschung eine Einschränkung der Nutzung;
- Die Verantwortlichen benötigen die Daten nicht mehr für die Verarbeitung, aber die betroffene Person benötigt sie zur Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen**;
- Die betroffene Person hat **Widerspruch** gegen die Verarbeitung eingelegt (siehe Art 21 DSGVO), während die Prüfung erfolgt, ob die berechtigten Gründe des Verantwortlichen die der betroffenen Person überwiegen.

Das Recht auf Einschränkung der Verarbeitung kann ebenfalls auf Grundlage des § 2d Abs 6 FOG eingeschränkt werden. Gefährdet die Löschung der personenbezogenen Daten die Verwirklichung des Forschungszwecks, muss das Recht der Datenspender:in zurückstehen.

4.2.3.6. Das Recht auf Datenübertragbarkeit

Das Recht auf Datenübertragbarkeit, das in Art 20 DSGVO zugesichert wird, ermöglicht es betroffenen Personen, ihre personenbezogenen Daten in einem „strukturierten, gängigen und

maschinenlesbaren Format“ von den Verantwortlichen zu erhalten. Betroffene Personen haben das Recht, diese Daten ohne Hürden an andere Verantwortliche zu übermitteln, und können gegebenenfalls die direkte Übertragung zwischen den Verantwortlichen verlangen, sofern dies technisch machbar ist.

Das Recht auf Datenübertragbarkeit kann geltend gemacht werden, wenn die Verarbeitung der personenbezogenen Daten:

- auf der Grundlage einer **Einwilligung oder** eines **Vertrags** erfolgt und
- mithilfe **automatisierter Verfahren** durchgeführt wird.

Das Recht auf Datenübertragbarkeit kann nicht ausgeübt werden, wenn die Verarbeitung zur Erfüllung einer Aufgabe im **öffentlichen Interesse oder zur Ausübung öffentlicher Gewalt** erfolgt, die den Verantwortlichen übertragen wurde.

Das Recht auf Datenübertragbarkeit kann nach § 2d Abs 6 FOG eingeschränkt werden.

4.2.3.7. Das Recht auf Widerspruch gegen die Verarbeitung

Betroffene Personen haben laut Art 21 DSGVO das Recht, der Verarbeitung ihrer personenbezogenen Daten in bestimmten Situationen zu widersprechen, insbesondere wenn die Verarbeitung:

- auf der Grundlage eines **öffentlichen Interesses oder** einer den Verantwortlichen **übertragenen offiziellen Aufgabe**, einschließlich Profiling, erfolgt;
- auf der Grundlage eines **berechtigten Interesses der Verantwortlichen**, einschließlich Profiling, erfolgt;
- für Zwecke der **Direktwerbung**, einschließlich Profiling, geschieht;
- der personenbezogenen Daten für wissenschaftliche oder historische **Forschungszwecke** oder für **statistische Zwecke** gem. Art 89 Abs 1 DSGVO vorgenommen wird.

Das Recht auf Widerspruch kann nach § 2d Abs 6 FOG eingeschränkt werden.

4.2.3.8. Rechte in Bezug auf automatisierte Entscheidungsfindung und Profiling

Art 22 DSGVO behandelt die automatisierte Entscheidungsfindung, also Fälle, in denen auf Grundlage von Datenprofilen Entscheidungen über die Betroffenen getroffen werden. Art 22 verbietet eine automatisierte Entscheidungsfindung, wenn diese keiner menschlichen Kontrolle unterliegt und die Entscheidung rechtliche oder ähnlich schwerwiegende Auswirkungen auf die Betroffenen.

Dieses Verbot gilt nicht, wenn:

- die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und den Verantwortlichen erforderlich ist;
- die Entscheidung durch das Recht der Union oder eines Mitgliedstaats, dem die Verantwortlichen unterliegen, erlaubt ist und dieses Recht auch Maßnahmen zum Schutz der Rechte, Freiheiten und berechtigten Interessen der betroffenen Person enthält;
- die betroffene Person ihre ausdrückliche Einwilligung gegeben hat.

Wenn diese Ausnahmen zutreffen, sind die Verantwortlichen verpflichtet, Maßnahmen zum Schutz der betroffenen Person zu ergreifen. Diese Maßnahmen umfassen:

- Schutzvorkehrungen zum Schutz der Rechte, Freiheiten und berechtigten Interessen der betroffenen Person;
- das Recht der betroffenen Person, menschliches Eingreifen zu verlangen;
- das Recht der betroffenen Person, ihren Standpunkt darzulegen und die Entscheidung anzufechten.

Das Recht, nicht Gegenstand einer automatisierten Entscheidungsfindung zu sein, kann nicht auf Grundlage von § 2d Abs 1 FOG eingeschränkt werden.

4.2.3.9. Bedingungen Einschränkung der Betroffenenrechte nach § 2d Abs 1 und Abs 6 FOG

§ 2d Abs 6 FOG definiert, welche Betroffenenrechte grundsätzlich eingeschränkt werden können. Diese sind:

- Auskunftsrecht der betroffenen Person (Art 15 DSGVO),

- Recht auf **Berichtigung** (Art 16 DSGVO),
- Recht auf **Löschung** bzw. Recht auf Vergessenwerden (Art 17 DSGVO),
- Recht auf **Einschränkung** der Verarbeitung (Art 18 DSGVO),
- Recht auf **Datenübertragbarkeit** (Art 20 DSGVO) sowie
- **Widerspruch**srecht (Art 21 DSGVO).

Voraussetzung ist dafür, dass die Wahrnehmung des jeweiligen Rechts der Betroffenen, die **Erreichung des Forschungszweckes unmöglich macht oder ernsthaft gefährdet**. Dass dies der Fall ist, muss glaubhaft begründet werden können und darf nicht als Vorwand gelten, um die administrative Arbeit der Einhaltung der Betroffenenrechte zu umgehen.

§ 2d Abs 1 FOG beschreibt überdies die spezifischen Bedingungen, unter denen die Betroffenenrechte eingeschränkt werden können. Die **wesentlichen Bedingungen** für die Datenverarbeitenden werden im Folgenden dargestellt.

- Erstens muss die Verarbeitung der Daten **protokolliert** werden, sodass alle Zugriffe, einschließlich Änderungen, Abfragen und Übermittlungen erfasst werden und ihre Rechtmäßigkeit bei Bedarf in der Zukunft überprüft werden kann.
- Zweitens sind die Datenverarbeitenden zur **Geheimhaltung** verpflichtet, um sicherzustellen, dass die Daten nicht außerhalb des festgelegten Rahmens bekannt werden.
- Daran anschließend verpflichtet § 2d Abs 1 FOG, drittens, dazu, dass die personenbezogenen Daten ausschließlich für die **Zwecke des spezifischen Forschungszwecks** genutzt werden und keine anderweitige Verwendung erfolgt.
- Viertens dürfen die betroffenen Personen **keine Nachteile** aus der Datenverarbeitung erleiden. Die Verarbeitung der Daten wird, sofern sie im Einklang mit dem Gesetz erfolgt, nicht als Nachteil gewertet.
- Fünftens müssen die Verantwortlichen für die Datenverarbeitung eine Reihe von **Maßnahmen** umsetzen, um Transparenz herzustellen und die Sicherheit der Daten zu gewährleisten. Zu diesen Maßnahmen gehören unter anderem:
    - öffentliche Hinweise auf die rechtliche Grundlage der Datenverarbeitung im Internet; Sicherstellung, dass die Daten pseudonymisiert sind;
    - Festlegung der Aufgabenverteilung bei der Datenverarbeitung;
    - Sicherstellung, dass nur autorisierte Mitarbeitende auf die Daten zugreifen können.
- Sechstens ist die **Veröffentlichung** von Personenkennzeichen verboten, durch die personenbezogene Daten öffentlich zugänglich gemacht werden und wodurch diese missbraucht werden können.

Die Einschränkung der Betroffenenrechte hinsichtlich Datenverarbeitungen innerhalb des „SmartFOX“-Projektes ist grundsätzlich möglich, wenn die oben genannten Bedingungen erfüllt werden, allerdings nur, wenn die Erreichung des Forschungszweckes sonst unmöglich oder ernsthaft gefährdet wäre. Dies ist nach momentaner Abschätzung nicht der Fall, weshalb die Betroffenenrechte vollständig gewährleistet werden müssen. Zudem ist zu betonen, dass eine Einschränkung der Betroffenenrechte ausschließlich für Zwecke des Art 89 Abs 1 DSGVO (Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken) möglich ist.

4.3. Datenschutzfolgeabschätzung und Ausnahmen

Im Rahmen des Forschungsprojekts Smart FOX wurden die Konsortialpartner:innen seitens des Teams der UNIVIE darauf hingewiesen, dass vor den Verarbeitungen von personenbezogenen Daten eventuell eine Datenschutzfolgeabschätzung (DSFA) nach Art 35 DSGVO erforderlich ist. Die Verantwortlichen haben demnach eine DSFA durchzuführen, wenn „eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat (Art 35 Abs 1 DSGVO). Eine Auflistung der Fälle, in denen jedenfalls eine DSFA erforderlich ist, findet sich in Art 35 Abs3 DSGVO, welche auch die umfangreiche Verarbeitung besonderer Kategorien von Daten gem. Art 9 Abs 1 DSGVO enthält. Da Gesundheitsdaten eine solche besondere Kategorie darstellen, wäre grds. zu erwarten, dass hinsichtlich des Forschungsprojekts Smart FOX vor der umfangreichen Verarbeitung von personenbezogenen Gesundheitsdaten eine solche DSFA durchzuführen wäre.

Die DSGVO verpflichtet Aufsichtsbehörden, eine Liste der Verarbeitungsvorgänge, für die jedenfalls eine DSFA durchzuführen ist, zu veröffentlichen (Art 35 Abs 4 DSGVO). Die DSGVO ermöglicht es Aufsichtsbehörden ebenso, das Gegenteil zu veröffentlichen – also eine Liste der Verarbeitungsvorgänge, für welche keine DSFA erforderlich ist (Art 35 Abs 5 DSGVO). Diese Listen werden oft „Blacklist“ (Notwendigkeit für eine DSFA) und „Whitelist“ (keine Notwendigkeit für eine DSFA) bezeichnet. Die österreichische Datenschutzbehörde als nationale Aufsichtsbehörde hat beide Listen erstellt: Die „Whitelist“ ist die DSFA-AV (Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), BGBl II 108/2018). Diese beinhaltet eine sehr breite Ausnahme von der Pflicht zur Vornahme einer DSFA für die wissenschaftliche Forschung, nämlich eine Ausnahme für den Zweck der „Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke aufgrund besonderer gesetzlicher Vorschriften oder mit Einwilligung der betroffenen Person.“ (DSFA-A14).

Da im AHDDS Gesundheitsdaten mit Einwilligung der betroffenen Personen zu wissenschaftlichen Forschungszwecken verarbeitet werden sollen, ist es grundsätzlich denkbar, dass diese Ausnahme des DSFA-A14 anwendbar wäre.[98] Hier ist festzuhalten, dass es nach österreichischem Recht möglich sein könnte, bei der Verarbeitung von Gesundheitsdaten auf Grundlage der Einwilligung im Rahmen

[98] *Schmidbauer/Kaltenbrunner*, Datenschutz-Folgenabschätzung und Grundrechte-Folgenabschätzung in der KI-Forschung. JusIT : Zeitschrift für IT-Recht, Rechtsinformation, Datenschutz, (5/2024), 192-198.

eines Forschungsprojekts von der DSFA-Pflicht ausgenommen zu sein. Zu bedenken ist jedoch, dass es fraglich ist, ob diese breit gefasste Ausnahme dem unionsrechtlichen Rahmen entspricht, da die DSGVO ja bei der umfangreichen Verarbeitung besonderer Datenkategorien eine DSFA fordert. Die DSGVO enthält keine Öffnungsklausel, die es nationale Datenschutzbehörden ermöglich würde, von der DSFA-Regelung in der DSGVO abzuweichen. Es ist bei Art 35 Abs 4 und Abs 5 DSGVO anzunehmen, dass diese nur der Konkretisierung der DSFA-Pflicht hätten dienen sollen. Des Weiteren ist laut Art 35 Abs 5 DSGVO die Whitelist an den Europäischen Datenschutzausschuss zu übermitteln. Dies ist mit der österreichischen Whitelist, soweit ersichtlich und im Gegensatz zur sogenannten Blacklist[99], nie erfolgt, daher gab es auch bis dato keine offizielle Auseinandersetzung des Europäischen Datenschutzausschusses mit der Unionsrechtskonformität dieser österreichischen Ausnahme. Es kann daher grundsätzlich davon ausgegangen werden, dass die DSFA-AV anwendbar ist – dabei muss aber auch bedacht werden, dass diese kurzfristigen Änderungen unterliegen könnte.[100]

Die Durchführung einer DSFA stellt oft einen erheblichen administrativen Aufwand dar, kann jedoch auch für Verantwortliche ein sinnvolles Instrument sein, um Risiken zu bewerten, Sicherheitsmaßnahmen und Garantien durchzudenken und die Einhaltung mit der DSGVO zu garantieren. Da die Forschungsausnahme basierend auf der DSFA-AV sich kurzfristig ändern könnte und es keine unionsrechtliche Grundlage für eine allgemeine Ausnahme für die wissenschaftliche Forschung gibt, ist es nicht ratsam, die Struktur des AHDDS auf der Annahme aufzubauen, dass keine DSFAs durchgeführt werden müssen.

Da es die Verantwortlichen für die Datenverarbeitung sind, die dieser Pflicht nachkommen müssen, wird der Prozess zur Durchführung einer DSFA bei der Gesundheitsdatenspende von der Struktur und den Datenschutzrollen innerhalb des AHDDS abhängen.

Nach Art 35 Abs 7 DSGVO sind die Mindestanforderungen an den Inhalt einer DSFA wie folgt:

- eine Beschreibung der **Verarbeitungsvorgänge und Zwecke**, ggfs. inklusive der verfolgten berechtigten Interessen;

[99] EDSA, Opinion 1/2018 on the draft list of the competent supervisory authority of Austria regarding the processing operations subject to the re-quirement of a data protection impact assessment (Article 35.4 GDPR) <https://www.edpb.europa.eu/sites/default/files/files/file1/2018-09-25-opinion_2018_art._64_at_sas_dpia_list_en.pdf> (12. 8. 2024).
[100] *Schmidbauer/Kaltenbrunner*, Datenschutz-Folgenabschätzung und Grundrechte-Folgenabschätzung in der KI-Forschung. JusIT : Zeitschrift für IT-Recht, Rechtsinformation, Datenschutz, (5/2024), 192-198.

- eine **Bewertung der Notwendigkeit und Verhältnismäßigkeit** der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine **Bewertung der Risiken für die Rechte und Freiheiten** der betroffenen Personen; sowie
- **Abhilfemaßnahmen**, inkl. Garantien, Sicherheitsvorkehrungen und Verfahren, zur Bewältigung der Risiken und zur Garantie der Einhaltung der DSGVO.

Da die DSFA von den Verantwortlichen durchgeführt werden müssen, ist für den AHDDS noch unklar, ob es eine zentrale Stelle geben wird, welche eventuell für mehrere ähnliche Verarbeitungsvorgänge auf einmal eine DSFA durchzuführen hat, oder ob die Leiter:innen einzelner Studien und Forschungsprojekte jeweils eine DSFA durchzuführen haben. Da es derzeit scheint, dass das Konsortium des Forschungsprojekts Smart FOX (bzw. einzelne Konsortialpartner:innen oder eine eigens gegründete juristische Person) eher die Rolle eines Auftragsverarbeiters gegenüber den Leiter:innen einzelner Studien einnehmen würde (siehe Kapitel 4.1.2),ist zweiteres wahrscheinlicher. Sollte das Konsortium des Forschungsprojekts Smart FOX (oder eine andere aus dem Projekt entstehende Rechtsperson oder eine:r der Partner:innen) jedoch Verarbeitungsschritte im AHDDS unternehmen, wie etwa die Pseudonymisierung oder Anonymisierung von Daten, welche als umfangreiche Verarbeitung von Gesundheitsdaten zu verstehen sind, so ist es aus Sicht des Teams der UNIVIE ratsam, trotz der DSFA-AV eine DSFA durchzuführen und dies von Anfang an in die Struktur und Abläufe des AHDDS einzuplanen. Die finale Verantwortung für diese Entscheidung liegt jedoch bei den datenschutzrechtlich Verantwortlichen, also entweder bei (sämtlichen) Konsortialpartner:innen oder einer aus dem Forschungsprojekt entstandenen Rechtsperson.

5. Wie kann Datenspende in Österreich rechtlich funktionieren?

Im folgenden Abschnitt wird thematisiert, wie die nationalen und internationalen Regelungen Einfluss auf die Spende von Gesundheitsdaten haben. Dabei soll geklärt werden, wie eine Verarbeitung von ELGA-Daten oder ELGA-standardisierte Daten innerhalb des Forschungsprojekts Smart FOX rechtlich zu bewerten ist. Außerdem wird auf die institutionelle Umsetzung eingegangen – dabei werden datenaltruistischen Organisationen nach dem DGA und die finanzielle Vergütung von Datenspenden untersucht.

5.1. Einschränkungen der Sekundärnutzung von ELGA-Daten

Die ELGA wird seit dem 1. Jänner 2013 im vierten Abschnitt des **GTelG** 2012 geregelt. In § 2 Z 6 des GTelG 2012 wird die ELGA als „ein Informationssystem, das allen berechtigten ELGA-Gesundheitsdiensteanbietern […] und ELGA-Teilnehmer/inne/n ELGA-Gesundheitsdaten […] in elektronischer Form orts- und zeitunabhängig (ungerichtete Kommunikation) zur Verfügung stellt“, definiert. Gem § 13 Abs 1 GTelG 2012 dient die ELGA einem **erheblichen öffentlichen Interesse**, was den lit g, h, i und j des Art 9 DSGVO entspricht und somit die Verarbeitung besonderer Kategorien personenbezogener Daten erlaubt (hinsichtlich Art 9 DSGVO siehe Kapitel 4.1.2.4.).

In Art 9 Abs 2 lit g und lit j DSGVO wird die **Verhältnismäßigkeit zwischen Eingriffsintensität der Datenverarbeitung** einerseits **und dem angestrebten Ziel** andererseits gefordert – dieser Regelung wird entsprochen, indem nur ELGA-Gesundheitsdaten im Rahmen einer Gesundheitsversorgung innerhalb eines Behandlungs-/Betreuungsverhältnisses von den konkret teilhabenden bzw. mitwirkenden ELGA-Gesundheitsdiensteanbieter:innen verarbeitet werden dürfen. Konkret werden die Anforderungen des Art 9 Abs 2 lit g, i und j DSGVO für angemessene und **spezifische Maßnahmen zur Wahrung der Freiheiten, Grundrechte und Interessen** der betroffenen Person durch die dezentrale Speicherung der ELGA-Gesundheitsdaten für maximal zehn Jahre im Gebiet der EU, Datensicherheitsmaßnahmen (siehe zweiter Abschnitt des GTelG 2012, §§ 18f GTelG 2012, §§ 17b bis 17j ELGA-Verordnung 2015 (ELGA-VO 2015)), die Verarbeitungsbeschränkungen und -verbote (§ 14 GTelG 2012) sowie die möglichst frühe Pseudonymisierung von personenbezogenen Daten (§ 4 Abs 6 sowie § 14 Abs 1 GTelG 2012) zu erfüllen versucht. Zusätzlich werden im Rahmen der ELGA-

Ombudsstelle und Teilnehmer:innenrechte die persönlichen Freiheiten, Grundrechte und Interessen geschützt.[101]

ELGA-Gesundheitsdaten sind folgendermaßen definiert:

§ 2 Z 9 GTelG 2012
„ELGA-Gesundheitsdaten“: Folgende personenbezogene Daten, die zur weiteren Behandlung, Betreuung oder Sicherung der Versorgungskontinuität von ELGA-Teilnehmer/inne/n wesentlich sein könnten und in ELGA verarbeitet werden dürfen: a) medizinische Dokumente einschließlich allfälliger Bilddaten in standardisierter Form gemäß § 28 Abs. 2 Z 1, die Gesundheitsdaten gemäß Z 1 oder genetische Daten gemäß Z 1a, mit Ausnahme von Daten, die ausschließlich die Verrechnung von Gesundheitsdienstleistungen oder gesundheitsbezogenen Versicherungsdienstleistungen betreffen, enthalten, wie: aa) Entlassungsbriefe gemäß § 24 Abs. 2 des Krankenanstalten- und Kuranstaltengesetzes (KAKuG), BGBl. Nr. 1/1957, bb) Laborbefunde, cc) Befunde der bildgebenden Diagnostik sowie dd) weitere medizinische Befunde in Struktur und Format gemäß § 28 Abs. 2 Z 3 lit. a, b) Medikationsdaten gemäß Z 1 betreffend verschreibungspflichtige sowie nicht verschreibungspflichtige Arzneimittel („e-Medikation“), c) Patientenverfügungen (§ 2 Abs. 1 des Patientenverfügungs-Gesetzes, BGBl. I Nr. 55/2006), d) Vorsorgevollmachten (§ 260 des Allgemeinen bürgerlichen Gesetzbuches, JGS. Nr. 946/1811), e) Daten aus den Registern gemäß den §§ 45 und 46 des Medizinproduktegesetzes 2021 (MPG 2021), BGBl. I Nr. 122/2021, sowie f) Patientendaten gemäß Art. 14 Abs. 2 lit. b sublit. i der Richtlinie 2011/24/EU über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung („patient summary“), wobei Geheimnisse gemäß § 10 Abs. 4 KAKuG, Daten dieser Art, wenn sie von anderen Gesundheitsdiensteanbietern verwendet werden, sowie Aufzeichnungen über Ergebnisse gemäß § 71a Abs. 2 des Gentechnikgesetzes (GTG), BGBl. Nr. 510/1994, keinesfalls ELGA-Gesundheitsdaten sind.

Gem § 14 Abs 2 GTelG dürfen ELGA-Gesundheitsdaten iSd § 2 Z 9 GTelG 2012 nur im Rahmen eines Behandlungs- oder Betreuungsverhältnisses und für die Zwecke der Gesundheitsversorgung verwendet werden, diese Beschränkung stellt nach *Stärker* einen Ausfluss des Verhältnismäßigkeitsprinzips dar.[102] Die ELGA-Gesundheitsdaten sind somit eine Teilmenge der Gesundheitsdaten, wie sie in § 2 Z 1 GTelG 2012 mit Verweis auf Art 4 Z 15 DSGVO definiert werden – dadurch werden nur Gesundheitsdaten gespeichert, die rein der medizinischen Versorgung der ELGA-Teilnehmenden dienen:[103]

§ 2 Z 1 GTelG 2012
„Gesundheitsdaten“: Gesundheitsdaten gemäß Art. 4 Z 15 DSGVO.

[101] Milisits/Pfandlsteiner in Aigner/Kletečka/Kletečka-Pulker/Memmer, Handbuch Medizinrecht Kap. I.9 (Stand 1.9.2023, rdb.at).
[102] Stärker in Neumayr/Resch/Wallner, GmundKomm² Einleitung GTelG 2012, RZ 8 (Stand 1.1.2022, rdb.at). Siehe auch die Erläuterungen zur Regierungsvorlage zum Elektronische Gesundheitsakte-Gesetz (1936 der Beilagen XXIV. GP., S. 5).
[103] Stärker in Neumayr/Resch/Wallner, GmundKomm² § 2 GTelG 2012 (Stand 1.1.2022, rdb.at).

Art 4 Z 15 DSGVO
"Gesundheitsdaten" personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen

ELGA-Gesundheitsdiensteanbieter:innen haben keine **Datenschutzfolgenabschätzung** gem. § 14 Abs 5 GTelG 2012 durchzuführen, da diese schon in den Erläuterungen zum Deregulierungsgesetz 2017 durch den Gesetzgeber vorweggenommen wurde (im Einklang mit Art 35 Abs 10 DSGVO).[104]

Zu beachten sind auch einschlägige Verordnungen: In der **ELGA-VO 2015** sind die für die ELGA einzuhaltenden Parameter für die ELGA-Gesundheitsdaten (Codierung, Format, Inhalt, Struktur) in Implementierungsleitfäden sowie die Servicecenter und Ombuds-/Widerspruchsstelle geregelt. In der **Gesundheitstelematikverordnung 2013** (GTelV 2013) werden die Rollen der Gesundheitsdiensteanbieter:innen sowie die kryptographischen Algorithmen klargestellt.

Zentral für die Verarbeitung von Gesundheitsdaten innerhalb von Smart FOX ist § 14 GTelG. Eine Verarbeitung von personenbezogenen von ELGA verfügbar gemachten ELGA-Daten ist gem. § 14 Abs 2 GTelG nur unter bestimmten Voraussetzungen erlaubt, die allesamt nicht eine Sekundärdatennutzung ermöglichen. Eine solche Verwendung ist also nur in Folge der Anonymisierung möglich.

Seit einer Gesetzesnovellierung, die ab dem 30. September 2024 anwendbar ist, ergaben sich Änderungen in § 14 GTelG. In dem novellierten Gesetz wird in § 14 GTelG Abs 3 geregelt, dass „das Verlangen von, der Zugriff auf oder die Verarbeitung von durch ELGA verfügbar gemachten ELGA-Gesundheitsdaten" verboten ist, „sofern diese Vorgangsweisen nicht **unionsrechtlich oder gesetzlich vorgesehen** sind". Hier wird also die Möglichkeit eröffnet, einen Ausnahmetatbestand für das Verbot der Verarbeitung von ELGA-Gesundheitsdaten durch nationale oder europäische Gesetze zu schaffen. Damit beugt diese Novellierung zu erwartenden Konflikten mit dem EHDS vor, der den Zugang zu Gesundheitsdaten ermöglichen soll (siehe dazu Kapitel 8.4). Allerdings könnte auch der DGA eine solche unionsrechtliche Grundlage sein, die ein Ausnahmetatbestand rechtfertigt und die Verarbeitung von ELGA-Daten zu datenaltruistischen Zwecken erlaubt (siehe Kapitel 5.2.). Dies ist allerdings zu diesem Zeitpunkt rechtlich unsicher.

§ 14 GTelG (geändert ab dem 30.09.2024)
(1) Die Verarbeitung (Art. 4 Z 2 DSGVO) von ELGA-Gesundheitsdaten ist nur zulässig, wenn

[104] Milisits/Pfandlsteiner in Aigner/Kletečka/Kletečka-Pulker/Memmer, Handbuch Medizinrecht Kap. I.9 (Stand 1.9.2023, rdb.at).

1. die ELGA-Teilnehmer/innen (§ 15 Abs. 1) gemäß § 18 eindeutig identifiziert wurden,
2. die ELGA-Gesundheitsdiensteanbieter oder die ELGA- und eHealth-Supporteinrichtung gemäß § 19 eindeutig identifiziert wurden und
3. die ELGA-Gesundheitsdiensteanbieter oder die ELGA- und eHealth-Supporteinrichtung gemäß § 21 zur Verarbeitung der ELGA-Gesundheitsdaten berechtigt sind.

(2) Die durch ELGA verfügbar gemachten ELGA-Gesundheitsdaten dürfen personenbezogen ausschließlich

1. für Zwecke gemäß Art. 9 Abs. 2 lit. h DSGVO, ausgenommen für die Zwecke der Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich sowie – unbeschadet der Fälle zulässiger Verarbeitung gemäß § 14 Abs. 3a – ausgenommen für Zwecke der Arbeitsmedizin und die Beurteilung der Arbeitsfähigkeit des Beschäftigten, von
   a. den/die ELGA-Teilnehmer/in behandelnden oder betreuenden ELGA-Gesundheitsdiensteanbietern,
   b. ELGA-Gesundheitsdiensteanbietern, an die ein/eine ELGA-Teilnehmer/in zur Behandlung oder Betreuung von einem ELGA-Gesundheitsdiensteanbieter gemäß lit a zugewiesen wurde
   c. Personen, die die in lit. a und b genannten ELGA-Gesundheitsdiensteanbieter bei der Ausübung ihrer Tätigkeit unterstützen und im konkreten Fall von diesen dazu angewiesen wurden oder
2. zur Wahrnehmung der Teilnehmer/innen/rechte gemäß § 16 von
   a. ELGA-Teilnehmer/inne/n,
   b. deren gesetzlichen oder bevollmächtigten Vertreter/inne/n sowie
   c. durch die ELGA- und eHealth-Supporteinrichtung noch (§ 17) oder
3. zur Wahrnehmung der Betroffenenrechte gemäß dem Kapitel III der DSGVO der ELGA- und eHealth-Supporteinrichtung (§ 17)

verarbeitet werden.

(2a) Die für die Wahrnehmung der ELGA-Teilnehmer/innenrechte erforderliche Entscheidungsfähigkeit (§ 24 Abs. 2 ABGB) wird im Zweifel ab Vollendung des 14. Lebensjahres (mündige Minderjährige) vermutet.

(2b) Soweit berufs- oder sozialversicherungsrechtliche Regelungen die Mitgabe von Daten gemäß § 2 Z 9 lit. a bis f vorsehen, dürfen ELGA-Gesundheitsdiensteanbieter zur Erfüllung dieser Pflichten diese Daten auch über ELGA zur Verfügung stellen. Auf Verlangen des ELGA-Teilnehmers/der ELGA-Teilnehmerin sind diese Daten auch auf andere geeignete Weise zur Verfügung zu stellen.

(3) Das Verlangen von, der Zugriff auf oder die Verarbeitung von durch ELGA verfügbar gemachten ELGA-Gesundheitsdaten sind verboten, sofern diese Vorgangsweisen nicht unionsrechtlich oder gesetzlich vorgesehen sind.

(3a) ELGA-Gesundheitsdiensteanbieter, die Arbeitgeber oder Beschäftiger und in die Behandlung oder Betreuung von ELGA-Teilnehmer/inne/n eingebunden sind, die ihre Arbeitnehmer/innen sind oder von ihnen beschäftigt werden, dürfen deren ELGA-Gesundheitsdaten nur dann verarbeiten, wenn sie

1. diese ELGA-Teilnehmer/innen zuvor ausdrücklich auf die Teilnehmer/innen/rechte gemäß § 16 hingewiesen haben und
2. durch technische Mittel sichergestellt haben, dass innerhalb von ELGA-Gesundheitsdiensteanbietern nur Personen auf ELGA-Gesundheitsdaten zugreifen können, die in den konkreten Behandlungs- oder Betreuungsprozess des jeweiligen ELGA Teilnehmers/der jeweiligen ELGA-Teilnehmerin eingebunden sind.

(4) ELGA-Gesundheitsdiensteanbieter, die ELGA- und eHealth-Supporteinrichtung, deren Auftragsverarbeiter (Art. 4 Z 8 DSGVO) sowie diesen im Sinne des Art. 29 DSGVO unterstellte Personen unterliegen dem Datengeheimnis gemäß § 6 DSG.

5.2. Rechtliche Verbote und Möglichkeiten für die Verarbeitung von Gesundheitsdaten innerhalb von Smart FOX

Wie im vorherigen Kapitel beschrieben, ist eine Weiterverarbeitung von ELGA-Gesundheitsdaten grundsätzlich verboten. Es stellt sich also die Frage, wie eine rechtlich sichere Ausgestaltung einer Gesundheitsdatenspende, wie sie im Forschungsprojekt Smart FOX durchgeführt werden soll, aussehen kann.

Option 1: Weitergabe von ELGA-Daten durch Patient:innen

Eine Möglichkeit besteht darin, dass ELGA-Daten dezentral von den Patient:innen selbst über das ELGA-Portal heruntergeladen und anschließend über das Smart FOX-Patient:innenportal für eine Weiterverarbeitung bereitgestellt werden. Die Patient:innen machen dabei von ihren **Teilnehmer:innenrechten nach § 16 GTelG** Gebrauch. In § 14 Abs 2 Z 3 GTelG wird ausdrücklich festgehalten, dass eine derartige Verarbeitung durch die Teilnehmenden einen rechtmäßigen Vorgang darstellt und daher vom Verarbeitungsverbot des § 14 Abs 2 GTelG ausgenommen ist.

Auch wenn Patient:innen unstrittig auf ihre Daten zugreifen dürfen, bleibt fraglich, ob eine Weitergabe an und Weiterverarbeitung durch Dritte gegen das GTelG verstößt. Eine **grund- und unionsrechtskonforme Auslegung des GTelG** kann jedoch nicht zu dem Ergebnis gelangen, dass das GTelG den Umgang mit den eigenen Gesundheitsdaten verbietet. Auch wenn der Tatbestand der Weitergabe von ELGA-Daten durch Patient:innen an Dritte nicht ausdrücklich im GTelG geregelt ist, würde ein solches Verbot in grundrechtlich geschützte Positionen der Patient:innen eingreifen. Hier sind insbesondere Art 8 GRC (Recht auf Schutz personenbezogener Daten) sowie das daraus ableitbare Recht auf informationelle Selbstbestimmung zu nennen (siehe Kapitel 4.2.3.).[105] Art 8 Abs 1 GRC gewährleistet nicht nur Schutz vor unzulässiger Datenverarbeitung, sondern impliziert auch die Befugnis der betroffenen Person, über die Verwendung ihrer personenbezogenen Daten selbst zu bestimmen. [106] Eine freiwillige und informierte Weitergabe rechtmäßig erlangter Gesundheitsdaten stellt daher keinen Eingriff in das Datenschutzgrundrecht dar, sondern verwirklicht das den Betroffenen durch Art 8 GRC gewährleistete Recht, über die Verwendung ihrer personenbezogenen Daten selbst zu entscheiden.

[105] *Calliess et al*, EUV/AEUV Art. 8 Rn. 5.
[106] *Calliess et al*, EUV/AEUV Art. 8 Rn. 10.

In diese Richtung weisen auch die Betroffenenrechte der DSGVO. Das Recht auf Datenportabilität nach Art 20 Abs 1 DSGVO, das den Betroffenen das Recht einräumt, personenbezogene Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese an andere Verantwortliche zu übermitteln, ist hier jedoch nicht unmittelbar anwendbar. Art 20 DSGVO greift nur, wenn „die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht". Die Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten durch ELGA-Gesundheitsdiensteanbieter stützt sich jedoch auf gesetzliche Verpflichtungen (§ 13 Abs 3 iVm § 20 Abs 1 und 2 GTelG 2012) sowie auf Gründe des erheblichen öffentlichen Interesses gemäß Art 9 Abs 2 lit g bis j DSGVO.[107]

Auch wenn Art 20 DSGVO daher nicht unmittelbar anwendbar ist, folgt aus Art 8 GRC, dass Betroffenen jedenfalls nicht untersagt werden darf, ihre rechtmäßig erlangten personenbezogenen Daten freiwillig an Dritte weiterzugeben. Eine gegenteilige Auslegung des GTelG würde einen nicht ausdrücklich vorgesehenen und unionsrechtlich nicht gerechtfertigten Eingriff in das Grundrecht auf Datenschutz darstellen. Das GTelG ist daher im Lichte von Art 8 GRC grundrechts- und unionsrechtskonform dahingehend auszulegen, dass eine solche Weitergabe durch Patient:innen zulässig bleibt.

Eine noch offene rechtliche Frage betrifft jedoch die Zulässigkeit einer Datenverarbeitung im Auftrag der Patient:innen durch Dritte zum Zweck der Wahrnehmung von Betroffenenrechten. Dies wäre im Forschungsprojekt Smart FOX der Fall, wenn Patient:innendaten nicht durch die Betroffenen selbst bereitgestellt, sondern mit deren ausdrücklicher Einwilligung von Dritten abgerufen und verarbeitet werden. Fraglich ist, ob in diesem Fall weiterhin auf die Ausnahme nach § 14 Abs 2 Z 3 GTelG abgestellt werden kann. Die Ausübung von Betroffenenrechten durch Dritte wird in der DSGVO weder ausdrücklich erlaubt noch untersagt. [108]

Aus systematischer und grundrechtlicher Sicht spricht jedoch vieles dafür, Patient:innen dabei zu unterstützen, ihre Gesundheitsdaten – ihrem erklärten Willen entsprechend – für Forschungszwecke verfügbar zu machen. Eine **ausdrückliche Einwilligung** der Patient:innen erscheint ausreichend, um eine solche Verarbeitung als Ausfluss des Rechts auf informationelle Selbstbestimmung als auch des unionsrechtlich gewährleisteten Datenschutzgrundrechts nach Art

[107] *OV*, Datenschutz | ELGA - Meine elektronische Gesundheitsakte https://www.elga-online.gv.at/web-gui/public/datenschutz.xhtml (aufgerufen am 07.01.2026).
[108] *Funke*, Die Vereinbarkeit von Data Trusts mit der Datenschutzgrundverordnung (DSGVO) https://algorithmwatch.org/de/gutachten-data-trusts-dsgvo/ (aufgerufen am 10.02.2025).

8 GRC zu qualifizieren. Es ist nicht ersichtlich, weshalb die technische Bereitstellung der Daten zwingend durch die Betroffenen selbst erfolgen müsste und nicht auch durch von ihnen ausdrücklich beauftragte Dritte erfolgen kann.

Zusammenfassend ist festzuhalten, dass die Weitergabe von ELGA-Daten durch Patient:innen zum Zweck der Datenspende, sofern diese Daten auf Grundlage der Teilnehmer:innenrechte gemäß § 16 GTelG rechtmäßig erlangt wurden, unter Berücksichtigung von Art 8 GRC rechtlich überzeugend begründbar ist, wenn auch nicht in allen Aspekten abschließend geklärt. Eine technische Umsetzung im Sinne einer faktischen Datenportabilität, bei der Betroffene lediglich in die Weitergabe einwilligen und diese sodann durch Verantwortliche oder beauftragte Dritte umgesetzt wird, erscheint aus praktischer Sicht wünschenswert, ist jedoch auch aus rechtlicher Perspektive derzeit nicht völlig unumstritten.

Option 2: Verwendung von ELGA-standardisierten Daten

Eine weitere Option verzichtet vollständig auf die Verarbeitung von ELGA-Daten im rechtlichen Sinn. Stattdessen werden **Gesundheitsdaten** herangezogen, die von Partner:innen des Forschungsprojekts Smart FOX, wie den Tirol Kliniken GmbH und den IT-Services der Sozialversicherung GmbH, bereitgestellt werden. Diese Daten liegen bereits in einem strukturierten Format vor, das perspektivisch eine spätere Integration in den ELGA-Datenraum ermöglicht.

Auf technischer Ebene fehlen diesen Datensätzen bestimmte **ELGA-spezifische Charakteristika**, weshalb sie in der bestehenden Praxis nicht als ELGA-Gesundheitsdaten qualifiziert werden. Die Verarbeitung dieser Daten, die hier als „ELGA-standardisierten Daten“ bezeichnet werden, unterliegt daher nicht den spezifischen Regelungen des GTelG, insbesondere nicht den dort vorgesehenen Verarbeitungsbeschränkungen, Teilnehmer:innenrechten oder Speicherfristen. Unberührt bleibt jedoch die Anwendbarkeit der DSGVO, sodass auch für diese Datenverarbeitung eine tragfähige Rechtsgrundlage erforderlich ist. Innerhalb von Smart FOX bildet die Einwilligung der Patient:innen diese Rechtsgrundlage.

Diese Möglichkeit zur Verarbeitung entspricht der gängigen Praxis und beschreibt, wie ELGA-standardiserte Daten bislang sowohl in früheren als auch in parallelen Forschungsprojekten durch Konsortialpartner:innen verarbeitet wurden. Einziger wesentlicher Einwand gegen diese Vorgehensweise besteht darin, dass die rechtliche Einordnung von ELGA-standardisierten Daten als Nicht-ELGA-Daten bislang nicht abschließend geklärt ist. Weder besteht hierzu eine explizite gesetzliche Regelung noch liegt eine einschlägige höchstgerichtliche Entscheidung vor. Eine verbindliche gesetzliche Einordnung wäre daher aus Gründen der Rechtssicherheit wünschenswert.

Aus rechtlicher Sicht ist sowohl Option 1 als auch Option 2 denkbar, um eine Datenspende von Gesundheitsdaten in Österreich zu ermöglichen - wenn auch beide mit einer gewissen Rechtsunsicherheit einhergehen. Aus ethischer Sicht sind beide Möglichkeiten unter den richtigen Rahmenbedingun vertretbar, da in jedem Fall die Einwilligung der Patient:innen eingeholt wird. Letztendlich obliegt es dem Konsortialpartner:innen von Smart FOX, die Vor- und Nachteile abzuwägen und die technische und organisatorische Umsetzbarkeit einzuschätzen.

5.3. Datenaltruismus unter dem DGA

Der „Datenaltruismus“ hat mit dem DGA Einzug in die europäische Digitalpolitik genommen. Das Instrument des Datenaltruismus soll freiwilligen Datenaustausch fördern (Art 1 Abs 1 DGA).

Das Ziel des Datenaltruismus ist laut Art 2 Abs 16 DGA, Daten freiwillig für Zwecke des Gemeinwohls zur Verfügung zu stellen – sei es für wissenschaftliche Forschung, soziale Innovationen oder andere gesellschaftliche Ziele. Die Daten können entweder auf Grundlage der **Einwilligung** nach Art 6 Abs 1 DSGVO von Individuen **oder** durch die **Erlaubnis** von Dateninhaber:innen bereitgestellt werden. In beiden Fällen wird für die Daten keine Gebühr verlangt, die über die durch die Datenbereitstellung entstandenen Kosten hinausgeht. Organisationen, die als datenaltruistische Organisationen anerkannt werden wollen, müssen sich zuerst registrieren, wie in Art 19 DGA beschrieben. Voraussetzung hierfür ist nach Art 18 DGA, dass sie:

- **datenaltruistische Tätigkeiten** ausführen, also im Datennutzung im Sinne des Gemeinwohls fördern;
- eine **Rechtspersönlichkeit** haben;
- **unentgeltlich und unabhängig** handeln; sowie
- funktionell und organisatorisch datenaltruistische Tätigkeiten von anderen **Tätigkeiten** der Organisation **trennen**.

Darüber hinaus bestehen erhöhte Transparenzverpflichtungen an datenaltruistische Organisationen, die genaue **Aufzeichnungen** führen müssen, z.B. über die Akteur:innen, an die Daten vermittelt wurden, und den Zweck, Zeitpunkt und Dauer der Datenverarbeitung sowie jährliche **Berichte** über ihre Tätigkeiten inklusive Informationen über die Einnahmequellen der altruistischen Organisation veröffentlichen müssen (Art 20 DGA).

Es ist die Aufgabe von datenaltruistischen Organisationen, Betroffene, die ihre personenbezogenen Daten bereitstellen, klar und umfassend über die Zwecke der Datenverarbeitung zu **informieren** und

Tools für die Einholung und den Widerruf von Einwilligungen bereitzustellen (Art 23 Abs 1 und 3 DGA). Art 23 Abs 4 und 5 DGA besagen zudem, dass datenaltruistische Organisationen angemessene Sicherheitsvorkehrungen für den Schutz der personenbezogenen Daten treffen und bei Datenverstößen die Betroffenen informieren müssen. Initiiert von der Europäischen Kommission soll ein Europäisches Einwilligungsformular für Datenaltruismus erarbeitet werden, dass durch einen modularen Aufbau für verschiedene Zwecke angepasst werden kann (Art 25 Abs 1 und 2 DGA). Das Formular ist jedoch bisher noch nicht verfügbar.

Laut Art 24 DGA wird die Einhaltung der Anforderungen von öffentlichen Stellen überwacht, die jeder Mitgliedsstaat benennt. Österreich hat noch nicht bekannt geben, welche Behörde dies hierzulande übernimmt.[109] Zudem können die Mitgliedsstaaten zusätzliche organisatorische oder technische Regelungen festlegen, sowie eine Datenaltruismus-Strategie, die die Datenweitergabe erleichtern (Art 16 DGA). Welche Form der Datennutzung im öffentlichen Interesse ist, müssen nationale Gesetz regeln.[110]

Eine Organisation, die Datenspenden von Gesundheitsdaten zum Zwecke von wissenschaftlicher Forschung ermöglicht, wie in Smart FOX vorgesehen, kann sich im Prinzip als datenaltruistische Organisation registrieren, wenn die oben genannten Voraussetzung erfüllt werden. Da dies evtl. ein Ergebnis aus dem Forschungsprojekt Smart FOX sein könnte, werden die Voraussetzungen in Kapitel 8.2 ausgeführt.

5.4. Zur Datenspende motivieren: Datenspende gegen Vergütung

Smart FOX untersucht Motivationsfaktoren zur Datenspende. Es ist daher auch notwendig, finanzielle Motivationen und Formen der Gegenleistung für die Datenspende aus rechtlicher und ethischer Sicht zu evaluieren. Rechtlich und ethisch stellen sich bei einem Angebot der Gegenleistungen für eine Datenspende schwierige Fragen – im Rahmen des Forschungsprojekts Smart FOX bestehen keine Absichten, Entgelt für Daten anzubieten. Es stellt sich jedoch, im Rahmen eines langfristigen Kommerzialisierungsplans, die Frage, ob dies eine Option wäre. Dementsprechend wurde diese Frage auch an den Smart FOX Legal Helpdesk herangetragen und in den Learning Clubs besprochen. Auch perspektivisch wurde vom Team der UNIVIE davon abgeraten,

[109] *Europäische Kommission*, National competent bodies and authorities under the Data Governance Act https://ec.europa.eu/newsroom/dae/redirection/document/98966 (Stand 24.11.2025).
[110] Siehe Definition „Datenaltruismus“ in Art 2 Abs 16 DGA.

Vergütung als Motivation zur Gesundheitsdatenspende zu verfolgen. Die ethischen und rechtlichen Gründe dafür sind hier zusammengefasst dargestellt.

Ob Menschen für ihre Gesundheitsdaten bezahlt werden können, wird heftig diskutiert.[111] Es gibt einerseits die Tradition der Diskussion in der Medizinethik über die Bezahlung für die Teilnahme an klinischen Studien, aus denen notwendigerweise auch Daten verarbeitet werden, und andererseits die Diskussion aus dem Data-Ethics-Feld zur Bezahlung für Daten. Beide Perspektiven, aber insbesondere die Fragen aus der Data-Ethics-Perspektive sind für Smart FOX äußerst relevant und werden daher in diesem Kapitel näher ausgeführt. Für **Datenaltruismus** unter dem DGA enthält der DGA eine eindeutige Klarstellung, dass diese entgeltlos sein muss, denn die Definition von Datenaltruismus beinhaltet, dass dieser erfolgt „ohne hierfür ein Entgelt zu fordern oder zu erhalten, das über eine Entschädigung für die (betroffenen Personen oder anderen Dateninhabern) durch die Bereitstellung ihrer Daten entstandenen Kosten hinausgeht," (Art 2 Abs 16 DGA). Ob eine Datenspende bzw. Datenbereitstellung gegen Entgelt dennoch stattfinden können, ist dadurch nicht geklärt. Daher werden folgend in Kürze einige generelle Aspekte zum „Kauf" von Daten analysiert.

Die Bezahlung für die Teilnahme an klinischen Studien wird ethisch heftig diskutiert, insbesondere da es durchaus Fälle gibt, in welchen Menschen von dem Einkommen aus der Teilnahme an klinischen Studien finanziell abhängig sind.[112] Dies ist für Smart FOX jedoch erst relevant, falls es in der Zukunft nicht nur um die Motivation zur Datenspende gehen sollte, sondern auch um die Motivation zur Teilnahme an bestimmten Studien, aus welchen Daten dann gespendet werden sollen. Derzeit konzentriert sich das Forschungsprojekt auf die Weiterverwertung von bereits vorhandenen ELGA-standardisierten Daten. Daher geht es bei den Risiken, die für Einzelne entstehen können, nicht um die möglichen negativen Effekte einer klinischen Studie, sondern um Risiken, die aus der Datenverarbeitung resultieren.

In der Praxis passiert es oft, dass Daten und Geld die Hand wechseln. Meist sind es aber nicht die Betroffenen selbst, welche ihre Daten monetarisieren, sondern z.B. sogenannte **Data Broker**, welche Daten sammeln und verkaufen.[113] Rechtlich fragwürdig ist dabei jedoch oft, ob es eine gültige

[111] Siehe z.B. *Prainsack/Forgó*, Why paying individual people for their health data is a bad idea, Nature Medicine 28, 2022, 1989; *Pal*, Health Data as a Commodity: Implications and Opportunities, SSRN 2025; *Sheaff, Ellis-Paine, Exworthy, Hardwick, Smith*, Commodification and healthcare in the third sector in England: from gift to commodity – and back?, TFO Collections, 2023.
[112] *Fisher/McManus/Kalbaugh/Walker*, Phase I trial compensation: How much do healthy volunteers actually earn from clinical trial enrollment?- Jill A Fisher, Lisa McManus, Julianne M Kalbaugh, Rebecca L Walker, Clinical Trials 18, 2021.)
[113] *Urbano*, The untamed and discreet role of data brokers in surveillance capitalism: A transnational and interdisciplinary overview, Internet Policy Review 11, 2022.

Rechtsgrundlage für die Verarbeitung gibt, ob die Grundsätze der DSGVO eingehalten werden und ob Betroffene ihre Rechte geltend machen können. Die EU hätte also zwar in der Theorie Instrumente in der DSGVO, um die Praktiken von Data Brokern einzuschränken, welche international zum Zeitpunkt des Inkrafttretens der DSGVO auch sehr gelobt wurden. Die EU sieht sich jedoch oft bei Data Brokern, welche in einem Drittland angesiedelt sind, mit einem Durchsetzungsproblem konfrontiert.[114] Aus dieser Praktik des Verkaufs von Daten wird oft das Argument hergeleitet: Daten sind sowieso bereits käuflich und kommodifiziert – wenn also Betroffenen Geld für ihre Daten angeboten wird, werden diese zumindest davon profitieren. Aus dieser Logik entstehen oft Argumente, Menschen für ihre Daten zu bezahlen, wie etwa oft für Google-, Amazon- oder Facebook-Daten vorgeschlagen.[115] Während diese auf den ersten Blick der Selbstbestimmung der Betroffenen dienlich erscheinen können, spricht viel dafür, dass solche Praktiken problematisch sind. Unter anderem muss Folgendes bedacht werden:

- Informationsasymmetrien und unvorhergesehene Risiken: Betroffene, die ihre Daten verkaufen, können evtl. nicht wirklich als informiert bezeichnet werden, selbst wenn eine Einwilligung vorliegt. Durch vorhandene Informationsasymmetrien wissen Einzelne oft nicht genau, wozu ihre Daten verwendet werden. Auch gibt es Risiken, welche schwer vorherzusehen sind und über die Betroffene nicht immer aufgeklärt werden – etwa, wenn aus einfachen Konsumdaten oder Google-Search-Daten Gesundheitsdaten abgeleitet werden, oder wenn Spendende nicht genau evaluieren können, wie sicher das technische Umfeld ist, in welchem ihre Daten gespeichert werden. Ein für Smart FOX relevantes Beispiel: Betroffene wissen möglicherweise nicht, dass z.B. aus eMedikationsdaten Schlüsse über ihre Lebensdauererwartung oder psychische Gesundheit gezogen werden können. Es ist daher sowieso bereits schwer von einer informierten Einwilligung zu sprechen. Wenn noch hinzukommt, dass auf potenzielle Spender:innen Druck durch das Angebot eines Entgelts erzeugt wird, so kann es sehr schwer sein, mit einer freiwilligen, informierten Einwilligung als Rechtsgrundlage zu argumentieren.
- Ungleichheiten und Kommodifizierung: Der Kauf und Verkauf von Daten führt zu einer Kommodifizierung der Privatsphäre,[116] welche oft als unethisch betrachtet wird, auch da es somit ökonomisch benachteiligte Gruppen sind, welche unter Druck stehen, ihre Privatsphäre

[114] *Yeh*, Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers, Telecommunications Policy 42, 2018.
[115] *Neuman*, Why We Should Get Paid for Our Online Data, TIME 2023, https://time.com/6340676/get-paid-personal-online-data-essay/.
[116] *Bilic/Zitko*, Personal data as pseudo-property: Between commodification and assetisation, European Journal of Communication 39(5), 2024.

zu verkaufen. Dadurch werden systemische Ungleichheiten verstärkt. Weiters kann eine finanzielle Abhängigkeit vom Verkauf von Daten entstehen.

- Schutz von Betroffenen: Wenn Daten also für Geld verkauft werden, kann der Eindruck entstehen, dass Betroffene keine Rechte mehr über ihre Daten haben. Dies stimmt jedoch rechtlich nicht (z.B. können Betroffenenrechte unter der DSGVO sehr wohl noch ausgeübt bzw. nur nach nationalen und europäischen Rechtsvorschriften eingeschränkt werden). Es ist auch ethisch für eine Kultur der Selbstbestimmung und des verantwortungsvollen Umgangs mit Daten nicht förderlich, wenn diese gehandhabt werden, als könnten sie verkauft werden, und Betroffenen dadurch ihre Rechte abgesprochen werden.
- Accuracy-Problem: Der Kauf von Daten kann zu einer Verzerrung dieser führen, da möglicherweise dadurch Anreize für die Generierung von vergüteten Daten geschaffen werden. Wenn also z.B. Daten für eine bestimmten seltenen Krankheit teuer verkauft werden können, kann dies zur Fälschung von Daten und zu irreführenden Zahlen führen.[117]
- Langfristige Erosion des Altruismus: Wie z.B. Prainsack und Forgó argumentieren, führt die Bezahlung für Daten dazu, dass Menschen langfristig nicht bereit sind, ihre Daten ohne Bezahlung zur Nutzung anzubieten. Daraus entstehen Vorteile für Großkonzerne und sehr wahrscheinlich Nachteile für kleine Unternehmen und für die Forschung. Dies ist wiederum nicht zielführend für den gesellschaftlich-verantwortlichen Umgang mit Daten.[118]

Im rechtlichen Rahmen gibt es hier eine eindeutige Klarstellung durch den DGA: Die Definition von Datenaltruismus im DGA enthält die klare Einschränkung, dass die Nutzung von Daten „ohne hierfür ein Entgelt zu fordern oder zu erhalten“ erfolgen muss (Art 2 Abs 16 DGA). In ErwGr 45 DGA wird weiter ausgeführt: „Die betroffenen Personen sollten eine Entschädigung nur für diejenigen Kosten erhalten können, die ihnen durch die Bereitstellung ihrer Daten für Ziele von allgemeinem Interesse entstehen.” Da sich das Forschungsprojekt Smart FOX an dem europäischen Konzept des Datenaltruismus orientiert, wäre es nicht sinnvoll bzw. schlüssig, Entgelt für Daten anzubieten. Für die Zukunft von Smart FOX nach Ablauf der Projektlaufzeit gilt zu bedenken, dass ein Angebot von Entgelt die Zertifizierung als datenaltruistische Organisation unter dem DGA ausschließen würde (siehe Kapitel 8.2) und dass es viele ethische Argumente gegen den Kauf und Verkauf von Gesundheitsdaten gibt.

Ein rechtlich unklarer Bereich in Bezug auf Entgelt für Daten sind Praktiken, welche nicht direkt Geld für Daten austauschen, sondern die z.B. einen Service im Austausch für Daten anbieten oder billigere

[117] *Prainsack/Forgó*, Why paying individual people for their health data is a bad idea, Nature Medicine 28, 2022, 1989.
[118] *Prainsack/Forgó*, Nature Medicine.

Preise für eine andere Leistung.[119] So sind finanzielle und nicht-finanzielle **Gegenleistungen** also nicht ganz klar in zwei Kategorien differenzieren, da z.B. das Angebot eines besseren Services nicht direkt eine finanzielle Gegenleistung ist, jedoch etwas darstellt, was oft auch mit Geld statt mit Daten hätte erkauft werden können. So fördern auch andere Formen der Gegenleistung evtl. die Kommodifizierung der Privatsphäre und die Erosion des Altruismus. Auch bei nicht-finanziellen Gegenleistungen gilt es also, diese vorsichtig abzuwägen.

Zuletzt gilt es noch in Betracht zu ziehen, dass es leicht passieren kann, dass Gegenleistungen bzw. positive Effekte im breiteren Sinn versprochen werden. Beispielsweise ist es in Einwilligungsformularen schwierig, Risiken und Vorteile möglichst objektiv zu beschreiben.[120] Es sollte hier darauf geachtet werden, keine überschwänglich positiven **Formulierungen** zu nutzen bzw. nicht die Einwilligungsformulare dazu zu nutzen, zur Datenspende zu motivieren. In diesem Aspekt können sich Forschende auf eine lange Tradition der Forschung mit menschlichen Teilnehmenden (also z.B. der qualitativen oder der medizinischen Forschung) stützen, welche Einwilligungsprozesse so entwickelt haben, dass Teilnehmenden nicht zu viel zu versprochen wird. Die Partner:innen des Forschungsprojekts Smart FOX, welche häufig **Einwilligungsprozesse** entwerfen, bringen hier auch ihre Erfahrungen und Expertise in das Projekt ein (beispielsweise durch die Involvierung des Patient:innenbeirats des LBI-DHPS), was die Entwicklung der Einwilligungsprozesse unterstützt. Die im Rahmen vom Forschungsprojekt Smart FOX entwickelten Patient:inneninformationensmaterialien haben hier eine komplexe Rolle: Sie bewerben nämlich einerseits den Zweck von Smart FOX, um Patient:innen zu erreichen; andererseits dienen die Materialien auch dazu, transparent zu informieren und über Risiken aufzuklären. Im Zuge der Vorbereitung von Survivors AT und LBI-DHPS und Feedback von Partnern auf diese Materialien wurde also hervorgehoben, dass diese die informierte Einwilligung nicht ersetzen und dass dennoch auch in den Materialien darauf geachtet werden muss, die Risiken und mögliche Vorteile objektiv zu beschreiben. Formulierungen, die z.B. einen positiven Effekt auf die eigene Gesundheit versprechen oder den Eindruck erwecken, dass die Einzelperson von der Spende der eigenen Daten direkt profitieren wird, sind zu vermeiden.

Bezahlung für Daten, abgesehen von einer Aufwandsentschädigung, im Gegenzug für Behandlung ist für Smart FOX keine Option, dies ist jedoch auch keine Frage, die sich derzeit stellt – das Forschungsprojekt plant derzeit nicht, medizinische Studien durchzuführen. Von einer **Bezahlung für**

[119] z.B. „Pay or Okay" Modelle, in welchen es eine Zahlversion für online Services gibt ohne Tracking und Werbung und eine Gratis-Version mit Tracking und Werbung.
[120] *Kahrass/Bossert/Schürmann/Strech*, Details of risk–benefit communication in informed consent documents for phase I/II trials, 2021.

die Weitergabe von bereits vorhandenen Daten ist abzuraten. Sowohl aus datenschutz- als auch aus medizin-, grundrechtlicher und ethischer Sicht könnte dies problematisch sein. Unter die DGA-Definition von Datenaltruismus würde die Zurverfügungstellung von Daten gegen Entgelt auch nicht mehr fallen, wodurch auch nicht dem Wesen der Datenspende bzw. des Datenaltruismus entsprochen würde, den Smart FOX verfolgt.

Bei nicht-finanziellen Gegenleistungen ist der rechtliche Rahmen sehr genau in Betracht zu ziehen und es sollten dabei nicht nur kurzfristige Probleme bedacht werden, sondern auch die langfristige Mission von Smart FOX und des Datenaltruismus generell. Allgemein ist einem Angebot von Gegenleistungen für eine Datenspende immer zumindest entgegenzuhalten, dass solche Angebote langfristig den Datenaltruismus erodieren.

6. Einbindung von Patient:innen in die Projektarbeit (Beitrag von LBI DHPS)

Das nachfolgende Unterkapitel 6. wurde vom Team des LBI DHPS (Elisabeth Klager, MSc und Benjamin Schuster, BSc) verfasst.

Die Gesundheitsdatenspende wirft neben technischen und organisatorischen auch ethische und gesellschaftliche Fragen auf, die im Dialog mit den Betroffenen thematisiert werden müssen. Aus diesem Grund ist **die Einbindung von Patient:innen** von zentraler Bedeutung in Smart FOX. Sie stellt sicher, dass Bedürfnisse, Ängste und Erwartungen frühzeitig berücksichtigt werden, was für die Akzeptanz und den langfristigen Erfolg der Gesundheitsdatenspende unerlässlich ist. Ein Projektteam von 13 Mitgliedern des österreichischen Patient:innenbeirats [121] hält regelmäßige Meetings ab, um wichtige Punkte rund um die Gesundheitsdatenspende in Tiefe zu diskutieren. Die bisherigen Erkenntnisse geben Einblicke in die zentralen Fragestellungen der Thematik aus Patient:innensicht und bieten Ansatzpunkte für die weitere Projektarbeit.

6.1.Unsicherheiten und Bedenken zur Nutzung der Daten vom Patient:innenbeirat

Ein Unsicherheitsfaktor ist die Frage, wer welche Daten wofür nutzt. Im Vergleich zu anderen Spenden existiert die Angst, dass die Spende theoretisch gegen den Spender verwendet werden kann, beispielsweise bei der Jobsuche, bei einer Kreditvergabe oder bei Versicherungsprämien.

Außerdem sind Bedenken aufgekommen, dass von der Spende Pharmaunternehmen einen Gewinn erzielen könnten „ohne etwas zurückzugeben“. In diesem Zusammenhang muss man wohl die Angst vor „Big Pharma“ in der Bevölkerung beachten.

Schließlich ist auch die Idee der Gemeinnützigkeit aufgekommen, also dass Unternehmen, die durch die Datenspenden höhere Gewinne erzielen, einen Teil davon an gemeinnützige Zwecke abgeben

[121] https://www.patientenbeirat.at/index.php.

müssen. Es ist zu klären, wie diese Gemeinnützigkeit konkret aussehen könnte und ob man dadurch eventuell auch mehr Leute zum Spenden bewegen kann.

6.2. Dauer und Umfang der Spende (Dauerauftrag oder Einzelspende)

Für manche Menschen könnte die Dauer der Nutzung ihrer Daten einen Unterschied machen. Ist es immer ein laufendes Abziehen von Daten oder ist eine einmalige Spende möglich? Macht das dann noch Sinn oder ist gerade die Kontinuität so essenziell?

Eine Frage ist auch ob es die Möglichkeit geben wird, nur die Daten bestimmter Ereignisse zu spenden, zum Beispiel jene einer Hüftoperation schon, die einer Abtreibung aber nicht.

6.3. Spendendanimation

Um spendenwillige Menschen tatsächlich zur Spende zu bewegen, müssen gute Orte oder Events gefunden werden, um den Leuten ein niederschwelliges Angebot für eine Einwilligung zu machen. Ein Beispiel für ein Event wäre der Krebsforschungslauf. Dort konnte man sich letztes Jahr vor Ort mit einer Probe für eine Stammzellenspende registrieren. Die Kombination von niederschwelligem Angebot und einer Zusammenkunft von vermutlich tendenziell spendenwilligeren Menschen hat funktioniert.

Geeignete Orte wären beim Hausarzt, in der Apotheke, in PVEs, … In diesem Zusammenhang ist es wichtig zu klären wie man skeptisches („älteres“?) von dem Mehrwert der Gesundheitsdatenspende überzeugen kann.

Es wird wichtig sein, mit Role Models, bekannten Personen und Influencern an einem Vertrauensaufbau in der Öffentlichkeit zu arbeiten.

6.4. Begriff „Spende“

Es gab eine Diskussion darüber, ob der Begriff Spende überhaupt der richtige ist. Denn wenn man spendet, hat man normalerweise danach weniger von etwas, z.B. wenn man Geld spendet, hat man nachher weniger. Wenn man Daten spendet, verliert man nichts dabei. Ist der Begriff „Daten teilen“ daher vielleicht treffender?

Ein Gegenargument war, dass der Begriff Spenden doch passend ist, da sehr wohl etwas hergegeben wird, nämlich Daten. Dabei wird auch die Kontrolle über diese abgegeben und an die Forschung gespendet.

In diesem Zusammenhang ist auch der Begriff der Investition als Vergleich angeführt worden. Auch hier weiß man nicht was genau daraus wird, aber potenziell entsteht ein Nutzen. Die Datenspende ist somit eine Investition in die Zukunft der Medizin.

6.5. Erwartungshaltung an persönlichen Nutzen

Damit Bürger:innen eine realistische Erwartungshaltung gegenüber einer Plattform zur Gesundheitsdatenspende entwickeln, ist es entscheidend, dass sie deren genaue Funktion verstehen. Bevor die Motivation zur Teilnahme gefördert werden kann, muss zunächst Klarheit darüber bestehen, was eine Gesundheitsspende für das Individuum tatsächlich bedeutet. Trotz ausführlicher Informationen zum Projekt und seiner Funktionsweise nahmen Patient:innen häufig an, dass ihre gespendeten Gesundheitsdaten unmittelbar dazu genutzt werden könnten, um individuelle Behandlungen zu verbessern und Doppelbefunden zu vermeiden. Zwar könnte dies langfristig eine mögliche Entwicklung sein, doch es entspricht nicht dem aktuellen Ziel der Gesundheitsspende. Ohne dieses Verständnis entsteht eine Diskrepanz zwischen Erwartung und Realität, die selbst eine anfänglich hohe Motivation schwächen kann.

6.6. Wichtigkeit von Aufklärung und Information

Aus diversen Diskussionsrunden in den letzten Monaten ist klar geworden, dass sich Laien oft schwer tun mit abstrakten Begriffen wie „anonymisierte“ oder „pseudonymisierte“ Daten. Ihre erste Reaktion ist häufig: „Daten müssen auf jeden Fall anonym sein!“ Gleichzeitig wünschen sie sich aber Transparenz darüber, wofür ihre Daten genutzt werden, oder dass sie theoretisch kontaktiert werden können, wenn neue, bessere Behandlungsmöglichkeiten verfügbar sind – ein klarer Widerspruch. In den bisherigen Gesprächen zeigt sich, dass es unterschiedliche Ausgangshaltungen gibt: Einige Menschen sind von Beginn an positiv eingestellt, während viele zunächst skeptisch sind und Fragen haben. Doch in Gesprächen und Diskussionen wird oft deutlich, dass sich ihr Verständnis mit der Zeit verändert und der Mehrwert immer klarer wird. Persönlicher Austausch braucht jedoch Zeit – eine Ressource, die fehlt, wenn es darum geht, große Teile der Bevölkerung zu erreichen und positiv zu stimmen. Deshalb muss die Kommunikation (egal ob Materialen, Kampagnen etc) präzise

und zielgerichtet sein: die richtigen Botschaften, zur richtigen Zeit, am richtigen Ort – vermittelt durch vertrauenswürdige Personen und Institutionen.

7. Datenspendeszenarien in Smart FOX

Im folgenden Abschnitt werden konkrete Fragestellungen bearbeitet, die sich in Hinblick auf Datenspendeszenarien stellen (könnten). Die Szenarien wurden vorab über ein Online-Umfragetool und in der Diskussion im Rahmen der Smart FOX Learning Clubs durch Konsortialpartner:innen angeregt. Zu beachten ist, dass vor allem dieser Teil des Data Governance Frameworks im Verlauf der Forschungsprojekts mit der Weiterentwicklung der Workpackage-Outcomes auch um weitere, neue rechtliche und ethische Fragestellungen und Szenarien erweitert wurde.

7.1. Gerichtete und ungerichtete Datenspende

Im Forschungsprojekt Smart FOX sind zwei Formen der Datenspende geplant, die zu unterschiedlichen Graden im Rahmen des Projekts bereits durchgeführt werden konnten: die gerichtete und die ungerichtete Datenspende. Technische Details zur Vorgangsweise in beiden Fällen wurden in WP3 und WP4 entwickelt, eine kurze Zusammenfassung davon ist jedoch:

- Eine **gerichtete Datenspende** findet in einem bereits definierten bzw. neu definierten Forschungskontext statt. Ein Forschungskontext kann z.B. ein klinisches Register oder eine klinische Studie sein, in welcher die Genehmigung für die Datennutzung eindeutig etabliert ist, etwa durch die Zustimmung einer Ethikkommission inkl. Informed Consent.
- Eine **ungerichtete Datenspende** findet in einem noch nicht definierten Forschungskontext statt. Daten werden von Patient:innen oder Bürger:innen mit der Absicht bereitgestellt, diese einem zukünftigem Forschungskontext zur Verfügung zu stellen. Die Patient:innen bzw. Bürger:innen stimmen also zu, dass die Daten unter festgelegten Konditionen, aber in bis dato undefinierten Kontexten genutzt werden können. Die tatsächliche Datennutzung benötigt aber eine weitere Genehmigung, z.B. durch Ethikkommission.

Was zunächst aufgeklärt werden muss, ist, dass manche Initiativen nur eine ungerichtete und zeitlich **uneingeschränkte Datenspende** als solche definieren. Aus dieser Interpretation entstehen dementsprechend oft Missverständnisse. In einer von Algorithm Watch vorgeschlagenen Definition ist z.B. Datenspende “the permanent provision of data for context-specific information-gathering

processing, without any direct incentive in return and without the donating party necessarily having any influence on the concrete use in the individual case".[122]

Im DGA ist dies jedoch nicht der Fall und es gibt auch sonst (vor allem rechtlich) keinen Grund, die Datenspende so zu definieren. Datenaltruismus in Bezug auf personenbezogene Daten wird im **DGA** nur als „die freiwillige gemeinsame Nutzung von Daten auf der Grundlage der Einwilligung betroffener Personen zur Verarbeitung der sie betreffenden personenbezogenen Daten (…), ohne hierfür ein Entgelt zu fordern oder zu erhalten, das über eine Entschädigung für die ihnen durch die Bereitstellung ihrer Daten entstandenen Kosten hinausgeht, für Ziele von allgemeinem Interesse gemäß dem nationalen Recht, wie (…) die wissenschaftliche Forschung im allgemeinen Interesse", definiert (Art 2 Abs 16 DGA).

Im Forschungsprojekt Smart FOX ist eine der Zielsetzungen, dass die **Kontrolle über die Zwecke der Datenspende** bei den Betroffenen bleibt. Einerseits ist daher die gerichtete Datenspende für einen vorbestimmten Zweck eingeschränkt und andererseits werden auch bei der ungerichteten Datenspende Konditionen definiert – Betroffene können jederzeit ihre Daten löschen bzw. kontrollieren, wo diese hinfließen.

Dies ist auch aus rechtlicher Sicht wichtig. Zwar versucht der DGA den Datenaltruismus zu fördern, der neue Rechtsakt rüttelt jedoch nicht an den Vorgaben der DSGVO und führt auch nicht etwa eine Privilegierung für datenaltruistische Verarbeitungen ein. Der DSGVO nach gibt es bei der Gestaltung der gerichteten und ungerichteten Spende im Forschungsprojekt Smart FOX jedenfalls die folgenden zwei Aspekte zu beachten: die freiwillige Einwilligung und die Einhaltung der Betroffenenrechte.

Kapitel 4.1.2.6. erklärt bereits die Einwilligung und die Rechtslage bezüglich des sogenannten „broad consent". Sollte nun die ungerichtete Einwilligung auf einer Form des „broad consent" beruhen, so gibt es dafür in Österreich in § 2d Abs 3 FOG die entsprechende Rechtsgrundlage. Laut dieser Rechtsvorschrift darf die Angabe eines Zwecks durch die Angabe eines Forschungsbereichs, mehreren Forschungsbereichen oder von Forschungsprojekten oder von Teilen von Forschungsprojekten erfolgen. Eine Formulierung wie „zu Forschungszwecken" würde demnach nicht genügen, es reicht aber die Nennung eines Forschungsbereichs. Dennoch wäre es ratsam, die Einwilligung auch bei der ungerichteten Spende so **konkret wie möglich** zu formulieren, ohne die Datennutzung zu verhindern, um ethischen Standards zu entsprechen und zur Konformität mit der DSGVO gewährleisten, da diese den „broad consent" nur in den Erwägungsgründen impliziert. Die Formulierung von möglichst konkreten Zwecken, ohne damit das Forschungsvorhaben zu

[122] *Veil*, Data altruism, Algorithm Watch, 2022. 2022_AW_Data_Altruism_final_publish.pdf (algorithmwatch.org).

verhindern, kann besonders gut durch die „dynamic consent"-Form geschehen, in welcher flexible Tools zum consent management angeboten werden. Diese bieten Bürger:innen die Möglichkeit nachzuvollziehen, wo ihre Daten verwendet werden, und ihre Einwilligung jederzeit zu widerrufen. Im Forschungsprojekt Smart FOX wurden daher bereits passende „smart consent management"-Ansätze in WP4 entwickelt.

Zusätzlich müssen die Betroffenenrechte geschützt werden, nur mit gewissen Einschränkungen, wie in Kapitel 4.2.3 analysiert. Dies sollte grundsätzlich auch bei der ungerichteten Spende möglich sein, da eben in Smart FOX keine Spende ohne jegliche Einschränkungen vorgesehen ist. Partner:innen des Forschungsprojekts werden auf § 2d Abs 5 FOG verwiesen, laut welchem die Betroffenenrechte in Art 15 bis 18 und Art 20 sowie 21 DSGVO eingeschränkt werden können, wenn diese „die Erreichung von Zwecken gemäß Art 89 Abs 1 DSGVO voraussichtlich unmöglich gemacht oder ernsthaft beeinträchtig(en)". Es muss daher immer evaluiert werden, wo diese umgesetzt werden können, bzw. ob die Einschränkung dieser Rechte unter dem FOG zulässig ist.

Der DGA betont außerdem in ErwGr 46 in Bezug auf Datenaltruismus, dass auch hier, wie unter der DSGVO erforderlich, die Möglichkeit gegeben sein muss, eine Einwilligung zurückzuziehen bzw. dass Betroffene sich über die Verarbeitung ihrer Daten informieren können müssen:

> *„Weitere Schutzvorkehrungen sollten umfassen, dass einschlägige Daten in einer von anerkannten datenaltruistischen Organisationen betriebenen sicheren Verarbeitungsumgebung verarbeitet werden können, dass mithilfe von Aufsichtsmechanismen wie Ethikräten oder -gremien, einschließlich Vertretern der Zivilgesellschaft, sichergestellt wird, dass der für die Verarbeitung Verantwortliche hohe wissenschaftliche Ethikstandards und den Schutz der Grundrechte einhält, dass wirksame und klar kommunizierte technische Mittel vorhanden sind, um die Einwilligung auf der Grundlage der Informationspflichten des Auftragsverarbeiters gemäß der Verordnung (EU) 2016/679 jederzeit widerrufen oder ändern zu können, sowie Mittel, mit deren Hilfe sich die betroffenen Personen über die Verwendung der von ihnen bereitgestellten Daten laufend informieren können."*

Dementsprechend müssen entsprechende technische Maßnahmen entworfen werden, um diese Rechte auch bei der ungerichteten Spende zu sichern, sofern diese nicht unter der DSGVO und dem FOG eingeschränkt werden können. Die Einhaltung der Betroffenenrechte spielt im Forschungsprojekt eine wichtige Rolle bei der Gestaltung des Einwilligungsprozesses („consent management") in WP4.

7.2. Rechtliche Implikationen der ungerichteten Spende von ELGA-standardiserten Gesundheitsdaten

Im Folgenden werden die rechtlichen Implikationen für eine ungerichtete Gesundheitsdatenspende mit ELGA-standardisierten Daten punktuell behandelt. Der Aufbau dieses Kapitels basiert auf dem Dokument „Requirements_Donation of health data_Smart FOX_V0-2.docx“, wo der Ablauf der ungerichtete Datenspende auf S. 29 dargestellt wird:

7.2.1. Patient:innenwunsch, ELGA-standardisierte Daten zu spenden

Im Nachgang einer erfolgten Diagnose und Behandlung können Patient:innen sich dazu entscheiden, dabei erhobene Gesundheitsdaten der Forschung und damit einer Sekundärnutzung zur Verfügung zu stellen. Die Einwilligung zu einer Datenverarbeitung im Rahmen einer Gesundheitsdatenspende kommt als Rechtsgrundlage für eine Verarbeitung gem. Art 6 und Art 9 DSGVO in Frage. Dafür muss eine Einwilligung ausdrücklich für einen oder auch mehrere festgelegte Zwecke vorliegen. Außerdem muss sie freiwillig erfolgen, also informiert und unmissverständlich getätigt werden (Art 4 Z 11 DSGVO). Bedacht werden muss, dass die Art und Weise, wie die Gesundheitsdienstanbietenden über die Möglichkeit, Gesundheitsdaten zu spenden, die potenziellen Spendenden informieren, die Freiwilligkeit der Einwilligung beeinflussen könnte: Der Zeitpunkt, zu dem die Patient:innen Informationen zu der Datenspende vermittelt bekommen, muss also so gewählt sein, dass die Patient:innen keinen Druck empfinden, Gesundheitsdaten zu spenden.

7.2.2. Recherche und Information über die Gesundheitsdatenspende

Um eine informierte Einwilligung zu ermöglichen, sind Informationsmaterialien für die Patient:innen unerlässlich. Dabei ist auf die Gestaltung sowie die Vollständigkeit der Inhalte zu achten. Insbesondere die Risiken, Rechte, Vorschriften und Garantien, die im Kontext der Verarbeitung von personenbezogenen (inkl. pseudonymisierten) Gesundheitsdaten vorliegen, und wie diese Rechte geltend gemacht werden können, sind dabei zu erläutern (ErwG 39 DSGVO).

7.2.3. Definition des Zwecks der Gesundheitsdatenspende durch Patient:innen

Im Zuge der Einwilligung sind die Zwecke, zu denen die gespendeten Daten verarbeitet werden, eindeutig und rechtmäßig anzuführen (Zweckbindung der Verarbeitung personenbezogener Daten gem. Art 5 Abs 1 lit b DSGVO). Die Daten, welche im Zuge der Gesundheitsdatenspende gespendet werden, müssen gem. ErwG 39 DSGVO angemessen, erheblich und auf das notwendige Maß beschränkt sein (Grundsatz der Datenminimierung gem. Art 5 Abs 1 lit c DSGVO). Dies bedeutet,

dass von den Verarbeitungsverantwortlichen Fristen für die Löschung oder die regelmäßige Überprüfung der Notwendigkeit vorzusehen sind.

Es besteht in Österreich das Konzept des Broad Consent, welcher im § 2d Abs 3 FOG gem. Art 89 DSGVO geregelt wurde. Dementsprechend kann für die Definition des Zwecks einer Datenspende für Verarbeitungen, die im Anwendungsbereich des FOG liegen, die Angabe von Forschungsbereich(en) oder (Teilen von) Forschungsprojekten ausreichen. Allerdings ist der Zweck so konkret wie möglich festzulegen, um DSGVO-Vorgaben wie auch ethische Grundsätze zu erfüllen.

7.2.4. Spende der Gesundheitsdaten

Im Rahmen der Datenspende ist in die Verarbeitung der Gesundheitsdaten einzuwilligen. Dies muss durch eine eindeutige Handlung passieren, die das Einverständnis der Patient:innen informiert, freiwillig, konkret und unmissverständlich widerspiegelt – das kann auch elektronisch und schriftlich durch das Ankreuzen der Zustimmung (beispielsweise auf einer Gesundheitsdatenspende-Webseite) durch die Patient:innen erfolgen (ErwG 32 DSGVO).

Ebenso sind die Anforderungen der DSGVO des Grundsatzes der Integrität und Vertraulichkeit gem. Art 5 Abs 1 lit f DSGVO zu bedenken.

Eine mögliche Schutzmaßnahme ist die Pseudonymisierung und Verschlüsselung von Daten iSv Art 32 Abs 1 lit a DGSVO, wie bereits im Forschungsprojekt Smart FOX vorgesehen. Als weitere Maßnahmen werden in Art 32 Abs 1 lit b bis lit d folgende Maßnahmen für die Sicherheit angeführt:

- „die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“

Außerdem ist eine Datenschutz-Folgeabschätzung gem. Art 35 Abs 3 lit b DSGVO durchzuführen.

Die Verarbeitung iSv Art 4 Z 2 DSGVO von ELGA-Gesundheitsdaten ist in § 14 GTelG geregelt. Das Verlangen einer Kopie der personenbezogenen Daten durch die Betroffenen gem. Art 15 Abs 3 DSGVO stellt eine Verarbeitung von personenbezogenen ELGA-Gesundheitsdaten dar, die gem. § 14 Abs 2 Z 3 GTelG erlaubt wird – somit stellt ein Download durch die Teilnehmer:innen einen rechtmäßigen Vorgang dar. In § 14 Abs 3 GTelG findet sich die das Verbot des Verlangens von sowie

des Zugriffs auf und der Verarbeitung von ELGA-Gesundheitsdaten, sofern diese Handlungen nicht unionsrechtlich oder gesetzlich fundiert sind. Wie eine Datenspende dennoch rechtlich gelingen kann, findet sich in Kapitel 5.2.

7.2.5. Nutzung der gespendeten Gesundheitsdaten

Zu bedenken ist, dass die personenbezogenen Daten gem. Art 15 Abs 1 sowie ErwG 39 DSGVO nur so lange gespeichert werden dürfen, wie diese Speicherung unbedingt erforderlich ist.

Nach der Spende ist die mögliche Ausübung der Betroffenenrechte zu bedenken, die Teil der bereitzustellenden Information für die Einwilligung in die Datenspende sind. Diese sind in Kapitel III der DSGVO gelistet und beinhalten z.B. die folgenden (im Kapitel 4.2.3. ausführlich dargestellten) Rechte:

- Auskunftsrecht (Art 15 DSGVO);
- Recht auf Berichtigung (Art 16 DSGVO);
- Recht auf Löschung (Art 17 DGSVO);
- Recht auf Einschränkung der Verarbeitung (Art 18 DSGVO);
- Widerspruchsrecht (Art 21 DSGVO).

All diese Betroffenenrechte können eingeschränkt werden, sofern durch die Erreichung der in Art 89 Abs 1 DSGVO definierten Zwecke unmöglich gemacht oder ernsthaft beeinträchtigt werden (§ 2d Abs 6 FOG). Daran ist beispielsweise zu denken, wenn die Löschung von Gesundheitsdaten nach der Publikation einer Studie verlangt wird, in der diese Daten verwendet wurden. Für die Ausübung der Betroffenenrechte ist die Definition der datenschutzrechtlichen Rollen sowie der Verantwortung für die Datenverarbeitungen vorzunehmen, sofern ein AHDDS etabliert ist.

7.3. Rechtliche Implikationen der gerichteten Spende von ELGA-standardisierten Gesundheitsdaten

Im Folgenden werden die rechtlichen Implikationen für eine gerichtete Gesundheitsdatenspende mit ELGA-strukturierten Daten behandelt. Der Aufbau dieses Kapitels basiert auf dem Dokument „Requirements_Donation of health data_Smart FOX_V0-2.docx“, wo der Ablauf der ungerichtete Datenspende auf S. 31 dargestellt wird:

7.3.1. Konzeption einer klinischen Studie durch die Forschenden

Bei der Planung durch die Forschenden sind die Grundsätze der DSGVO zu beachten – folgende Prinzipien sind in Hinblick auf die gerichtete Gesundheitsdatenspende hervorzuheben:

- Grundsatz der rechtmäßigen Verarbeitung (Art 5 Abs 1 lit a DSGVO);
- Grundsatz der Zweckbindung (Art 5 Abs 1 lit b DSGVO);
- Grundsatz der Datenminimierung (Art 5 Abs 1 lit c DSGVO);
- Grundsatz der Integrität und Vertraulichtkeit (Art 5 Abs 1 lit f DSGVO);
    - technische Maßnahmen;
    - organisatorische Maßnahmen.

Die Einwilligung zu einer Gesundheitsdatenspende kommt als Rechtsgrundlage für eine Verarbeitung gem. Art 6 Abs 1 lit a und Art 9 Abs 2 lit a DSGVO in Frage. Dafür muss eine Einwilligung ausdrücklich für einen oder auch mehrere festgelegte Zwecke erfolgt sein. Außerdem muss sie freiwillig erfolgen, also informiert und unmissverständlich getätigt werden (Art 4 Z 11 DSGVO). Diese Einwilligung muss durch eine eindeutige Handlung passieren, die das Einverständnis der Patient:innen zusätzlich zur Informiertheit und Freiwilligkeit auch konkret und unmissverständlich widerspiegelt – das kann elektronisch und schriftlich durch das Ankreuzen der Zustimmung (beispielsweise auf einer Gesundheitsdatenspende-Webseite) durch die Patient:innen erfolgen (vgl ErwG 32 DSGVO Bedacht werden muss, dass die Art und Weise, wie die Gesundheitsdienstanbietenden über die Möglichkeit, Gesundheitsdaten zu spenden, die potenziellen Spendenden informieren, die Freiwilligkeit der Einwilligung beeinflussen könnte: Der Zeitpunkt, zu dem die Patient:innen Informationen zu der Datenspende vermittelt bekommen, muss also so gewählt sein, dass die Patient:innen keinen Druck empfinden, Gesundheitsdaten zu spenden.

Im Zuge der Einwilligung sind die (im Zeitpunkt der Einwilligung bereits festzustehenden) Zwecke, zu denen die gespendeten Daten verarbeitet werden, eindeutig und rechtmäßig anzuführen (Zweckbindung der Verarbeitung personenbezogener Daten gem. Art 5 Abs 1 lit b DSGVO). Die Daten, welche im Zuge der Gesundheitsdatenspende gespendet werden, müssen gem. ErwG 39 DSGVO angemessen, erheblich und auf das notwendige Maß beschränkt sein (Grundsatz der Datenminimierung gem. Art 5 Abs 1 lit c DSGVO). Dies bedeutet, dass von den Verarbeitungsverantwortlichen Fristen für die Löschung oder die regelmäßige Überprüfung der Notwendigkeit vorzusehen sind. Zu bedenken ist, dass die personenbezogenen Daten gem. ErwG 39 DSGVO nur so lange gespeichert werden dürfen, wie diese Speicherung unbedingt erforderlich ist (Grundsatz der Speicherbegrenzung gem. Art 5 Abs 1 lit e DSGVO) und nur Daten zu erheben sind, die auch benötigt werden (Grundsatz der Datenminimierung/Speicherbegrenzung gem. Art 15 Abs 1 DSGVO).

7.3.2. Organisatorische Vorbereitung der klinischen Studie

Zur Förderung des freiwilligen Datenaustausches wurde die Idee des Datenaltruismus im Rahmen des DGA eingeführt. Um als datenaltruistische Organisation anerkannt zu werden, ist die Registrierung und Akkreditierung gem. Art 18 und 19 DGA Voraussetzung. Dafür müssen die Kriterien der Ausführung datenaltruistischer Tätigkeiten, der vorliegenden Rechtspersönlichkeit, der Unentgeltlichkeit sowie Unabhängigkeit und der funktionellen plus organisatorischen Trennung der datenaltruistischen Tätigkeit von anderen Tätigkeiten der Organisation erfüllt sein. Der AHDDS bzw. die daran teilnehmenden Organisationen könnten eine solche Registrierung für die Zertifizierung als besonders vertrauenswürdige (Datenspende-)Organisation anvisieren – damit gehen neben Aufzeichnungs- und Berichtspflichten auch die Information von Betroffenen und das Bereitstellen von Tools für Einholung und Widerruf von Einwilligungen einher. Außerdem müssen angemessene Sicherheitsvorkehrungen für den Schutz personenbezogener Daten erfüllt werden.

Zu beachten ist außerdem, dass der Zugang zu Forschungsdaten alleine nicht eine Erlaubnis zur rechtmäßigen Verarbeitung dieser bedeutet. Es bedarf neben einer Rechtsgrundlage wie der bereits angeführten Einwilligung der Betroffenen auch der Erfüllung anderer Voraussetzungen: Beispielsweise dürfen ELGA-Daten gem. des GTelG nur zu bestimmten Zwecken und von bestimmten Personengruppen verarbeitet werden (iSv Art 4 Z 2 DSGVO). Weitere Ausführungen zu ELGA-Gesundheitsdaten finden sich im Kapitel 5.1..

7.3.3. Set-Up der FOX BOX

Hinsichtlich der Informationssicherheit der FoxBox sind die Anforderungen der DSGVO, insb. hinsichtlich des Grundsatzes der Integrität und Vertraulichkeit gem. Art 5 Abs 1 lit f DSGVO zu bedenken, die technische und organisatorische Schutzmaßnahmen seitens der/des Verarbeitungsverantwortlichen erfordern. Als geeignete Maßnahmen werden in Art 32 Abs 1 DSGVO folgende genannt:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Mögliche Schutzmaßnahmen iSv Art 32 Abs 1 lit a DGSVO stellen also die Verschlüsselung sowie die Pseudonymisierung von Daten dar – beides ist für das Forschungsprojekt Smart FOX geplant. Es liegt allerdings weiterhin ein Zuordnungsrisiko vor, da eine Re-Identifikation der Personen nicht ausgeschlossen ist. Außerdem ist eine Datenschutz-Folgeabschätzung gem. Art 35 Abs 3 lit b DSGVO durchzuführen (siehe Kapitel 4.3.).

7.3.4. Durchführung der klinischen Studie

Bei der Durchführung von Studienteilnehmenden-Recruitment sind die ethischen und medizinrechtlichen Aspekte zu beachten und auch einzuhalten. Für die Kontaktierung von Patient:innen stellt sich die (datenschutzrechtliche) Frage, wie diese Kontaktierung verläuft – dabei muss die Quelle der Informationen (z.B. über Gesundheitsdiagnosen oder der Kontaktdetails) geklärt werden und für deren Verarbeitung auch eine entsprechende Rechtsgrundlage nach Art 6 DSGVO (z.B. Einwilligung oder berechtigtes Interesse) und ebenfalls nach Art 9 DSGVO, sofern es sich um Gesundheitsdaten handelt, (z.B. Forschungsprivileg) vorliegen

Um eine informierte Einwilligung zu ermöglichen, sind Informationsmaterialien für die Patient:innen unerlässlich. Dabei ist auf die Gestaltung der dargebotenen Informationen, aber auch die Vollständigkeit der Inhalte zu achten. Insbesondere die Risiken, Rechte, Vorschriften und Garantien, die im Kontext der Verarbeitung von personenbezogenen (inkl. pseudonymisierten) Gesundheitsdaten vorliegen, und wie diese Rechte geltend gemacht werden können, sind dabei zu erläutern (ErwG 39 DSGVO).

Auch die Zwecke der Datenverarbeitung im Rahmen der Studiendurchführung sollen aus datenschutzrechtlicher wie ethischer Perspektive so konkret wie möglich definiert sein – um Forschungsvorhaben dabei so umfangreich wie möglich realisieren zu können, empfiehlt sich die Einwilligung in Form eines „dynamic consent“ zu gestalten. Patient:innen können somit flexibel ihre Einwilligung in die Datenverarbeitung erteilen, diese genau nachvollziehen und die Einwilligung auch widerrufen.

Vor einer Datenverarbeitung der Gesundheitsdatenspende ist auch die Klarstellung der (datenschutzrechtlichen) Rollen wichtig – auch in Hinblick auf einen eventuellen AHDDS,dessen Errichtung und Ausgestaltung nach dem Forschungsprojekt Smart FOX in Frage kommen könnte. Hier ist zu (er)klären, ob die Institution, welche die Studie durchführt, auch die datenschutzrechtliche Verarbeitungsverantwortung trägt. Es empfiehlt sich, diese Klarstellung vertraglich zwischen den teilnehmenden Organisationen zu gestalten.

7.3.5. Data Linkup zwischen ELGA-standardisierten Daten und Biobanken-Daten oder klinischen Registern

Aus der Verknüpfung von Gesundheitsdaten aus unterschiedlichen Quellen kann sich ein erheblicher Nutzen für die Forschung ergeben. Dies wird daher bei der Datenspende in Smart FOX als Option in Betracht gezogen und in den Demonstrators erprobt. Da sich aus der Verknüpfung von Daten jedoch evtl. neue rechtliche Fragen und ein erhöhtes Reidentifizierungsrisiko ergeben, müssen Risiken von Anfang an im Prozess bedacht werden (z.B muss die Nutzung von Daten aus anderen Quellen bereits in der Einwilligung feststehen).

Daraus ergeben sich auch Fragen zur Re-Kontaktierung, da evtl. Personen, deren Daten einmal erhoben wurden, nun eine Anfrage zur Spende und Nutzung ihrer ELGA-standardisierten Daten erhalten sollen. Hinsichtlich der Re-Kontaktierung von Datenspendenden ist aus rechtlicher Perspektive hervorzuheben, dass auch bei dieser Datenverarbeitung, die in Zusammenhang mit den gespendeten Gesundheitsdaten steht, eine Rechtsgrundlage erforderlich ist. Die Möglichkeiten dazu werden in diesem Kapitel illustriert.

Nach einer Gesundheitsdatenspende ist die mögliche Ausübung der Betroffenenrechte zu bedenken, die Teil der bereitzustellenden Information für die Einwilligung in die Datenspende sind. Diese sind in Kapitel III der DSGVO gelistet und beinhalten z.B. die folgenden (im Kapitel 4.2.3. ausführlich dargestellten) Rechte:

- Auskunftsrecht (Art 15 DSGVO);
- Recht auf Berichtigung (Art 16 DSGVO);
- Recht auf Löschung (Art 17 DGSVO);
- Recht auf Einschränkung der Verarbeitung (Art 18 DSGVO);
- Widerspruchsrecht (Art 21 DSGVO).

All diese Betroffenenrechte können eingeschränkt werden, sofern durch die Erreichung der in Art 89 Abs 1 DSGVO definierten Zwecke unmöglich gemacht oder ernsthaft beeinträchtigt werden (§ 2d Abs 6 FOG).

Für die Ausübung der Betroffenenrechte ist die Definition der datenschutzrechtlichen Rollen sowie der Verantwortung für die Datenverarbeitungen vorzunehmen, sofern ein AHDDS etabliert ist.

7.3.6. Analyse der erhobenen Daten

Die Methoden, welche zur Auswertung von gespendeten Daten genutzt werden, sind im Rahmen des Forschungsprojekts Smart FOX insoweit zu bedenken, als bestimmte Auswertungsmethoden

evtl. ein erhöhtes Risiko für die Rechte und Freiheiten der Betroffenen bergen, welches bei der Gesundheitsdatenerhebung bekannt gemacht werden muss. Oft im Fokus stehen dabei KI-Methoden, die auch seit kurzem durch die KI-Verordnung weiter reguliert werden. Einer der umstrittenen Aspekte ist jedoch, ob die Nutzung von KI-Methoden bei der Datenverarbeitung immer als solche in den Informationen, die vor der Einwilligung bereitgestellt werden, festgehalten sein muss. Gründe, dies nicht zu tun, sind in der Praxis beispielsweise mangelnde Informationen über die genaue Datenverarbeitung zum Erhebungszeitpunkt und auch die Sorge bei Betroffenen, die allein schon die Erwähnung von KI hervorrufen kann.[123]

Rechtlich ist nicht eindeutig beantwortet, ob die Nutzung von KI-Technologien immer explizit in der Information zur Einwilligung behandelt werden muss, bzw. ob darin auch explizit eingewilligt werden muss. Anforderungen für die Transparenz gegenüber Betroffenen ergeben sich jedoch weiterhin aus der DSGVO, welche nicht festlegt, wie explizit Verarbeitungsmethoden genannt werden müssen, jedoch sehr wohl vorschreibt, dass über Risiken aufgeklärt werden muss (nach dem Grundsatz der Transparenz in Art 5 Abs 1 (a) iZm ErwGr 39 DSGVO). Interessanterweise scheinen sich aus der KI-Verordnung keine neuen Informationspflichten im Kontext medizinischer KI zu ergeben, da sowohl Art 86 als auch Art 50 Abs 1 und Art 13, welche Informations- und Transparenzpflichten betreffen, hier wohl nicht anwendbar sind. [124] Es besteht allerdings bei Hochrisikosystemen die Verpflichtung, vor der Anwendung eine Grundrechte-Folgenabschätzung durchzuführen (Art 27 KI-VO). Dadurch kann sich indirekt ergeben, dass neue Vorgaben zur Informiertheit eingeführt werden, als Maßnahme um den Einschnitt in die Grundrechte Betroffener zu reduzieren.

Des Weiteren können sich aus den Methoden, welche in der Forschung genutzt werden sollen, Anforderungen an die Daten ergeben. Dies von Anfang an in Betracht zu ziehen, kann Daten in dem Forschungsprojekt Smart FOX oder einem daraus eventuell resultierenden AHDDS breiter nutzbar machen. Wenn also mit KI-Methoden geforscht werden soll, ist zu beachten, dass aus der KI-Verordnung evtl. auch Anforderungen für die eingespeisten Daten abzuleiten sind. Wenn KI-Systeme

[123] Siehe z.B. Katarzyna Wałdoch, “Informed Consent for the Use of AI in the Process of Providing Medical Services” (2024) 57 Review of European and Comparative Law 121, 128.

[124] Diese Artikel behandeln die Information von Betroffenen bei einer automatisierten Entscheidung, die Transparenzpflichten von Entwickler:innen gegenüber Anwender:innen und gegenüber denjenigen, welche direkt mit KI-Systemen interagieren. Es geht also hier nicht um Information an Personen, deren Daten zu Trainings- oder Forschungszwecken verarbeitet werden. KI im medizinischen Bereich ist außerdem gänzlich von Art 86 dadurch ausgeschlossen, dass nur Hochrisiko-KI, welche in Annex III genannt wird, unter diesen Artikel fällt und Medizinprodukte in Anhang I genannt werden.

in den Hochrisikobereich fallen (was bei KI im Gesundheitsbereich regelmäßig der Fall sein wird)[125], so ist Art 10 (Data and Data Governance) auf die KI-Systeme anwendbar.[126] Im Learning Club am 4. Juni 2025 wurden Partner:innen demnach darum gebeten, sich mit Art 10 auseinanderzusetzen und zu überlegen, ob daraus evtl. zusätzliche Anforderungen für Daten im Rahmen des Forschungsprojekts Smart FOX oder eines AHDDS resultieren, welche über die gewöhnliche Praxis zur Sicherung von Datenqualität hinausgehen (z.B. hinsichtlich einer Evaluierung der Datenerhebungsprozesse oder möglicher „biases“ (Art 10 Abs 2lit b und Art 10 Abs 2 f).

In der technischen Dokumentation, welche für die Kommerzialisierung von Hochrisikosystemen notwendig ist (Art 11), sollen, wenn relevant, auch die Trainingsdaten und deren Herkunft beschrieben werden (siehe Annex IV (2) (d) der KI-VO). Da das Forschungsprojekt Smart FOX selbst keine KI-Systeme entwickelt oder anwendet, entstehen aus der KI-VO keine direkten Verpflichtungen. Da über Smart FOX bereitgestellte Daten aber sehr wahrscheinlich der Entwicklung von KI-Systemen zugutekommen könnten, ist es an dieser Stelle bereits relevant, zu überlegen, welche Formen der Dokumentation der Datenerhebung und Verarbeitung in Smart FOX möglich sind.

[125] Da die EU-Medizinprodukteverordnung in Annex I der KI-VO aufgelistet ist, gelten KI-Produkte, welche unter der Medizinprodukteverordnung bisher eine Konformitätsbewertung durchlaufen mussten, so werden diese nun auch als Hochrisiko-KI-System eingestuft.

[126] Es gibt auch in der KI-Verordnung Ausnahmen für die Forschung (siehe Art 2(6)), welche im Einzelfall anwendbar sein können. Die Verordnung wäre aber dennoch anwendbar, sobald z.B. KI-Systeme als Medizinprodukte auf den Markt gebracht werden.

7.4. Follow-Up bei klinisch relevanten Zufallsbefunden („incidental findings“)

Im Kontext medizinischer Forschung sind sogenannte „incidental findings“ als im Rahmen einer klinischen Untersuchung oder von klinischer Forschung auftretende klinisch relevante Erkenntnisse, welche außerhalb des ursprünglichen Fokus der Forschung fallendefiniert.[127] Die Gewinnung dieser Erkenntnisse war nicht Teil des ursprünglichen Zwecks der Studie und daher sind Patient:innen möglicherweise unwissend darüber, dass diese Information über ihre Gesundheit personenbezogen gewonnen werden könnte.

Grundsätzlich spricht viel dafür, Patient:innen über solche Erkenntnisse zu informieren, um diesen zu erlauben, informierte Entscheidungen über die eigene Gesundheit zu treffen und eventuelle Folgeuntersuchungen durchführen zu lassen oder Präventivmaßnahmen zu setzen. Aus verschiedenen Gründen können Patient:innen es jedoch auch vorziehen, nicht informiert zu werden: es gilt zu bedenken, dass die vermeintliche Entdeckung von „incidental findings“ (oft mit einer hohen Rate an falsch positiven Befunden) belastende Folgeuntersuchungen nach sich ziehen kann, welche nicht immer eindeutige Vorteile für die Patient:innen mit sich bringen.[128] Des Weiteren ist es eine sehr individuelle Entscheidung, über Erkrankungen oder Risiken informiert zu werden. Durch die Übermittlung von Zufallsbefunden, ohne dies vorher abgesprochen zu haben, wird Einzelnen die Entscheidung verwehrt. Dies kann immer problematisch sein, basierend auf individuellen Präferenzen, Werten und Erfahrungen.[129] Es zeigt sich jedoch besonders klar am Beispiel von unheilbaren Krankheiten. In der Literatur ist daher neuerdings öfter von dem „right not to know“ die Rede (insb in Bezug auf genetische Sequenzierung aber auch darüber hinaus),[130] das Patient:innen das Recht einräumt, zu entscheiden etwas über die eigene Gesundheit nicht zu erfahren.

Durch neue Technologien, wie etwa innovative Imaging-Methoden, verbessern sich die Möglichkeiten, Patient:innen über „incidental findings“ aufzuklären – vor allem, wenn dabei ein Mechanismus vorgesehen ist, durch den Einzelne entscheiden können, ob sie diese Möglichkeit ggfs wahrnehmen wollen. Bei datengetriebener Forschung (insb KI) können zusätzlich neue Muster und Verbindungen erkannt werden und es wird dadurch noch schwieriger vorherzusehen, welche Art

[127] Christenhusz/Devriendt/Dierickx, Disclosing incidental findings in genetics contexts: A review of the empirical ethical research, European Journal of Medical Genetics 2013, 56(10), 529.
[128] Ells/Thombs, The ethics of how to manage incidental findings, Canadian Medical Association Journal 2014, 186(9).
[129] Christenhusz/Devriendt/Dierickx, Disclosing incidental findings in genetics contexts: A review of the empirical ethical research, European Journal of Medical Genetics 2013, 56(10).
[130] Berkman/Hull, The “Right Not to Know” in the Genomic Era: Time to Break From Tradition?, The American Journal of Bioethics 2014, 14(3).

der „incidental findings“ in welchem Ausmaß auftreten können.[131] Im Rahmen von Datenspenden, wie diese im Forschungsprojekt Smart FOX anvisiert werden, könnte es auch der Fall sein, dass in Studien genutzte Daten zu “incidental findings“ führen. Durch den relativen langen Zeitraum für den der Datenspende zugestimmt werden kann, kann dies evtl. auch Jahre nach der ursprünglichen Einwilligung zur Datenspende eintreten. Es hat sich in dem Forschungsprojekt zunächst die Frage gestellt, ob es auf technischer Ebene überhaupt die Möglichkeit geben wird, Ergebnisse zurückzuverfolgen. Diese Frage ist derzeit noch offen, obwohl dies zumindest im Szenario der gerichteten Datenspende mit hoher Wahrscheinlichkeit möglich sein wird.

Sollte die Rückverfolgbarkeit von „incidental findings“ technisch möglich sein, stellt sich die Frage, ob diese Möglichkeit genutzt werden sollte, oder ob Gegenargumente überwiegen. Etwa ist fraglich, ob alleinig zur Übermittlung von “incidental findings“ ein Schlüssel zur Re-Identifikation der Einzelnen aufbewahrt werden sollte, wenn diese sonst nicht notwendig wäre und die Privatsphäre der Datenspendenden durch Löschung des Schlüssels besser geschützt wäre. Um diese Abwägung zwischen Datenschutz und Gesundheitsversorgung auch aus Patient:innenperspektive zu evaluieren, haben der Patient:innenbeirat des LBI DHPS und Survivors AT dieses Thema auch in Fokusgruppen behandelt.

Sollte die Übermittlung möglich sein und ein Schlüssel sowieso zu anderen Zwecken aufbewahrt werden, wie derzeit für das Consent Management geplant, kann Betroffenen die Option zur Re-Kontaktierung eingeräumt werden. Diese sollte dann zeitgleich mit der Abgabe der Einwilligung erfolgen, über das Smart-FOX-User-Interface. Es sollte dabei klar sein, dass es sich bei der Einwilligung zur Re-Kontaktierung im Falle von „incidental findings“ um eine zusätzliche Option handelt, welche frei mit Ja/Nein beantwortet werden kann, unabhängig von anderen Einschränkungen bei der Einwilligung. Falls durch die eventuelle Rückübermittlung von „incidental findings“ Zusatzrisiken entstehen (etwa, weil ausschließlich ein Schlüssel aufbewahrt wird, um die pseudonymen Daten zuordnen zu können), muss auf diese Risiken in der Einwilligung ausdrücklich hingewiesen werden.

Es gilt auch zu überlegen, in welchem Format “incidental findings“ von den Forschenden an die Patient:innen übermittelt werden können. Meist ist hier die Empfehlung, dass „incidental findings“ von Gesundheitsfachkräften, etwa einer Ärztin des Vertrauens der Betroffenen, übermittelt werden, damit diese auch kontextualisiert und Folgeuntersuchungen besprochen

[131] Siehe z.B. im Kontext der Bilderkennung de Jong/Poon/Foo/Maingard/Kok/Barras/Yazdabadi/Shaygi/Fitt/Egan/Brooks/Asadi, Incidental findings in research brain MRI: Definition, prevalence and ethical implications, Journal of Medical Imaging and Radiation Oncology 2023, 69, 41.

werden können.[132] In Smart FOX wäre dies evtl. möglich, wenn die Datenspende über Gesundheitspersonal als Kooperationspartner:innen koordiniert wird. Da die Datenspende allerdings über ein Online-Portal möglich sein soll, ohne Kontakt mit Gesundheitsfachpersonal zu erfordern, ist dies nicht unbedingt immer umsetzbar. Sollte letztendlich nur eine Übermittlung von „incidental findings" per Email oder über das Online-Portal möglich sein, ist gut zu überlegen, in welchem Format und mit welcher Zusatzinformation diese übermittelt werden, etwa mitsamt Empfehlung eines Termins bei einer Haus- oder Fachärztin mit den erhaltenen Ergebnissen.

Zuletzt gilt auch noch zu beachten, dass Patient:innen auch in den von Survivors AT und LBI DHPS vorbereiteten Patient:inneninformationsmaterialien über die Bedeutung und praktische Ausgestaltung von „incidental findings" informiert werden sollten. Dabei ist jedoch darauf zu achten, dies nicht als zusätzlichen Nutzen zu präsentieren, denn es gibt keine Garantie, dass Teilnehmende „incidental findings" erhalten werden, oder dass diese von Nutzen für sie sein werden.

[132] Townsend/Adam/Birch/Lohn/Rousseau/Friedman, ''I Want to Know What's in Pandora's Box'': Comparing Stakeholder Perspectives on Incidental Findings in Clinical Whole Genomic Sequencing, American Journal of Medical Genetics 2012, 2522.

7.5. Datenspende durch Minderjährige

Ein mögliches Szenario innerhalb des Forschungsprojekts Smart FOXist, dass Daten von Kindern gespendet werden. Hier stellt sich die Frage, ab welchem Alter Minderjährige selbst dazu in der Lage sind, über die Datenverarbeitung zu bestimmen, und ob die Erziehungsberechtigten an ihrer Stelle in die Datenspende einwilligen können.

Ein wichtiger Referenzpunkt, wenn es um die Rechte von Kindern geht, ist die **UN-Kinderrechtskonvention**, die in Art 12 besagt, dass Kinder in Entscheidungen, die sie betreffen, entsprechend ihren Fähigkeiten und ihrer Entwicklung einbezogen werden sollten. Folgt man der UN-Kinderrechtskonvention, sollten Kinder also so früh wie möglich und so spät wie nötig in die Entscheidung über eine Datenspende einbezogen werden. Entscheidend ist, dass sie über das entsprechende Wissen und die Fähigkeiten verfügen, um die Risiken und Folgen der Datenspende abzuwägen.

Auf Ebene des EU-Rechts ist der **DGA** einschlägig, der Datenspenden für altruistische Zwecke reguliert. Dieser beinhaltet aber keine Regelungen zu den Datenspenden von Kindern. Da eine Datenspende eine Datenverarbeitung im Sinne der **DSGVO** ist, könnten somit eine Antwort auf die Frage in der DSGVO gefunden werden. Laut Art 8 Abs 1 DSGVO können Kinder erst ab einem bestimmten Alter in eine Datenverarbeitung für Dienste der Informationsgesellschaft einwilligen. Die Altersgrenze für die Einwilligung liegt hierbei 16 Jahren; die Mitgliedsstaaten können diese Altersgrenze allerdings bis auf 13 Jahre herabsetzen. Österreich hat die Altersgrenze für die Einwilligung auf 14 Jahre festgelegt. Dienste der Informationsgesellschaft werden in der Regel gegen ein Entgelt erbracht (§ 3 Abs 1 E-Commerce-Gesetz). Auch Services, die sich durch Werbung finanzieren, fallen unter diesen Begriff (Recital 18 E-Commerce Gesetz). Eine Datenspende stellt zwar eine Verarbeitung personenbezogener Daten dar, ist aber kein Dienst der Informationsgesellschaft, da wie im DGA vorausgesetzt keine Vergütung erfolgt oder eine Finanzierung auf Grundlage von Werbung. Dennoch wird Art 8 Abs 1 DSGVO oft analog auch auf andere Formen der Datenverarbeitung angewendet.[133] Eine **Einwilligung** in eine Datenverarbeitung setzt immer voraus, dass die betroffene Person über die Datenverarbeitung ausreichend informiert ist und somit dessen Konsequenzen abschätzen kann.[134] Diese Einsichtsfähigkeit muss bei Kindern individuell eingeschätzt werden. [135] Die Altersgrenze von 14 Jahren, die für Dienste der

[133] *Klement*, Art. 8 DSGVO, in *Simitis/Hornung/Spiecker Döhmann* (Hrsg), Datenschutzrecht DSGVO mit BDSG (2023).
[134] Siehe Erwägungsgrund 32 DSGVO.
[135] Klement in Simitis/Hornung/Spiecker Döhmann.

Informationsgesellschaft gilt und auch im ABGB als Altersgrenze für die beschränkte Geschäftsfähigkeit genannt wird, kann im Smart-FOX-Projekt als Orientierungspunkt dienen.[136] Man könnte jedoch auch argumentieren, dass, anders als bei einer transaktionalen Weitergabe von Daten an Dienste der Informationsgesellschaft, weniger Nachteile für eine Minderjährigen durch eine Datenspende entstehen können und diese deshalb bereits zu einem jüngeren Alter möglich sein sollte. Jedoch ist zu betonen, dass es sich bei für die Datenspende vorgesehenen Daten um sensible Gesundheitsdaten handelt und eine Datenverarbeitung deshalb durchaus mit besonderen Risiken verbunden ist.

Ebenfalls zur analogen Anwendung könnte auch das GTelG herangezogen werden, dass zwar nicht direkt einschlägig ist, aber ein sehr ähnliches Szenario regelt, nämlich, ab welchem Alter Kinder über ihre eigenen ELGA-Patient:innendaten verfügen dürfen. Das GTelG sieht in § 14 Abs 2a vor, dass minderjährige Patient:innen erst ab einem Alter von 14 Jahren Nutzen von ihren Teilnehmer:innenrechte nach § 16 ELGA-G machen können. Ab 14 Jahren wird die Mündigkeit der Minderjährigen *vermutet* und damit auch die Fähigkeit, ihre Rechte (wie Auskunft über und der Zugriff auf die eigenen ELGA-Daten) selbst wahrzunehmen. Unter 14 Jahren können die Erziehungsberechtigten die im Rahmen der ELGA bestehenden Rechte im Namen der Kinder wahrnehmen (§ 14 Abs 2 GTelG).

In der Erläuterung zur Regierungsvorlage[137] zur letzten Änderung des GTelG 2012 wird diese Altersgrenze (die auch in der aktuellen Fassung bestehen bleibt) mit Verweis auf § 173 ABGB, der die Einwilligung von Kindern in medizinische Behandlungen regelt, sowie auf Art 8 DSGVO erlassen.

Zusammenfassend findet sich keine Regelung zu der Datenspende von Minderjährigen im DGA. Die Regelungen der DSGVO beschränken sich auf Dienste der Informationsgesellschaft. Dennoch kann die DSGVO, als auch die Altersgrenze für die Wahrnehmung von Teilnehmer:innenrechten im ELGA-Gesetz als Referenzpunkt dienen, da diese für jeweils ähnliche Szenarien festlegen, ab welchem Alter Kinder die Konsequenzen und Risiken einer Datenverarbeitung einschätzen können. Die UN-Kinderrechtekonvention besagt, dass Kinder eingebunden werden sollen, sobald sie über die nötige Einsichtsfähigkeit verfügen. Zur Bestimmung dieser Einsichtsfähigkeit kann analog die Altersgrenze von 14 Jahren aus DSGVO und GTelG herangezogen werden. Folgt man der analogen Anwendung,

[136] Für den Fall, dass ein Kind mit der Entscheidung seiner Eltern zu einem späteren Zeitpunkt nicht einverstanden ist, ermöglicht Art 17 DGSVO, dass das Kind nachträglich die Löschung der Daten erwirken kann.
[137] *Parlament Österreich*, Gesundheitstelematikgesetz, Allgemeine Sozialversicherungsgesetz u.a., Änderung (2530 d.B.), Erläuterungen der Regierungsvorlage.

können sodann über eine Spende von Daten von jüngeren Kindern die Erziehungsberechtigten entscheiden, dabei sollten die Kinder jedoch in die Entscheidung einbezogen werden.

7.6. Die Datenspende durch nicht-entscheidungsfähige Personen

Entscheidungsfähigkeit bedeutet nach § 24 Abs 2 ABGB, dass eine natürliche Person die Bedeutung und Folgen ihres Handelns versteht, dementsprechend ihren Willen richten und sowie sich verhalten kann. Die Entscheidungsfähigkeit ist Voraussetzung für die **Handlungsfähigkeit** (§ 24 Abs 1 ABGB), bei deren Vorliegen die Person sich durch ihr eigenes Handeln rechtlich zu berechtigen und zu verpflichten.

Die Entscheidungsfähigkeit von natürlichen Personen sowie die Volljährigkeit (also die Vollendung des 18. Lebensjahres, § 21 ABGB) sind Voraussetzung für die Einwilligung in die **Vornahme von medizinischen Behandlungen** – nach § 252 ABGB zählen dazu „diagnostische, therapeutische, rehabilitative, krankheitsvorbeugende oder geburtshilfliche Maßnahme[n]“. Wenn die erforderliche Entscheidungsfähigkeit nicht vorliegt, haben die behandelnden Ärzt:innen gemäß § 252 Abs 2 ABGB Angehörige, Nahestehende, Vertrauenspersonen oder Fachpersonal beizuziehen, welche zur Entscheidungsfähigkeit verhelfen können; so ist allerdings nur vorzugehen, sofern nicht zu erkennen ist, dass die Beiziehung oder Informationsweitergabe unerwünscht sind. Sollte die Entscheidungsfähigkeit dadurch nicht erreicht werden (können), so muss die vorsorgebevollmächtigte Person oder Erwachsenenvertretung, sofern diese mit medizinischen Angelegenheiten betraut sind, gemäß §§ 253f ABGB der medizinischen Behandlung **zustimmen**.[138]

Personen, die aus anderen Gründen als des zu jungen Alters nicht entscheidungsfähig sind, also aufgrund von psychischen Krankheiten oder vergleichbaren Beeinträchtigungen, sollen gem. § 239 ABGB möglichst selbstständig handeln können – soweit dies nicht möglich ist, werden sie von dafür **bevollmächtigten Personen** oder gewählten/gesetzlichen oder gerichtlichen dazu bestimmte **Erwachsenenvertretungen** vertreten. Die vertretenden Personen haben dabei den Willen der vertretenen Person zu verwirklichen, solange dadurch deren Wohlbefinden nicht erheblich gefährdet wird, und dürfen nur beim Vorliegen der Voraussetzungen von § 250 ABGB (Teil des Wirkungsbereichs, fehlende Entscheidungsfähigkeit, Stellvertretung nicht ausgeschlossen, Vertretungshandlung zum Wohl der Person notwendig) tätig werden.

[138] Neumayr in Neumayr/Resch/Wallner, GmundKomm2 § 254 ABGB (Stand 1.1.2022, rdb.at).

Die zu vertretenden Personen können gemäß § 14 Abs 2 Z2 lit b und § 18 Abs 8 GTelG 2012 in Hinblick auf die ELGA vertreten werden: Dazu ist eine Einzelvertretungsbefugnis im Sinne des § 5 E-Government-Gesetzes notwendig.[139]

[139] Stärker in Neumayr/Resch/Wallner, GmundKomm2 § 18 GTelG 2012 (Stand 1.1.2022, rdb.at).

7.7. Gesundheitsdaten als Teil des Nachlasses

Nach dem Tod von Menschen können **vermögensrechtliche, nicht-höchstpersönliche Rechte** an die bestimmten oder gesetzlichen Erb:innen vererbt werden. Wenn Rechtsgeschäfte Rechte und Pflichten begründen, können diese Parteipositionen aus Verträgen ebenso auf Erb:innen übergehen. Das bezieht sich auch auf Auskunftsrechte über die durch die verstorbene Person getätigten Rechtsgeschäfte, aber auch auf Internetdienste wie beispielsweise Mail-, Webseiten- oder Nutzendenkonten.[140] Dabei kommt es nicht auf einen eventuellen Vermögenswert an, da im Rahmen der Gesamtrechtsnachfolge die digitale Verlassenschaft mit Ausnahme von höchstpersönlichen Rechtsverhältnissen und Daten an die Erb:innen übergeht.[141]

Von diesen Rechtsgeschäften sind auch **Gesundheitsbehandlungen als Behandlungsverträge** erfasst. Erb:innen und nahen Angehören wird soweit ein Auskunftsrecht bezüglich der Krankenhistorie von Verstorbenen eingeräumt, wie die Persönlichkeitsrechte dieser verstorbenen Personen dadurch nicht berührt werden und wie die mutmaßliche Einwilligung der Verstorbenen angenommen werden kann.[142] Nach der OGH-Entscheidung 2 Ob 162/16m richtet sich die Verschwiegenheitspflicht von behandelnden Ärzt:innen im Sinne des § 54 Abs 2 Z4 ÄrzteG also nach dem feststellbaren oder vermuteten Willen der Verstorbenen – wenn ein solcher Wille oder Anhaltspunkte dafür nicht gegeben sind, ist auf „die Maßfigur des verständigen und einsichtigen Menschen“[143] (im vorliegenden Fall in Hinblick auf die Feststellung der Testierfähigkeit) abzustellen.[144] Diese Maßfigur könnte auch als Maßstab für das Auskunftsrecht hinsichtlich der Krankenhistorie herangezogen werden.

In der ELGA werden medizinische Daten digital auf entsprechenden Plattformen gespeichert, die unter Umständen höchstpersönliche Inhalte darstellen. Hinsichtlich der Herausgabe dieser Daten wird von der Rechtsprechung vertreten, dass diese nur geschehen darf, wenn berechtigte Interessen an den Daten bestehen und dies mit dem **Persönlichkeitsschutz** der verstorbenen Person vereinbar

[140] Werkusch-Christ in Kletečka/Schauer, ABGB-ON1.11 § 531 (Stand 15.12.2023, rdb.at), RZ 1f.
[141] ianca Dorigatti/Wolfgang Lackner, Das digitale Leben nach dem Tod, iFamZ 2019, 196.
[142] Werkusch-Christ in Kletečka/Schauer, ABGB-ON1.11 § 531 (Stand 15.12.2023, rdb.at), RZ 3.
[143] OGH 27.7.2017, 2 Ob 162/16m, iFamZ 2017/239.
[144] OGH 27.7.2017, 2 Ob 162/16m, iFamZ 2017/239.

ist.[145] Dies ist der Fall, wenn durch die Herausgabe die Testierfähigkeit der verstorbenen Person bestimmt oder Erbkrankheiten aufgedeckt werden können.[146]

[145] OGH 23. 5. 1984, 1 Ob 550/84; 25. 5. 2000, 1 Ob 341/99z.
[146] Bianca Dorigatti/Wolfgang Lackner, Das digitale Leben nach dem Tod, iFamZ 2019, 196.

7.8. Data Linkup

ELGA-standardisierte Daten mit Daten aus zusätzlichen Quellen zu verknüpfen, kann für Forschungszwecke wünschenswert sein. Im Rahmen einer solchen Verknüpfung werden zusätzlich unterschiedliche Daten eingespeist, welche ein detaillierteres Bild über den Gesundheitszustand der Betroffenen bieten können. Im Forschungsprojekt Smart FOX wurde diese Option in WP5 untersucht. Es werden dazu *use cases* innerhalb des Biobankings und des Clinical-Registry-Bereichs definiert. Bei Data Linkup gilt es jedoch aus rechtlicher Perspektive, einige Aspekte zu beachten.

7.8.1. Daten aus anderen Quellen

Für jede Verarbeitung personenbezogener Daten braucht es eine gültige Rechtsgrundlage. Bei der Nutzung von ELGA-standardisierten Daten stützt sich das Konsortium des Forschungsprojekts Smart FOX auf die Einwilligung als Rechtsgrundlage (Art 6 Abs 1 lit a iZm Art 9 Abs 2 lit a DSGVO). Bei Daten aus anderen Quellen ist es aber keinesfalls als gegeben anzunehmen, dass diese auf Grundlage der Einwilligung gesammelt wurden. Selbst wenn eine Einwilligung in die ursprüngliche Datenverarbeitung vorliegt, ist nicht garantiert, dass diese Einwilligung auch die Verknüpfung mit ELGA-standardisierte Daten erfasst. Wenn der Zweck in der Einwilligung eng formuliert wurde, gilt diese Rechtsgrundlage für die Verarbeitung evtl. nur für spezifische klinische Studien, Biobanken, etc. Wenn die Einwilligung allerdings zu breit formuliert wurde (z.B. „für Forschungszwecke“), ist es auch nicht ratsam, sich auf diese zu stützen, da diese wohl kaum den Anforderungen einer Einwilligung im Sinn der DSGVO genügt. Auch bei einer Aufweichung des Zweckbindungsgrundsatzes zu Gunsten der wissenschaftlichen Forschung wird in der DSGVO zumindest eine „Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung“ gefordert (ErwGr 33 DSGVO)[147]. Selbst unter Einwilligung in Form vom „broad consent“ des österreichischen FOGs (§ 2d Abs 3) ist zumindest Eingrenzung auf einen oder mehrere Forschungsbereich(e) erforderlich.

Es muss daher die rechtliche Grundlage für die Verarbeitung sämtlicher Daten, die verarbeitet werden sollen, genau analysiert werden. Forschende dürfen also nicht automatisch davon ausgehen, dass, nur weil ELGA-standardisierte Daten und Daten aus anderer Quelle jeweils mit Einwilligung erhoben wurden, diese nun auch verknüpft werden dürfen.

[147] Diese Aufweichung des Zweckbindungsgrundsatzes ist umstritten, da nur in den Erwägungsgründen enthalten und somit nicht rechtlich bindend, siehe dazu Kapitel 4.1.2.5.

7.8.2. Re-Kontaktierung

Es ist außerdem zu bedenken, über welchen Weg Betroffene identifiziert werden, deren Daten verknüpft werden sollen. Werden etwa in einer Biobank vorhandene Daten auf ihre Relevanz oder Verknüpfbarkeit mit anderen Daten untersucht, so kann dieser Prozess selbst schon eine Verarbeitung personenbezogener Daten darstellen. Ebenso ist dies der Fall, wenn z.B. Teilnehmende an einer Studie re-kontaktiert werden sollen. Auch für den Re-Kontaktierungsvorgang muss geprüft werden, ob eine gültige Rechtsgrundlage vorliegt. Diese könnte sich z.B. daraus ergeben, dass bei der ursprünglichen Sammlung der Daten (z.B. durch die Biobank oder im Rahmen einer Studie) bereits die Re-Kontaktierung bzw. Nutzung der Daten zu weiteren Zwecken in der Einwilligung geregelt wurde. Sollte dies nicht der Fall sein, könnte die Re-Kontaktierung evtl. aufgrund des berechtigten Interesses (Art 6 Abs 1 lit f DSGVO) rechtskonform sein, welches unter Umständen als Grundlage für die Datenverarbeitung zum Zweck der Direktwerbung herangezogen werden kann (ErwGr 47 DSGVO). Diese Rechtsgrundlage erfordert jedoch eine Abwägung der Interessen der Verantwortlichen und der Interessen, Grundrechte und Grundfreiheiten der Betroffenen. Es ist also zu hinterfragen, ob aus der Datenverarbeitung Risiken oder Einschnitte in die Grundrechte betreffend des Schutzes der personenbezogener Daten der Betroffenen entstehen, welche im Vergleich zu den Forschendeninteressen überwiegen würden. Außerdem ist der Zweckbindungsgrundsatz weiter zu beachten (Art 5 Abs 1 lit b), laut dem Daten nicht in einer mit den Zwecken, für die sie erhoben wurden, nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Wenn Kontaktdaten z.B. rechtmäßig erhoben wurden, um eine Kontaktierung zur Teilnahme an medizinischen Studien zu ermöglichen, so ist eine Re-Kontaktierung (also eine Weiterverarbeitung der Daten) wohl nicht entgegen dem Zweckbindungsgrundsatz. Partner:innen müssen aber aus diesem Grund beachten, ob Daten ursprünglich „für festgelegte, eindeutige und legitime Zwecke“ erhoben wurden und ob die jetzt geplante Verarbeitung mit den ursprünglichen Zwecken vereinbar ist.

7.8.3. Erhöhte Risiken bei der Datenverknüpfung

Des Weiteren muss auch beachtet werden, dass die Verknüpfung von Daten aus unterschiedlichen Quellen evtl. ein erhöhtes Reidentifizierungsrisiko zur Folge hat. Dieses Risiko ergibt sich aus zumindest zwei Quellen. Einerseits ist zu beachten, dass eine detailliertere Datenabbildung einer Person (z.B. eine spezifische Kombination aus ärztlichen Behandlungen und Untersuchungsergebnissen oder gar die Einspeisung von genetischen Daten) Rückschlüsse auf deren Identität leichter ermöglicht. Andererseits setzt die Verknüpfung von verschlüsselten Daten voraus, dass ein Schlüssel vorhanden und den Verknüpfenden zugänglich ist. Dieser kann zwar direkt oder

weniger direkt auf eine Person rückführbar sein, es gilt jedoch jedenfalls zu evaluieren, wer im Besitz dieses Schlüssels ist und welche Risiken dadurch entstehen.

Da das Forschungsprojekt Smart FOX insb. die Verknüpfung mit klinischen Registern (WP5) in Betracht zog, geht die rechtliche Analyse im Folgenden konkret auf diese Datenquellen ein.

7.8.4. Herzinsuffizienz-Register und CRC-Kohorte

Im Rahmen von Smart FOX sollte getestet werden, wie die Verknüpfung mit Registern funktionieren könnte. Das sollte anhand des Beispiels des LIV-Herzinsuffizienz-Registers und der MUG CRC-Kohorte geschehen. Diese sind nicht zu verwechseln mit bundesgesetzlich vorgesehenen Registern, auf welche sich Ausschnitte des FOG konkret beziehen. Da es derzeit keine Verordnung nach § 38b FOG gibt, welche auf direkterem Weg Zugang zu diesen Registerdaten ermöglichen würde, gilt derselbe Rechtsrahmen wie bei jeder anderen Verarbeitung von Gesundheitsdaten, inkl. den im FOG vorgesehenen Rechtsrahmen für die Einwilligung und die Forschungsausnahme.

Diese klinischen Register enthalten personenbezogene Daten. Selbst wenn diese oft aggregiert genutzt werden und Ergebnisse aus diesen Datenbanken dann als anonymisiert gelten könnten, so ist davon auszugehen, dass sie, in der Form, in der sie für Smart FOX genutzt werden sollen, reidentifizierbar sind, da sie ja auch mit ELGA-standardisierte Daten verknüpft werden sollen. Dies soll mithilfe eines Schlüssels geschehen, der das Data Linkup tatsächlich auch ermöglicht.

Für die Nutzung dieser Registerdaten ist ein Ausnahmetatbestand in Art 9 DSGVO und eine Rechtgrundlage nach Art 6 DSGVO notwendig. Grds könnte für die Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken die Forschungsausnahme (Art 9 (2) (j) DSGVO, konkretisiert in § 2d Abs 2 FOG, in Betracht gezogen werden.

Dies wird in vorliegenden Fall aus folgendem Grund jedoch nicht empfohlen: Registerdaten sollen eben dazu genutzt werden, mit ELGA-standardisierten Daten verknüpft zu werden, um ein detailliertes Datenabbild der jeweiligen Person zu ermöglichen. ELGA-standardisierten Daten, welche ursprünglich als ELGA-Daten gesammelt wurden, können nur auf Grundlage der Einwilligung genutzt werden, nicht der Forschungsausnahme (siehe dazu Kapitel 4.1.2.5). Im Zuge dieser Einwilligung nun nicht darzustellen, dass ELGA- standardisierte Daten auch mit Registerdaten verknüpft werden sollen, würde kein klares Bild der Datennutzung ergeben und nicht der Informiertheit entsprechen, welche ErwGr 32 der DSGVO voraussetzt für eine gültige Einwilligung entsprechend Art 7 DSGVO. Insbesondere, da sich durch die Verknüpfung der Daten aus unterschiedlichen Quellen ein erhöhtes Reidentifizierungsrisiko ergeben kann und Betroffene in der

Einwilligung über Risiken informiert werden müssen, würde es nicht dem Wesen der informierten Einwilligung entsprechen, für die Verknüpfung mit Registerdaten keine Einwilligung einzuholen.

Der derzeit gewählte Zugang im Projekt ist daher, bei der Einholung der Einwilligung zur Verarbeitung der ELGA- standardisierte Daten auch die Einwilligung zur Verarbeitung der Registerdaten einzuholen. Es muss dabei für Betroffene verständlich sein, worin sie einwilligen. Ist die Verarbeitung sowohl mit als auch ohne Verknüpfung mit Registerdaten geplant, so soll für diese getrennt die Einwilligung eingeholt werden (z.B. zwei unterschiedliche Boxen anzukreuzen), denn: „wenn die Verarbeitung mehreren Zwecken dient, sollte für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden.“ (ErwGr 33 DSGVO).

8. Ausblick für die Sekundärdatennutzung in Österreich

Im letzten inhaltlichen Abschnitt wird versucht, eine Perspektive auf die kommenden Entwicklungen im Zusammenhang mit der Sekundärnutzung von Daten zu geben. Hauptaugenmerk liegt dabei auf der Datenspende von Gesundheitsdaten.

8.1. Datennutzung im öffentlichen Interesse

Wie im Folgenden dargestellt, greift das europäische Digitalrecht immer wieder auf den Begriff des „öffentlichen Interesses" zurück, um bestimmte Formen der Datenverarbeitung von anderen abzugrenzen. Allerdings stellt sich dadurch die Frage, was eine Datennutzung im öffentlichen Interesse begründet und wer dies definiert. Im Rahmen des Forschungsprojekts Smart FOX ist relevant zu klären, ob eine Datenspende eine Datennutzung im öffentlichen Interesse darstellt und somit unter Datenaltruismus im Sinne des DGA vorliegt.

Im Datenschutzrecht kann das Verfolgen eines öffentlichen Interesses eine Datenverarbeitung legitimieren. Art 6 Abs 1 DSGVO wie auch Art 9 Abs 2 lit i DSGVO nennen das öffentliche Interesse. Die DSGVO definiert allerdings nicht, was ein öffentliches Interesse ist, sondern verweist hierfür auf Unionsrecht oder Recht der Mitgliedstaaten. Auch der DGA, der ebenfalls Datennutzung im öffentlichen Interesse durch Datenaltruismus fördern möchte, definiert ein öffentliches Interesse nicht abschließend. Art 2 Abs 16 DGA beschreibt Datenaltruismus als „die freiwillige gemeinsame Nutzung von Daten […] für Ziele von allgemeinem Interesse gemäß dem nationalen Recht, wie die Gesundheitsversorgung, die zu Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Entwicklung, Erstellung und Verbreitung amtlicher Statistiken, die Verbesserung der Erbringung öffentlicher Dienstleistungen, die staatliche Entscheidungsfindung oder die wissenschaftliche Forschung im allgemeinen Interesse".

Bemerkenswert ist, dass der DGA nicht wie häufig in Rechtsvorschriften Privilegien für gemeinnützige Datennutzung, sondern eine Reihe von organisatorischen und technischen Anforderungen an datenaltruistische Organisationen schafft. Um als gemeinnützige Organisation anerkannt zu werden und im öffentlichen Interesse zu handeln, bestehen also nicht nur Voraussetzungen hinsichtlich des Zwecks selbst, sondern auch im Hinblick auf die Art und Weise der Datenverarbeitung.

Der Verweis an Unions- und nationales Recht für die Festlegung des öffentlichen Interesses war während des Gesetzgebungsprozess der DSGVO durchaus umstritten.[148] Diskutiert wurde, ob die Kommission genauer definieren solle, welche Zwecke im öffentlichen Interesse liegen. Der Widerstand der Mitgliedsstaaten und das Argument, dass diese die Möglichkeit haben sollten, auf nationale und neuartige Themen einzugehen, überwog allerdings schlussendlich.[149]

Infolgedessen stellt sich die Frage, ob eine (Gesundheits)**Datenspende** einem **öffentlichen Interesse** im Sinne des österreichischen Rechts dient. Um sich als datenaltruistische Organisation zu registrieren, bedarf es eines österreichischen Gesetzes, das bestätigt, dass das der jeweilige Zweck der Organisation im öffentlichen Interesse liegt. Für eine Organisation, die Datenspenden von ELGA-standardisierten Daten auf Grundlage der Einwilligung der Patient:innen für Forschungszwecke ermöglicht, könnte eine Rechtsgrundlage im FOG oder im GTelG liegen.

Das FOG regelt die **Forschungsprivilegien nach Art 89 DSGVO**, die der „Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken" dienen. Das FOG beschreibt wissenschaftliche Einrichtungen in § 2b Abs 12 FOG als „natürliche Personen, Personengemeinschaften sowie juristische Personen, die Zwecke gemäß Art 89 Abs 1 DSGVO verfolgen". § 1 FOG führt die Ziele der Förderung von Wissenschaft und Forschung weiter aus und nennt unter anderem „die Erweiterung und Vertiefung der wissenschaftlichen Erkenntnisse" und das Ziel „zur Lösung sozialer, wirtschaftlicher, kultureller und wissenschaftlicher Problemstellungen verantwortlich beizutragen, vor allem zur Sicherung und Hebung der allgemeinen Lebensqualität und der wirtschaftlichen Entwicklung". Daraus lässt sich folgern, dass **Datenspenden an wissenschaftliche Einrichtungen** zu Forschungszwecken im öffentlichen Interesse nach dem FOG im öffentlichen Interesse liegen.

Weiter könnte das GTelG eine Datenspende von ELGA- standardisierten Daten als öffentliches Interesse festlegen. **§ 13 Abs 1 GTelG** besagt, dass die „Verwendung der Elektronischen Gesundheitsakte (…) ein erhebliches öffentliches Interesse gemäß Art 9 Abs 2 lit. g bis j der DSGVO" erfüllt. Das öffentliche Interesse ergebe sich, neben anderen Zielen, insbesondere aus „der Aufrechterhaltung einer qualitativ hochwertigen, ausgewogenen und allgemein zugänglichen Gesundheitsversorgung". Wenn argumentiert werden kann, dass eine Datenspende von ELGA-

[148] *Slokenberga/Tzortzatou/Reichel*, GDPR and Biobanking: Individual Rights, Public Interest and Research Regulation across Europe 43 (2021) 24.
[149] Ibid.

standardisierten Daten diesem Zweck dient, könnte auch § 13 Abs 1 GTelG herangezogen werden, um ein öffentliches Interesse zu rechtfertigen.

Daraus folgt, dass eine Datenspende unter den oben genannten Bedingungen im öffentlichen Interesse ist und somit das Forschungsprojekt Smart FOX sich grundsätzlich als datenaltruistische Organisation registrieren lassen kann. Allerdings sind dafür die Voraussetzungen im folgenden Kapitel einzuhalten.

8.2. Möglichkeit der Registrierung als datenaltruistische Organisation

Der DGA führt nicht nur das Konzept des Datenaltruismus in EU-Recht ein, sondern eröffnet auch die Möglichkeit der Registrierung als datenaltruistische Organisation. Aus den Erwägungsgründen geht hervor: „Juristische Personen, die bestrebt sind, Zwecke von allgemeinem Interesse zu unterstützen, indem sie einschlägige Daten auf der Grundlage von Datenaltruismus in größerem Maßstab zur Verfügung stellen und bestimmte Anforderungen erfüllen, sollten sich als ‚in der Union anerkannte datenaltruistische Organisationen' eintragen lassen (…) können" (ErwGr 3 DGA). Die Eintragung in einem Mitgliedsstaat ist unionsweit gültig.

Die allgemeinen Eintragsanforderungen für eine datenaltruistische Organisation sind in Art 18 DGA enthalten. Die Organisation muss:

> *„a) datenaltruistische Tätigkeiten durchführen;*
>
> *b) gemäß nationalem Recht Rechtspersönlichkeit haben, um gegebenenfalls gemäß dem nationalen Recht Ziele von allgemeinem Interesse zu erreichen;*
>
> *c) selbst ohne Erwerbszweck tätig sein und rechtlich unabhängig von jeder Organisation, die Erwerbszwecke verfolgt, handeln;*
>
> *d) die Datenaltruismus-Tätigkeiten über eine Struktur ausüben, die von ihren anderen Tätigkeiten funktionell getrennt ist;*
>
> *e) dem in Artikel 22 Absatz 1 genannten Regelwerk entsprechen, und zwar spätestens 18 Monate nach dem Tag des Inkrafttretens der delegierten Rechtsakte, auf die in jenem Absatz Bezug genommen wird."*

Jede Organisation, welche diese Kriterien erfüllt, kann die Eintragung in einem Unionsregister datenaltruistischer Organisationen beantragen (Art 17 Abs 1 DGA). ErwGr 48 stellt außerdem klar: „Diese Verordnung sollte die Einrichtung, Organisation und Funktionsweise von Einrichtungen, die sich nach nationalem Recht dem Datenaltruismus verschreiben, unberührt lassen und sich auf die Anforderung stützen, dass die Tätigkeiten einer Organisation ohne Erwerbszweck in einem Mitgliedstaat nach nationalem Recht rechtmäßig sein müssen." Daraus lässt sich entnehmen, dass, wie zu erwarten, die in Frage kommenden Organisationen sich nach allen nationalen Anforderungen für Organisationen ohne Erwerbszweck richten müssen, und die Einordnung als „datenaltruistische Organisation" dann nur noch zusätzlich erreicht werden kann, in dem die Kriterien des DGA erfüllt werden.

Beim **Eintragungsantrag** müssen eine Reihe an Informationen übermittelt werden, welche in Art 19 Abs 4 DGA aufgelistet sind, inklusive u.A. Informationen über den Rechtsstatus der Organisation, über die Einnahmequellen und die Zwecke, welche die Organisation mit der Datensammlung fördern will. Einige dieser Angaben werden laut Art 19 Abs 6 DGA als Bestandteil des nationalen Registers veröffentlicht.

Datenaltruistische Organisationen sollten Daten direkt bei juristischen oder natürlichen Personen sammeln, oder von Dritten gesammelte Daten verarbeiten. Die **Rechtsgrundlage** dafür wäre, in der Regel, die Einwilligung der betroffenen Personen (ErwGr 50 des DGA).

Grds. entspricht das Konzept der Datenspende in Smart FOX der Idee des Datenaltruismus im DGA. Der geplante AHDDS könnte, je nach finaler Form, durchaus ein System sein, welches Datenaltruismus wie im DGA vorgesehen ermöglicht. **Es ist daher zu überlegen, ob es für eine:n Smart-FOX-Konsortialpartner:in (oder mehrere Konsortialpartner:innen gemeinsam durch Etablierung einer neuen Organisation) sinnvoll wäre, sich als datenaltruistische Organisation registrieren zu lassen**.

Voraussetzung dafür ist jedoch zunächst, dass Österreich ein **Register datenaltruistischer Organisationen** aufsetzt, wie in Art 20 Abs 1 DGA von Mitgliedsstaaten gefordert. In Österreich war lange Zeit unklar, welche Stelle für die Umsetzung des DGA zuständig ist, bis letztendlich im Juli 2023 das Finanzministerium (konkret das Staatssekretariat für Digitalisierung und Telekommunikation) für zuständig erklärt wurde.[150] Im Mai 2024 wurde Staatssekretärin Claudia Plakolm zusätzlich zu Jugend und Zivildienst auch für Digitalisierung zuständig, womit sich auch die Zuständigkeit für die

[150] *BMF*, Tursky: Bundesregierung einigt sich auf Europäische Datenstrategie (2023), https://www.bmf.gv.at/presse/pressemeldungen/2023/juli/tursky-datenstrategie.html.

Umsetzung des DGA verschiebt. Zuständige Stellen, inkl. der zuständigen Behörde für datenaltruistische Organisationen, müssen jedoch noch ernannt werden. Die Europäische Kommission hat im Mai 2024 Vertragsverletzungsverfahren gegen 18 Mitgliedsstaaten, unter ihnen Österreich, eingeleitet, da diese die zuständigen Behörden unter dem DGA noch nicht benannt hatten. Die betroffenen Staaten hätten eine Frist von zwei Monaten, um zu reagieren, aber auch seitdem hat es in Österreich, soweit im Februar 2026 öffentlich ersichtlich, noch keine klare Benennung der zuständigen Behörden gegeben.

Zusätzlich zu dem nationalen Register fordert Art 15 Abs 2 DGA, dass die EU ebenfalls ein Register aufsetzt. Dieses existiert bereits und ist online einsehbar,[151] auch wenn derzeit erst eine (spanische) Organisation registriert ist.[152] Die **Registrierung im EU-Register** wird durch die Mitgliedsstaaten über ein simples, ebenfalls online verfügbares Formular durchgeführt.[153] Es ist also in jedem Fall die Ernennung einer österreichischen zuständigen Behörde abzuwarten, da die Registrierung nicht direkt über die Europäische Kommission erfolgen kann.

Einige Anforderungen an datenaltruistische Organisation stehen bereits fest:

- In Art 19 DGA sind die oben genannten allgemeinen **Eintragsanforderungen**, welche die Rechtspersönlichkeit der Organisation betreffen.
- Aus Art 20 DGA ergeben sich **Transparenzanforderungen** für alle eingetragenen datenaltruistische Organisation. So müssen nach Art 20 Abs 1 DGA Aufzeichnungen über die vorgenommenen Datenverarbeitungen; die Personen, welche die Möglichkeit hatten, Verarbeitungen vorzunehmen; den Zweck der Verarbeitungen; sowie etwaige Gebühren, die von den die Daten verarbeitenden Personen gezahlt wurden, geführt werden. Nach Art 20 Abs 2 DGA ist ebenfalls ein jährlicher Tätigkeitsbericht erforderlich, welcher Information über die Tätigkeit der Einrichtung, über die in dem Jahr vorgenommenen Datenverarbeitungen und die Einnahmequellen der Einrichtung enthält. Eine detaillierte Auflistung ist in der Rechtsvorschrift selbst nachzulesen.
- Art 21 DGA enthält **Anforderungen zum Schutz der Rechte und Interessen** betroffener Personen und juristischer Personen, u.A. Pflichten der Dateninhaber:innen und betroffenen Personen über Verarbeitungszwecke und etwaige Verarbeitung außerhalb der Union zu

[151] *EC*, EU register of recognised data altruism organisations (2024), https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations.
[152] Die Organisation ist Datalog (Barcelona), https://datalog.es/.
[153] *EC*, EU register of recognised data altruism organisations (2024), https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations.

informieren und die Pflicht sicherzustellen, dass die Daten nicht für andere Zwecke als die vorgesehenen verarbeitet werden. Das Weiteren sollen laut Art 21 Abs 3 DGA datenaltruistische Organisationen Werkzeuge zur Einholung der Einwilligung sowie auch Werkzeuge zum Widerruf der Einwilligung zur Verfügung stellen. Nach Art 21 Abs 4 DGA muss die Organisation Maßnahmen ergreifen, um ein angemessenes Sicherheitsniveau für die Speicherung und die Verarbeitung sicherzustellen.

Die Angaben, die für die Einreichung des Antrags nach Art 19 Abs 4 DGA zunächst erforderlich sind, sind Dokumente, welche den Rechtsstatus der Organisation nachweisen und somit vermutlich nicht viel zusätzlichen **Aufwand** erfordern würden. Der organisatorische und bürokratische Aufwand des jährlichen Berichts, der Aufzeichnungen über die Datenzugriffe und -verarbeitung und die Informationspflichten könnten jedoch erheblich sein. Des Weiteren ist dadurch, dass die zuständige Stelle in Österreich noch nicht ernannt wurde, die genaue Gestaltung des Antragsprozesses noch offen.

Die Registrierung als datenaltruistische Organisation ist freiwillig und hat wohl das Ziel und den Vorteil, **Vertrauen** in die registrierten Organisationen zu stärken. Die Registrierung als datenaltruistische Organisation ist jedoch keine Voraussetzung für die Ausübung der datenaltruistischen Tätigkeit (ErwGr 46 DGA). Mit der Registrierung kommt das Recht, das dafür vorgesehene Logo zu nutzen, mit der Schrift „EU Recognised Data Altruism Organisation".[154] Falls sich der AHDDS weiter in die derzeit geplant Richtung entwickelt und der oder die Anbieter:innen des AHDDS die Vorreiter in Österreich für Datenaltruismus bzw. Datenspende sein wollen, wird es sehr wahrscheinlich ratsam sein, sich als Betreiber:in des AHDDS in Österreich, wie im Nachgang von Smart FOX geplant, als datenaltruistische Organisation zu registrieren. Derzeit sind jedoch einige Fragen zu dem Prozess dafür noch offen.

[154] *EC*, Logos for data intermediaries and data altruism organisations recognised in the Union (2023), https://digital-strategy.ec.europa.eu/en/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union.

8.3. Möglichkeit der Registrierung als Datenvermittlungsdienst

Neben dem Konzept des Datenaltruismus führt der DGA ebenfalls sogenannte „Datenvermittlungsdienste" ein. Datenvermittlungsdienste sollen einige der zentralen Hindernisse beseitigen, die Dateninhabende bislang davon abhalten, ihre Datensätze mit Dritten zu teilen. Zu diesen Hindernissen zählen insbesondere das Fehlen einer geeigneten technischen Infrastruktur, rechtliche Unsicherheiten sowie mangelndes Vertrauen.[155] Nach Ditfurth und Lienemann geht die Entstehung des Konzepts der Datenvermittlungsdienste und der damit verbundenen Verpflichtungen auf die Erfahrungen der EU mit großen Technologieplattformen („Big Tech") zurück, die in erheblichem Umfang Daten sammeln. [156] Entsprechend zielt die Regulierung der Datenvermittlungsdienste in des DGA darauf ab, ein Gleichgewicht zwischen der Stärkung solcher Vermittler:innen durch den Aufbau von Vertrauen und der präventiven Begrenzung eines möglichen Machtmissbrauchs zu schaffen.[157]

Der DGA definiert einen Datenvermittlungsdienst als

> *„einen Dienst, mit dem durch technische, rechtliche oder sonstige Mittel Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabenden einerseits und Datennutzern andererseits hergestellt werden sollen, um die gemeinsame Datennutzung, auch für die Zwecke der Ausübung der Rechte betroffener Personen in Bezug auf personenbezogene Daten, zu ermöglichen." (Art 2 Nr. 11 DGA)*

In Art 2 führt der DGA außerdem aus, welche Dienste nicht unter diese Definition fallen, darunter insbesondere:

- Dienste, die Daten von Dateninhabenden einholen und aggregieren, anreichern oder umwandeln, um deren Wert erheblich zu steigern, und anschließend die Nutzung der resultierenden Daten an Datennutzende lizenzieren, ohne eine direkte Geschäftsbeziehung zwischen Dateninhabenden und Datennutzenden herzustellen;
- Dienste, die sich auf die Vermittlung urheberrechtlich geschützter Inhalte konzentrieren;

[155] *Schweihoff et al*, Stuck in the middle with you: Conceptualizing data intermediaries and data intermediation services, Electronic Markets 34, 48; *Von Ditfurth/Lienemann*, The Data Governance Act: – Promoting or Restricting Data Intermediaries?, Competition and Regulation in Network Industries 23, 270.
[156] *Von Ditfurth/Lienemann*, Competition and Regulation in Network Industries 23, 271.
[157] *Von Ditfurth/Lienemann*, Competition and Regulation in Network Industries 23, 271.

- Dienste, die ausschließlich von einem Dateninhabenden genutzt werden, um eigene Daten bereitzustellen, oder von mehreren juristischen Personen innerhalb einer geschlossenen Gruppe – etwa in Lieferanten- oder Kundenbeziehungen oder vertraglich geregelten Kooperationen –, insbesondere wenn deren Hauptzweck darin besteht, die Funktionalität vernetzter Geräte sicherzustellen;
- Datenvermittlungsdienste öffentlicher Stellen, die nicht darauf abzielen, Geschäftsbeziehungen zu schaffen.

Weiter werden in Art 10 bestimmte Arten von Datenvermittlungsdiensten genannt, deren Tätigkeiten angemeldet werden müssen. Darunter fallen auch „Vermittlungsdienste zwischen betroffenen Personen, die ihre personenbezogenen Daten zugänglich machen wollen, […] und potenziellen Datennutzern, einschließlich Bereitstellung der technischen oder sonstigen Mittel als Voraussetzung dieser Dienste, sowie insbesondere Ermöglichung der Ausübung der in der Verordnung (EU) 2016/679 verankerten Rechte betroffener Personen“.

Grundsätzlich scheint Smart FOX unter die Definitionen eines Datenvermittlungsdienstes zu fallen. Hinsichtlich der Ausnahmen bleibt es schwer zu bestimmen, ab wann eine Dienstleistung den Daten „erheblichen Wert“ hinzufügt und damit nicht mehr als Datenvermittlungsdienst im Sinne des Art 2 Z 11 gilt. In Smart FOX werden die Patient:innendaten aufbereitet und pseudonymisiert – allerdings nicht um deren Wert zu steigern, sondern allein um die Sicherheit der Betroffenen zu garantieren.

Grundsätzlich könnte Smart FOX als Datenvermittlungsdienst gelten, da Smart FOX Daten von Betroffenen für Datennutzer:innen zugänglich macht und technische und rechtliche Mittel für den Datenaustausch zur Verfügung stellt (siehe Art 11 Abs 1 DGA). **Dennoch ist der Datenaltruismus eindeutig das passendere Instrument, da Daten nur für altruistische Zwecke und auf Grundlage der Einwilligung geteilt werden sollen**. Fraglich könnte aber sein, ob eine Registrierung als Datenvermittlungsdienst zusätzlich zur Registrierung als datenaltruistische Organisation möglich oder gar geboten ist.

Die Erwägungsgründe des DGAs geben hierüber Aufschluss:

> *„Die in dieser Verordnung geregelten **datenaltruistischen Organisationen sollten nicht als Anbieter von Datenvermittlungsdiensten gelten**, sofern diese Dienste keine Geschäftsbeziehungen zwischen potenziellen Datennutzern einerseits und betroffenen Personen und Dateninhabern, die Daten für altruistische Zwecke zugänglich machen, andererseits herstellen.“*

Da die Patient:innen keine Vergütung für die Datenspende erhalten, und somit also keine Geschäftsbeziehung zwischen den Akteur:innen entsteht, **ist Smart FOX also kein Datenvermittlungsdienst** nach Art 2 bzw. Art 10 lit b) DGA. Dies würde sich ändern, falls Smart FOX Patient:innen-Daten für nicht-altruistische Zwecke vermittelt, was allerdings momentan nicht vorgesehen ist.

8.4. Verändert der EHDS die österreichische Rechtslage? (Beitrag von GÖG)

Das nachfolgende Unterkapitel 8.4. wurde vom Team der GÖG (Lorenz Dolanski-Aghamanoukjan, BSc, Ekin Fidel Tanriverdi, BA, MSc und Kristina Weishäupl, MSc, MSc, BSc) verfasst.

Der **European Health Data Space (EHDS)**[158] [159] stellt eine Schlüsselinitiative der Europäischen Union im Bereich der Nutzung von Gesundheitsdaten dar, die auf die Schaffung eines einheitlichen digitalen Binnenmarktes für Gesundheitsdaten abzielt. Durch die Verordnung wird erstmals ein einheitlicher regulatorischer Rahmen für die (auch grenzüberschreitende) Nutzung von Gesundheitsdaten geschaffen, wobei sowohl die primäre als auch die sekundäre Nutzung adressiert werden. Die Sekundärnutzung bezieht sich auf die Verarbeitung von Gesundheitsdaten, die ursprünglich für die primäre Nutzung, d.h. die medizinische Versorgung, die Administration von Leistungserstattungen u.s.w. erhoben wurden, nun aber für weitere Zwecke, insbesondere in den Bereichen Forschung, Innovation, Public Health und regulatorische Tätigkeiten, verwendet werden können.

Die Verordnung trat im März 2025 in Kraft, und alle Teilbereiche werden aufgrund diverser gestaffelter Übergangsfristen in den darauffolgenden Jahren anzuwenden sein.

Da es sich (wie bei der DSGVO) um eine **europarechtliche Verordnung**[160] handeln wird, wird sie auch nationalstaatlich direkt gelten und muss nicht erst national umgesetzt werden. Allerdings regelt der Verordnungstext nicht alle Details, sondern sieht auch eine Reihe von **Durchführungsrechtsakten**

[158] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den Europäischen Raum für Gesundheitsdaten (EHDS), Interinstitutional File 2022/0140(COD).
[159] Gemeinsamer Europäischer Gesundheitsdatenraum; Gesundheit Österreich; https://datenplattform-covid.goeg.at/node/43.
[160] Arten von Rechtsvorschriften, Europäische Union, https://european-union.europa.eu/institutions-law-budget/law/types-legislation_de.

und delegierten Rechtsakten[161] vor. Delegierte Rechtsakte ermöglichen der Kommission, technische Details und Standards zur Nutzung von Gesundheitsdaten anzupassen, während Implementing Acts für eine einheitliche Umsetzung der Verordnung in allen Mitgliedstaaten sorgen. Weiters wird die konkrete Ausgestaltung einiger Teilaspekte im Verordnungstext explizit den Mitgliedsstaaten überlassen. Aufgrund dieser unmittelbaren Anwendbarkeit wird Österreich (so wie alle Mitgliedsstaaten) zahlreiche bestehende nationale Rechtsvorschriften, insofern sie der Verordnung widersprechen, anzupassen haben, sowie auch den genannten Spielraum in der Ausgestaltung einiger Teilaspekte nützen und diese in nationalen Vorschriften festlegen müssen. In etlichen EU-(ko)finanzierten Projekten werden außerdem Guidelines, technische Spezifikationen, Standards, Referenzimplementierungen etc. entwickelt, mit dem Ziel, den Mitgliedstaaten als Unterstützung bei der Umsetzung der EHDS-Verordnung zu dienen, zu einer noch weitergehenden Harmonisierung zu führen und die Entwicklung von Parallelsystemen samt der entsprechenden Kosten zu reduzieren. Ein Beispiel hierfür ist das Projekt TEHDAS2[162], das im Laufe der nächsten zwei Jahre konkrete Handlungs- und Implementierungsempfehlungen ausarbeiten wird.

Angesichts der weit gefassten und einheitlichen Anwendbarkeit der EHDS-Verordnung werden die dadurch geschaffenen Möglichkeiten zur Sekundärnutzung von Gesundheitsdaten weit über die derzeitige Situation in Österreich hinausgehen. Diverse sektorale Regelungen sowie die oftmals recht strikt definierten Nutzungseinschränkungen einzelner Datenbestände (wie z.B. etlicher Register oder eben ELGA[163]) sorgen für eine zersplitterte „Datennutzungslandschaft“ mit hohen Hürden, ganz besonders, wenn eine Fragestellung die Verschneidung unterschiedlicher Datenquellen erfordert. Siehe dazu die obige Analyse der derzeitigen Situation in den Kapiteln 3 und 4.

Ein wesentlicher Teil der Verordnung befasst sich mit der Primärnutzung von Gesundheitsdaten, insbes. für grenzüberschreitende Dienste, und wird z.B. auch für EHR-Systeme („Electronic Health Record“) tiefgreifende Veränderungen bringen. Allerdings beschränkt sich die folgende Analyse auf die Vorschriften im Zusammenhang mit der Sekundärnutzung von Gesundheitsdaten, die ja für Smart FOX von vorrangigem Interesse ist. Darin werden einige Begriffe in Englisch verwendet, da der finale Kompromisstext nur in dieser Sprache vorliegt und dem korrekten deutschen Sprachgebrauch nicht vorgegriffen werden kann.

[161] Europäische Kommission https://commission.europa.eu/law/law-making-process/adopting-eu-law/implementing-and-delegated-acts_en
[162] Second Joint Action Towards European Health Data Space, https://tehdas.eu/.
[163] Allgemeines zu ELGA, https://www.oesterreich.gv.at/themen/gesundheit/elektronisches-gesundheitssystem/elga___elektronische_gesundheitsakte/Seite.3110001.html.

8.4.1 Allgemeines

Die Verordnung hält explizit fest, dass sie die **DSGVO** konkretisiert und ergänzt („*specifies and complements*“) und somit neben ihr besteht, aber nicht vorrangig („*without prejudice to*“) oder nachrangig. Viele Begriffsdefinitionen werden aus anderen Rechtsakten übernommen, inbes. in der Definition von „*personal electronic health data*“ wird auf die Begriffsbestimmungen in Art 4 der DSGVO verwiesen.

In der aktuellen Fassung der EHDS-Verordnung findet sich keine eigenständige Regelung bezüglich **"Data Donation"** oder **"Data Altruism"**. Diese Konzepte wurden ursprünglich im Verordnungsentwurf diskutiert, jedoch in den späteren Fassungen entfernt. Stattdessen verpflichtet die EHDS-Verordnung HDABs lediglich dazu, mit der für datenaltruistische Organisationen zuständigen nationalen Behörde zu kooperieren und verweist in den Erwägungsgründen allgemein auf den **Digital Governance Act (DGA)**[164]. Vgl. dazu die obigen Analysen.

Die **Kategorien von elektronischen Daten**, die aufgrund der Verordnung verfügbar zu machen sind, sind breit gefasst und beinhalten unter anderen EHR-Daten, administrative Daten (z.B. zu Medikamentenausgabe oder Abrechnungsdaten), durch Medizinprodukte automatisch generierte Daten, Registerdaten, Daten aus klinischen Studien, Daten von Biobanken, bishin zu „*factors impacting on health*“ (also z.B. sozio-ökonomische Daten) inkl. Daten von „*wellness applications*“. Nicht für alle Datenkategorien gelten die selben Übergangsfristen. Mitgliedstaaten dürfen diese „*minimum categories*“ um weitere Kategorien ergänzen, können diese Liste aber nicht einschränken. Für einige Kategorien, wie z.B. genetische Daten, können allerdings die Vorgaben zum Schutz besonders sensibler und wertvoller Daten national strenger geregelt werden („*safeguarding the sensitivity and value of the data*“).

Die Sekundärnutzung elektronischer Gesundheitsdaten darf **nur zu bestimmten Zwecken** gewährt werden, wovon manche nur öffentlichen Körperschaften bzw. von diesen Beauftragten vorbehalten sind. Für Smart FOX sind einige dieser Zwecke relevant, nämlich wissenschaftliche Forschung, die zu Public Health beiträgt, die Verbesserung der Qualität oder Sicherheit der medizinischen Versorgung, worin der Nutzen für die Endnutzer:innen (also Patient:innen, GDAs etc.) hervorgehoben wird. Auch Training, Testen und Evaluierung von Algorithmen und KI-Systemen fällt darunter. Dem gegenüber ist jede Nutzung zum Schaden Einzelner oder ganzer Gruppen **explizit untersagt** (das umschließt auch potentiellen Schaden wie durch die Entwicklung von Waffen, illegalen Drogen oder Gesundheitsrisiken im Allgemeinen), ebenso wie für Werbe- oder Marketingzwecke. Explizit wird

[164] Verordnung (EU) 2022/868 über europäische Daten-Governance (Data Governance Act, DGA)

auch festgehalten, dass die Nutzung der **nationalen Gesetzgebung in Bezug auf Ethik** nicht widersprechen darf ("*ethical provisions pursuant to national law*").

Die EHDS-Verordnung verpflichtet Datenhalter:innen direkt zur Verfügungstellung von Daten unter bestimmten Voraussetzungen (s.u.), ohne von natürlichen Personen eine Zustimmung, **consent**, Opt-In oder Ähnliches einzuholen. Das gilt also auch für Daten in ELGA, für deren Nutzung ja derzeit die oben beschriebenen Einschränkungen gelten. Allerdings können natürliche Personen im Rahmen des EHDS jederzeit und ohne Angabe von Gründen ihr individuelles **Recht auf einen Opt-Out** aus der Verarbeitung der auf sie bezogenen Daten für sekundäre Nutzung ausüben und das auch jederzeit wieder zurücknehmen. Diese Entscheidung kann nicht rückwirkend geltend gemacht werden, d.h. breits bestehende Bewilligungen bleiben unverändert aufrecht. V.a. im Lichte der rezenten Pandemie dürfen Mitgliedsstaaten allerdings z.B. für wissenschafliche Forschung aus gewichtigen Gründen im öffentlichen Interesse („*for important reasons of public interest*") in ihrer nationalen Gesetzgebung den Opt-Out unter Einhaltung etlicher Auflagen einschränken: Dazu zählt die Unmöglichkeit, anders an die notwendige Information zu kommen; auch die Abwägung („*necessary and proportionate measure*") der Erfüllung des öffentlichen Interesses gegenüber den Grundrechten und Freiheiten in einer demokratischen Gesellschaft ist vorgeschrieben.

Inbes. für die Primärnutzung und in den grenzüberschreitenden EHDS-Anwendungsfällen spielt auch **Standardisierung** z.B. von Datenaustauschformaten eine große Rolle, ebenso wie Anforderungen an EHR-Systeme. Das strahlt mittels der betroffenen Datenquellen natürlich auch auf die Sekundärnutzung aus, auch wenn i.A. nicht vorgeschrieben ist, die vorliegenden Datenbestände extra für die Sekundärnutzung zu standardisieren oder sonstwie „passend zu machen".

8.4.2 HDAB

Die Verordnung verpflichtet die Mitgliedstaaten zur Einrichtung (mindestens) einer Zugangsstelle für Gesundheitsdaten (*Health Data Access Body, HDAB*), die eine Schlüsselrolle bei der Umsetzung des EHDS spielen wird. In all seinen Aufgaben ist der HDAB verpflichtet, im öffentlichen Interesse und unabhängig zu handeln.

Dazu gehört u.a.

- einen öffentlich einsehbaren Metadatenkatalog zu führen;
- Datenzugangsanträge entgegenzunehmen, zu bewerten und zu entscheiden;

- im Erfolgsfall die entsprechende Bewilligung auszustellen und zu erteilen, worin die Beschränkung der Zwecke und Datenminimierung auf das der Fragestellung angemessene und unbedingt notwendige Maß zu gewährleisten sind;
- die aufgrund einer Nutzungsbewilligung notwendigen Daten von den betroffenen Datenhalter:innen zu beschaffen und entsprechend aufzubereiten (z.B. Verschneidung, Anonymisierung oder Pseudonymisierung, Minimierung);
- die notwendigen Maßnahmen zur Einhaltung von Datenschutzvorschriften und zum Schutz von geistigem Eigentum und Geschäftsgeheimnissen treffen;
- die benötigten Daten in einer sicheren Verarbeitungsumgebung (*Secure Processing Environment, SPE*) zugänglich machen;
- die Einhaltung der entsprechenden Vorschriften sowohl der Datennutzer:innen aber auch der Datenhalter:innen zu überwachen;
- die Öffentlichkeit über Rechtsgrundlagen, technische und organisatorische Maßnahmen, individuelle Rechte und die Wege diese auszuüben, ausgestellte Nutzungsbewilligungen sowie die Ergebnisse der Datennutzungsprojekte zu informieren;
- mit anderen Mitgliedsstaaten und der Eur. Kommission für grenzüberschreitende Anträge zu kooperieren.

8.4.3 Datenhalter:innen

Die EHDS-Verordnung verpflichtet Datenhalter:innen, den Zugang zu Gesundheitsdaten zu gewährleisten, insbesondere für die Sekundärnutzung. Die Verordnung sieht in ihrer Festlegung der betroffenen Datenhalter:innen für Kleinstunternehmen (das sind solche, die weniger als 10 Personen beschäftigen und deren Jahresumsatz bzw. Jahresbilanz 2 Mio. € nicht überschreitet[165]) eine Ausnahme vor, welche allerdings durch nationales Recht wiederum aufgehoben oder eingeschränkt werden darf.

Für den genannten Metadatenkatalog müssen die Datenhalter:innen ihre Datenbestände nach vorgegebenen Standards und regelmäßig aktualisiert beschreiben, was u.a. auch Informationen zur Datenqualität beinhaltet.

Im Falle eines bewilligten Antrags sind die benötigten Daten dem HDAB fristgerecht bereitzustellen.

[165] Empfehlung der Kommission betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, (2003/361/EG) https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361&from=DE

Die Verordnung sieht Kostenersätze für den anfallenden Aufwand vor, allerdings können bei Nichteinhaltung der relevanten Vorschriften auch Strafen verhängt werden.

8.4.4 Datennutzer:innen

Datennutzer:innen müssen in ihren Datenzugangsanträgen u.a. detailliert erklären, zu welchen Zwecken sie welche Daten verarbeiten wollen, welcher Nutzen daraus zu erwarten ist, und gegebenenfalls auch, warum anonymisierte Daten für die Zielerreichung nicht ausreichend sind und daher pseudonymisierte Daten erforderlich sind.

Die Datennutzer:innen, die Zugang zu den Gesundheitsdaten im Rahmen des EHDS erhalten, können diese für definierte Zwecke, inbes. medizinische Forschung, Innovation im Gesundheitssektor und evidenzbasierte politische Entscheidungsfindung nutzen. Sie müssen jedoch datenschutzrechtliche Anforderungen erfüllen und die Daten ausschließlich für genehmigte Zwecke verarbeiten. Missbrauch, wie z.B. unzulässige Weiterverarbeitung, Reidentifizierung(sversuche) von natürlichen Personen, kann zu erheblichen Sanktionen (wie empfindlichen Verwaltungsstrafen, oder auch einer 5-jährigen Sperre jeglicher weiterer Nutzung im Rahmen des EHDS) führen.

Ergebnisse, inbes. Forschungsergebnisse mit Relevanz für die Gesundheitsversorgung, müssen fristgerecht veröffentlicht werden. Dies soll sicherstellen, dass die Nutzung öffentlicher Infrastrukturen auch öffentlichen Wert generiert. Neben wissenschaftlichen Publikationen gehört dazu auch, den HDAB in einer Weise zu informieren, die diesem wiederum ermöglicht, seiner Verpflichtung nachzukommen, auch die breite Öffentlichkeit in umfassender und allgemeinverständlicher Weise über Ergebnisse und Nutzen aufzuklären.

Die Datennutzer:innen haben auch die angesprochenen Kostenersätze zu leisten. Dabei sind (transparente, nicht diskriminierende) Ermäßigungen zulässig, um auch weniger zahlungskräftige Nutzer:innengruppen, wie z.B. universitär Forschende, nicht von der Sekundärdatennutzung auszuschließen.

8.4.5 Fazit

Alle erwähnten Vorgänge und Prozesse im Rahmen des EHDS entspringen zwar Vorschriften, was auch mit Konsequenzen bei Nichteinhaltung einhergehen kann. Die Verordnung betont aber mehrfach die Verpflichtung zu kooperativen Vorgehensweisen und Unterstützung der jeweils anderen beteiligten Stakeholder. Beispielhaft sei herausgegriffen, dass die HDABs die Datenhalter:innen darin unterstützen sollen, Standards einzuhalten, ihre Datenbestände gut zu beschreiben, die Erkenntnisse zur Hebung der Datenqualität zu nutzen, u.s.w.

Nur in so einem kooperativen Umfeld kann tatsächlich das enorme Erkenntnis- und Innovationspotential von Sekundärdatennutzung ausgeschöpft werden. Der damit durchaus auch verbundene Kulturwechsel gehört sicher zu den großen Herausforderungen, neben der Harmonisierung nationaler Rechtsvorschriften, neben dem Zusammenspiel mit Datenschutzregelungen wie der DSGVO, die weiterhin ein Grundpfeiler im Schutz der Rechte von Einzelpersonen ist, und auch neben den Anforderungen, Infrastrukturen auszubauen, zu digitalisieren, zu standardisieren, und alle damit verbundenen Prozesse zu entwickeln. Smart FOX kann sicherlich in vielen dieser Aspekte dazu beitragen, eine großen Schritt vorwärts zu machen, nicht zuletzt auch durch sein Kooperationsmodell.

9. Schlussbemerkungen

Eine Datenspende von ELGA-standardisierten Daten mit Einverständnis der betroffenen Person über den AHDDS ist rechtlich möglich, wenn Betroffene ihr Recht unter §16 GTelG ausüben, um auf ihre Daten zuzugreifen und diese dann außerhalb des Anwendungsbereichs des GtelG der Forschung zur Verfügung stellen. Ein weiterer, der Meinung des Teams der UNIVIE nach weniger rechtssicherer Weg, welcher jedoch der allgemeinen Praxis entspricht, ist die Zurverfügungstellung, mit Einwilligung der Betroffenen, von ELGA-standardisierten Daten, welche noch nicht Teil der ELGA sind, jedoch bereits in dem Format, dass sie für das Projekt nützlich macht.

Aus urheberrechtlicher Perspektive wirft die Verwendung reiner Tatsachenberichte und faktischer Daten keine Bedenken auf. Hinsichtlich des Datenschutzes sind keine Hindernisse bei der Spende von Gesundheitsdaten zu erkennen, wenn die Prinzipien der DSGVO eingehalten werden.

Beachtung ist jedenfalls den Rechten und dem Schutz von betroffenen Personen zu schenken. Nicht nur die Einhaltung von entsprechenden Rechtsvorschriften, sondern auch die informierte und selbstbestimmte Entscheidung von Patient:innen sollten, wie bisher bereits im Rahmen des Forschungsprojekts, auch in Zukunft bei der Umsetzung von Datenspenden einen Fokus darstellen. Dazu empfiehlt sich, die Ressourcen im Rahmen des Konsortiums zu nutzen und die Patient:innenperspektive aktiv bei der Weiterentwicklung einzuholen und bei der Gestaltung beizuziehen.

Die rechtlichen Neuerungen auf Ebene der EU bieten vor allem durch den DGA und den damit verbundenen Datenaltruismus eine Chance für die Datenspende in Österreich. Die Möglichkeit der Registrierung als datenaltruistische Organisation stellt trotz der bisher noch unklaren Prozesse mangels österreichischer Ausgestaltung nach derzeitigem Stand eine erstrebenswerte Weiterentwicklung aus dem Forschungsprojekt Smart FOX dar.

10. Literaturverzeichnis

Aigner Gerhard/Kletečka Andreas/Kletečka-Pulker Maria/Memmer Michael (Hrsg), Handbuch Medizinrecht für die Praxis (2024)

Asswad/Gómez Data Ownership: A Survey. Information 2021, 12, 465.

Ballantyne, How should we think about clinical data ownership?, Journal of Medical Ethics 2020, 289.

Berka/Binder/Kneihs, Die Grundrechte: Grund- und Menschenrechte in Österreich: Handbuch2. Auflage (2019).

BMF, Tursky: Bundesregierung einigt sich auf Europäische Datenstrategie (2023), https://www.bmf.gv.at/presse/pressemeldungen/2023/juli/tursky-datenstrategie.html

Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl, Datenschutzgesetz (2018) §7 Rz 10; Feiler/Forgó, EU-DSGVO und DSG: Kommentar, 527.

Carovano/Finck, Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy, Computer Law & Security Review 50, 105830.

Cofonet, Beyond Data Ownership, Law Review 2021-2022 501 (523).

Dokalik Dietmar/Zemann Adolf (Hrsg), Österreichisches und internationales Urheberrecht[8] (2023)

Dorigatti Bianca/Lackner Wolfgang, Das digitale Leben nach dem Tod, iFamZ 2019

EC, EU register of recognised data altruism organisations (2024), https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations

EC, EU register of recognised data altruism organisations (2024), https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations

EC, Logos for data intermediaries and data altruism organisations recognised in the Union (2023), https://digital-strategy.ec.europa.eu/en/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union

Europäische Kommission, National competent bodies and authorities under the Data Governance Act https://ec.europa.eu/newsroom/dae/redirection/document/98966 (Stand 29.07.2024).

Europäische Kommission, National competent bodies and authorities under the Data Governance Act https://ec.europa.eu/newsroom/dae/redirection/document/98966 (Stand 29.07.2024).

European Union Agency of Fundamental Rights, Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level: guidance (2020).

Fisher/McManus/Kalbaugh/Walker, Phase I trial compensation: How much do healthy volunteers actually earn from clinical trial enrollment? - Jill A Fisher, Lisa McManus, Julianne M Kalbaugh, Rebecca L Walker, Clinical Trials 18, 2021.)

Handig Christian, Fotomotiv - Schutz oder Freiheit?, ipCompetence 2011 H 6, 54

Handig Christian/Hofmarcher Dominik/Kucsko Guido (Hrsg), urheber.recht[3] (2023)

He, From Privacy-Enhancing to Health Data Utilisation: The Traces of Anonymisation and Pseudonymisation in EU Data Protection Law, DISO 2, 2023, 16.

Herda Helene, Die Verwendung von Patientenbildern durch die Krankenanstalt: Zustimmungserfordernis für Patienten?, RdM 2024/27

Hummel/Braun/Dabrock, Own Data? Ethical Reflections on Data Ownership, Philosophy & Technology 2021, 545.
Kahrass/Bossert/Schürmann/Strech, Details of risk–benefit communication in informed consent documents for phase I/II trials, 2021.

Klement, Art. 8 DSGVO, in Simitis/Hornung/Spiecker Döhmann (Hrsg), Datenschutzrecht DSGVO mit BDSG (2023).

Kletečka Andreas/Schauer Martin (Hrsg), ABGB-ON (2017)

Lachmayer/Souhrada-Kirchmayer, Datenschutzrecht in der wissenschaftlichen Forschung, zfhr 2018, 153 (157)).

Micheli et al, Mapping the landscape of data intermediaries, 24.08.2023.

Mirchev/Mircheva/Kerekovska, The Academic Viewpoint on Patient Data Ownership in the Context of Big Data: Scoping Review, Journal of Medical Internet Research 2020.

Molnár-Gábor, Ausgestaltung der Einwilligung in die Datenspende für die Gesundheitsforschung, Datenschutz und Datensicherheit – DuD 2021, 799 (801).
Neuman, Why We Should Get Paid for Our Online Data, TIME 2023, https://time.com/6340676/get-paid-personal-online-data-essay/.

Neumayr Matthias/Resch Reinhard/Wallner Felix (Hrsg), Gmundner Kommentar zum Gesundheitsrecht[2] (2012)

Podda/Vigna, Anonymization Between Minimization and Erasure: The Perspectives of French and Italian Data Protection Authorities in Kö/Francesconi/Kotsis/Tjoa/Khalil (Hrsg), Electronic Government and the Information Systems Perspective: 10th International Conference, EGOVIS 2021, Vol. 12926, Proceedings (2021), 103.

Prainsack/Forgó, Why paying individual people for their health data is a bad idea, Nature Medicine 28, 2022, 1989.

Rummel Peter/Lukas Meinhard (Hrsg), Kommentar zum Allgemeinen bürgerlichen Gesetzbuch[4] (2021)

Schwimann Michael/Kodek Georg E. (Hrsg), ABGB Praxiskommentar[5] (2018).

Slokenberga/Tzortzatou/Reichel, GDPR and Biobanking: Individual Rights, Public Interest and Research Regulation across Europe 43 (2021) 24.

Thiele Clemens/Burgstaller Peter (Hrsg), Urheberrechtsgesetz[4] (2022)

Tzanou, Health Data Privacy under the GDPR (2021),7.

Urbano, The untamed and discreet role of data brokers in surveillance capitalism: A transnational and interdisciplinary overview, Internet Policy Review 11, 2022.

Wessels/Laubach/Buxmann, Personenbezogene Daten in der digitalen Ökonomie – Eine wirtschaftliche und juristische Betrachtung, in In: Ochs/Friedewald/Hess/Lamla (eds) Die Zukunft der Datenökonomie. Medienkulturen im digitalen Zeitalter, Springer VS.

Yeh, Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers, Telecommunications Policy 42, 2018.

11. Abkürzungsverzeichnis

ABGB	Allgemeines Bürgerliches Gesetzbuch
Abs	Absatz
AHDDS	Austrian Health Data Donation Space
AIA	AI Act
AIT	Austrian Institute of Technology GmbH
Art	Artikel
bzw.	beziehungsweise
DA	Data Act
dBVerfG	deutsches Bundesverfassungsgericht
DGA	Data Governance Act
dGG	deutsches Grundgesetz
DGF	Data Governance Framework (im Rahmen des Forschungsprojekts Smart FOX erstellt)
DSFA	Datenschutzfolgeabschätzung
DSFA-VO	Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung
DSG	Datenschutzgesetz
DSGVO	Datenschutzgrundverordnung
EHDS	European Health Data Space
ELGA	Elektronische Gesundheitsakte
ELGA-VO	ELGA-Verordnung
EMRK	Europäische Menschenrechtskonvention
etc.	et cetera
EU	Europäische Union

evtl.	eventuell
FOG	Forschungsorganisationsgesetz
gem.	gemäß
ggb.	gegebenenfalls
GÖG	Gesundheit Österreich GmbH
GTelV	Gesundheitstelematikverordnung
GTelG	Gesundheitstelematikgesetz
GRC	Charta der Grundrechte der Europäischen Union
grds.	grundsätzlich
inkl.	inklusive
IoT	Internet of Things
LBI DPHS	Ludwig Bolzmann Institut - Digital Health and Patient Safety
lit	litera
OGH	Oberster Gerichtshof
u.a./u.A.	unter Anderem
UNIVIE	Universität Wien
UrhG	Urheberrechtsgesetz
vgl.	vergleiche dazu
z.B.	zum Beispiel