



MASTER THESIS | MASTER'S THESIS

Titel | Title

Revolution im Datenzugang - Eine rollenbezogene Darstellung der
Sekundärnutzung elektronischer Gesundheitsdaten im Europäischen
Gesundheitsdatenraum (EHDS)

verfasst von | submitted by

Mag.iur. Michael Schmidbauer

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

Master of Laws (LL.M.)

Wien | Vienna, 2025

Studienkennzahl lt. Studienblatt |
Degree programme code as it appears on
the student record sheet:

UA 992 942

Universitätslehrgang lt. Studienblatt |
Postgraduate programme as it appears on
the student record sheet:

Informations- und Medienrecht

Betreut von | Supervisor:

Univ.-Prof. Mag. Dr. Nikolaus Forgó

Danksagung/Acknowledgment

Mein ausdrücklicher Dank gilt dem Team des Christian Doppler Labors für Maschinelles Lernen zur Präzisionsbildgebung:

Prof. *Georg Langs*, Prof. *Helmut Prosch*, Dr. *Philipp Seeböck* und Dr. *Roxane Licandro* für den fruchtbaren interdisziplinären Austausch

Prof. *Nikolaus Forgó* für die Betreuung der Masterarbeit, das entgegengebrachte Vertrauen in allen Aspekten meiner Arbeit und das große Privileg, forschend am Institut für Innovation und Digitalisierung im Recht tätig sein zu dürfen

Saskia Kaltenbrunner für die außerordentlich angenehme Zusammenarbeit, die anregenden Diskussionen und ihre Freundschaft

Christian Doppler Laboratory for Machine Learning Driven Precision Medicine, Department of Biomedical Imaging and Image-guided therapy, Medical University Vienna.

The financial support by the Austrian Federal Ministry for Economy, Energy and Tourism, the National Foundation for Research, Technology and Development and the Christian Doppler Research Association is gratefully acknowledged.

Inhaltsverzeichnis

1 Einleitung.....	5
1.1 Grundkonzept des EHDS.....	5
1.2 Rollenverteilung im EHDS	8
2 Datennutzer	11
2.1 Datenantrag	11
2.1.1 Zuständigkeit	11
2.1.2 Inhalt	13
2.1.3 Zweck der Verarbeitung.....	15
2.1.4 Opt-Out.....	17
2.1.5 Datenschutzrechtliche Rollenverteilung	19
2.2 Datenverarbeitung	21
2.2.1 Sichere Verarbeitungsumgebung.....	21
2.2.2 Anonymisierung und Pseudonymisierung	22
2.2.2.1 Vorgaben im EHDS	22
2.2.2.2 Anforderungen an Datennutzer.....	25
2.2.3 Verarbeitungsgrundlage pseudonymisierter Daten.....	28
2.2.3.1 Art 6 Abs 1 lit e DSGVO – Öffentliches Interesse	29
2.2.3.2 Art 6 Abs 1 lit f DSGVO – Berechtigtes Interesse	34
2.2.4 Zweckbindung und Datenminimierung.....	36
2.3 Pflichten der Datennutzer nach erfolgter Verarbeitung	38
2.3.1 Betroffenenrechte.....	38
2.3.2 Information der Betroffenen über klinisch signifikante Resultate	40
2.3.3 Veröffentlichung und Publikation der Ergebnisse	41

2.3.4 Begleichen der Kosten	43
3 Dateninhaber	44
3.1 Datenabfrage	44
3.2 Geistiges Eigentum und Geschäftsgeheimnisse	47
3.2.1 Rechte an Daten.....	47
3.2.1.1 Datenbankschutz durch Urheberrecht und verwandte Schutzrechte	48
3.2.1.2 Sonstige geschützte elektronische Gesundheitsdaten	54
3.2.1.3 Geschäftsgeheimnisschutz.....	55
3.2.2 Abwägungen im EHDS.....	56
3.3 Vertrauenswürdige Dateninhaber.....	59
3.4 Vergütung	62
4 Zusammenfassung und Fazit	66
5 Abstract	69
6 Literaturverzeichnis.....	70
7 Judikaturverzeichnis.....	79

1 Einleitung*

1.1 Grundkonzept des EHDS

Unter dem Eindruck des fehlenden Datenaustausches während der COVID-19-Pandemie schlug die EU-Kommission am 3.5.2022, auf die Europäische Datenstrategie¹ aufbauend, eine Verordnung über den Europäischen Raum für Gesundheitsdaten (European Health Data Space, kurz EHDS) als einen von neun bereichsspezifischen, EU-weiten Datenräumen vor.² Die EHDS-VO (im Folgenden: EHDS)³ wurde am 5.3.2025 im Amtsblatt der Europäischen Union kundgemacht, ihre Bestimmungen werden gestaffelt nach den Vorgaben in Art 105 EHDS über die darauf folgenden Jahre anwendbar.

Der EHDS verfolgt zwei Ziele gleichzeitig: Einerseits soll durch ein Regelwerk für grenzübergreifende EHR (Electronic Health Records) die Kontrolle der einzelnen betroffenen Personen über ihre Gesundheitsdaten erhöht werden. Dafür ist gem Art 23 EHDS MyHealth@EU als zentrale Plattform für den grenzüberschreitenden Datenaustausch angedacht. Andererseits sollen bereits erhobene oder erstellte Daten für andere als die ursprünglichen Zwecke, unter anderem für Forschung, Dritten zur Sekundärnutzung zugänglich gemacht werden.⁴ Diese Masterthesis widmet sich der

* Diese Master Thesis ist Ergebnis der Forschung des Autors im rechtswissenschaftlichen Arbeitspaket des Christian Doppler Labors für Maschinelles Lernen zur Präzisionsbildung. Das CD-Labor ist ein interdisziplinäres Forschungsprojekt zur Integration von künstlicher Intelligenz und Machine Learning in der onkologischen Bildgebung und klinischen Entscheidungsfindung. Das Institut für Innovation und Digitalisierung im Recht, an welchem der Autor beschäftigt ist, nimmt als Kooperationspartner am CD-Labor teil.

¹ *Europäische Kommission*, Europäische Datenstrategie, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de (abgefragt am 14.4.2025).

² Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten, COM/2022/197 fin.

³ Verordnung (EU) 2025/327 des Europäischen Parlaments und des Rates vom 11. Februar 2025 über den europäischen Gesundheitsdatenraum sowie zur Änderung der Richtlinie 2011/24/EU und der Verordnung (EU) 2024/2847, ABl L 2025/327.

⁴ *Löffler/Kastelitz*, Was ist der Europäische Raum für Gesundheitsdaten (EHDS)?, *Dako* 2023, 79.

eingehenden Behandlung letzterer Bestimmungen, normiert in Kapitel IV EHDS und im Wesentlichen anwendbar ab 26.3.2029.

Die Sekundärnutzungsbestimmungen des EHDS zielen auf das unionsweite Aufbrechen von Datensilos ab, in denen sich Gesundheitsdaten derzeit befinden.⁵ Im Gesundheitsbereich Österreichs sehen sich Forschende mit einer unübersichtlichen Fülle an öffentlichen Quellen zu Real World Data (RWD) konfrontiert, welche ebenso viele uneinheitliche Zugangsverfahren zur Folge haben. Das Fehlen eines zentralen Datensatzkatalogs mit klaren Zugangsregeln ist demnach als großes Hemmnis im Bereich der Forschung und evidenzbasierten Politikgestaltung zu werten.⁶ Für Zugang zu externen Datensätzen sind Forschende daher regelmäßig auf bilaterale Kooperationen mit Dateninhabern angewiesen.

Versuche, bestehende Datensilos zumindest auf nationaler Ebene aufzubrechen, schafften für den Gesundheitsbereich bis dato keine zufriedenstellenden Ergebnisse. Die Etablierung des Austrian Micro Data Centers (AMDC) im Jahr 2022 ist als ein solcher Versuch zu werten. Hierbei wurde in der Bundesanstalt Statistik Austria eine Stelle geschaffen, welche Forschenden den Zugang zu Statistik-Mikrodaten nach dem Bundesstatistikgesetz⁷ und Registerdaten nach dem FOG⁸ ermöglicht.⁹ Für Forschende im Gesundheitsbereich wäre gem § 31a Bundesstatistikgesetz iVm § 2d Abs 2 Z 3 FOG insbesondere der Zugang zu jenen Daten von Interesse, welche in Register der Bundesverwaltung geführt werden. Wissenschaftlichen Einrichtungen gem § 2b Z 12 FOG wird durch § 2d Abs 2 Z 3 FOG ein eigener Erlaubnistatbestand für die Verarbeitung dieser Daten gewährt. Der Zugang zu solchen Registern muss jedoch gem § 38b FOG durch eine Verordnung des Wissenschaftsministers im Einvernehmen mit dem Gesundheitsminister geschaffen werden, da das FOG und das Bundesstatistikgesetz nur den Rahmen für die Registerforschung schaffen, aber per se keine spezifischen Register freigeben. Dies ist im

⁵ *Heinzke*, Ein neues Datenrecht für die EU: Digitaler Wandel zum Wohle aller?, BB 2022 H 18, 1.

⁶ *Mikl et al.*, A national evaluation analysis and expert interview study of real-world data sources for research and healthcare decision-making, Scientific Reports 2024, 9751.

⁷ Bundesgesetz über die Bundesstatistik (Bundesstatistikgesetz 2000), BGBl. Nr. 163/1999.

⁸ Bundesgesetz über allgemeine Angelegenheiten gemäß Art. 89 DSGVO und die Forschungsorganisation (Forschungsorganisationsgesetz – FOG), BGBl. Nr. 341/1981.

⁹ *Kotschy*, Registerforschung nach der Novelle 2021 zum FOG, zfhr 2022, 139.

Gesundheitsbereich jedoch bis dato nicht geschehen,¹⁰ was von Interessengemeinschaften wie der Plattform Registerforschung¹¹ bemängelt wird. Selbst bei Freigabe der Gesundheitsdaten aus den bundesgesetzlich vorgesehen Registern iSd § 2b Z 10 FOG bestünden durch die föderale Struktur des Gesundheitswesens weiterhin Datensilos der Landesverwaltung, deren Inhalt nicht der Forschung zugänglich wäre. Auch Datenbestände Privater wären nicht davon betroffen.

Daneben wurde durch den Data Governance Act (DGA)¹² auf EU-Ebene bereits ein rechtliches Rahmenwerk für die Förderung des Datenaustausches von öffentlichen Stellen geschaffen. Der DGA leistet zwar organisatorische Vorarbeit für das institutionalisierte Teilen von Daten, normiert jedoch keine Pflicht für öffentliche oder private Stellen, Daten tatsächlich zur Verfügung zu stellen.¹³

Das soll durch den EHDS geändert werden. Aufbauend auf dem allgemeinen Rahmenwerk des DGA sollen verpflichtende Bestimmungen für das Teilen von Gesundheitsdaten normiert und somit Datensilos für Zwecke der Sekundärnutzung geöffnet werden.¹⁴

¹⁰ jedoch im Regierungsprogramm der Regierung Stocker I bis zum Stichtag 1.7.2026 vorgesehen: *Bundesregierung*, Regierungsprogramm Stocker I, https://www.dievolkspartei.at/Download/Regierungsprogramm_2025.pdf, 179 (abgefragt am 14.4.2025).

¹¹ *Plattform Registerforschung*, <https://www.registerforschung.at> (abgefragt am 14.4.2025).

¹² Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), ABl L 2022/152.

¹³ *Knyrim/Urban*, DGA, DMA, DSA, DA, AI-Act, EHDS - ein Überblick über die europäische Datenstrategie (Teil I), *Dako* 2023, 55 (57).

¹⁴ *Terzis*, Compromises and Asymmetries in the European Health Data Space, *European Journal of Health Law* 2023, 345 (348).

1.2 Rollenverteilung im EHDS

Für die Umsetzung der Sekundärnutzungsbestimmungen unterscheidet der EHDS vier Rollen: (Gesundheits-)Datennutzer, (Gesundheits-)Dateninhaber, datenschutzrechtlich Betroffene und (Gesundheitsdaten-)Zugangsstellen. Datennutzer, Dateninhaber und die Zugangsstellen sind dabei gänzlich neue Kategorien, welche durch den EHDS eingeführt werden. Datenschutzrechtlich Betroffene sind auch unter diesem System weiterhin relevant.

Datennutzer sind gem Art 2 Abs 2 lit u EHDS natürliche oder juristische Personen, welche im System der Sekundärnutzung rechtmäßig Zugang zu elektronischen Gesundheitsdaten erhalten haben. Hierfür muss ein Antrag auf Zugang zu Gesundheitsdaten (Datenantrag) gem Art 67 EHDS positiv beurteilt worden sein.

Der Begriff „Dateninhaber“ ist unglücklich gewählt, weil er fälschlicherweise eine sachenrechtliche Behandlung des immateriellen Guts Daten suggeriert.¹⁵ Art 2 Abs 2 lit t EHDS versteht darunter, in äußerst komplexer Wortwahl, eine natürliche oder juristische Person oder öffentliche Stelle oder Behörde, welche die Pflicht oder das Recht hat, elektronische Gesundheitsdaten für bestimmte Zwecke, einschließlich der Gesundheitsversorgung und Forschung, zu verarbeiten. Dabei ist unerheblich, ob sie öffentlicher oder privater Natur sind und ob sie gewinnorientiert oder nicht-gewinnorientiert sind.¹⁶ Der Anspruch des EHDS, einen möglichst umfassenden Katalog von Gesundheitsdaten zur Sekundärnutzung freizugeben,¹⁷ wird durch diese Definition deutlich. Ausgenommen von den Pflichten der Dateninhaber sind gem Art 50 Abs 1 EHDS lediglich natürliche Personen, einschließlich einzeln tätige Forschende und Kleinstunternehmen iSv Artikel 2 Abs 3 des Anhangs der Empfehlung 2003/361/EG der Kommission.¹⁸ Kleinstunternehmen sind nach dieser Definition Unternehmen, welche weniger als zehn Personen beschäftigen und deren Jahresumsatz bzw Jahresbilanz 2 Mio.

¹⁵ Näheres unter 3.2.1.

¹⁶ ErwGr 59 EHDS.

¹⁷ ErwGr 54 EHDS.

¹⁸ Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl. L 124, 36.

EUR nicht überschreiten. Mitgliedsstaaten steht es gem Art 50 Abs 2 EHDS jedoch frei, diese Ausnahmen durch nationale Gesetzgebung aufzuheben.

Bei der Erläuterung der Rollenverteilung im EHDS sollte zusätzlich nicht übersehen werden, dass die natürlichen Personen, auf die sich die genutzten Daten beziehen, weiterhin Betroffene gem Art 4 Z 1 DSGVO sind. Da der EHDS auf das Fundament der DSGVO aufsetzt und, wie es bei den Rechtsakten der Europäischen Datenstrategie üblich ist, dieses gem Art 1 Abs 3 EHDS „unberührt“ lassen möchte,¹⁹ sind die datenschutzrechtlichen Regelungen für Betroffene auch im System der Sekundärnutzung weiterhin relevant.²⁰

Für die Abwicklung des Datenzugangs werden gem Art 55 EHDS in allen Mitgliedstaaten Zugangsstellen für Gesundheitsdaten eingerichtet, welche als Intermediäre²¹ zwischen den drei oben genannten Akteuren agieren sollen. Sie veröffentlichen Listen von verfügbaren Datensätzen als Datensatzkataloge, bearbeiten Datenanträge, stellen die elektronischen Gesundheitsdaten in einer sicheren Verarbeitungsumgebung zur Verfügung und sollen dadurch als Drehscheibe zwischen Datennutzer und Dateninhabern agieren. Hierfür ist breite Expertise im Datenschutz, geistigen Eigentum, Geschäftsgeheimnisschutz und insbesondere an der Schnittstelle Medizin und (IT-)Technik gefordert. Ursprünglich war die Gesund Österreich GmbH alleine als Zugangsstelle vorgesehen.²² Gemäß Regierungsprogramm der Regierung Stocker I soll hierfür jedoch auf die Statistik Austria, das AMDC und die Gesundheit Österreich GmbH zurückgegriffen werden,²³ wodurch Stand April 2025 noch unklar ist, welche dieser Einrichtungen konkret die Behördenfunktion als Zugangsstelle gem Art 55 EHDS zukommen wird.

¹⁹ kritisch Böning, EHDS: Ein ambitioniertes Projekt mit Folgefragen, ZD-Aktuell 2024, 01695.

²⁰ Näheres unter 2.3.1.

²¹ Buchholtz/Schmalhorst/Brauneck, Der Gesetzgeber im Spannungsfeld zwischen Patientensouveränität und Forschungsinteressen – eine Bewertung der neuesten Gesetzgebungsaktivitäten auf EU-Ebene und nationaler Ebene, MedR 2024, 471 (476).

²² Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz, Presseaussendung betreffend EHDS-Umsetzung in Österreich, https://www.ots.at/presseaussendung/OTS_20240313_OT0157/rauch-europaeischer-gesundheitsdatenraum-ermoeeglicht-verbesserungen-fuer-patientinnen-und-forschung (abgefragt am 14.4.2025).

²³ Bundesregierung, Regierungsprogramm, 178.

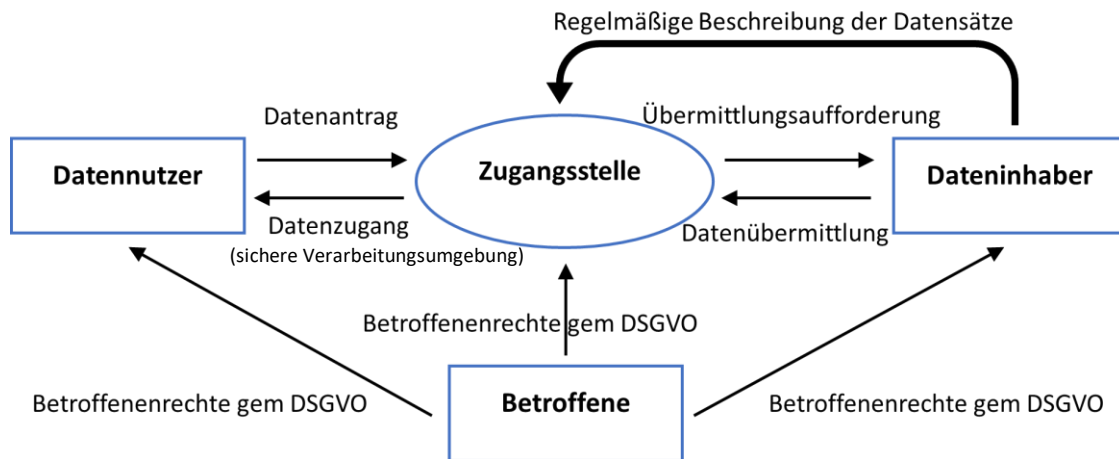


Abb 1: Vereinfachte Darstellung der Rollen im Sekundärnutzungssystem des EHDS

Die Konzeption des EHDS ist gemäß der oben beschriebenen Aufteilung und der Abb 1 rollenbezogen. Es kann demnach ein und dieselbe Einrichtung sowohl als Datennutzer als auch als Dateninhaber von dem EHDS erfasst werden. In dieser Arbeit sollen daher die wesentlichen Sekundärnutzungsbestimmungen aus der Sicht beider Rollen kritisch erläutert und insbesondere auf deren Zusammenspiel mit datenschutzrechtlichen und urheberrechtlichen Bestimmungen eingegangen werden.

2 Datennutzer

2.1 Datenantrag

Natürliche oder juristische Personen, die Zugriff auf elektronische Gesundheitsdaten zur Sekundärnutzung erhalten möchten, haben im System des EHDS die Wahl zwischen den Instrumenten Datenantrag und Datenanfrage. Die Datenanfrage gem Art 69 EHDS soll Datennutzern lediglich Zugang zu anonymisierten Daten in einem statistischen Format verschaffen und deckt sich im Wesentlichen inhaltlich mit dem Datenantrag. Da sie auch systematisch als eine Abwandlung des Datenantrags zu sehen ist, wird im Folgenden nur auf diese Grundform gem Art 68 EHDS näher eingegangen.

Bei Erfüllung der Voraussetzungen des Datenantrags besteht gegenüber den Zugangsstellen gem Art 68 Abs 3 EHDS ein öffentlich-rechtlicher Anspruch auf Datenzugang.²⁴ Die Entscheidung der Zugangsstellen soll diesbezüglich eine gebundene sein, ohne umfassendes Ermessen.²⁵ Fehlerhafte Entscheidungen sollten als Verwaltungsakt,²⁶ der nach österreichischem Verwaltungsverfahrenrecht in Bescheidform zu ergehen hat, durch Bescheidbeschwerde angefochten werden können. Auch hier bleibt jedoch die konkrete Ausgestaltung den Mitgliedsstaaten überlassen, da durch das Unionsrecht die Verfahrensautonomie der Mitgliedsstaaten gewahrt bleibt.²⁷

2.1.1 Zuständigkeit

Der Datenantrag wird an jene Zugangsstelle gestellt, welche die gewünschten Datensätze in ihrem Datensatzkatalog ersichtlich gemacht hat.²⁸ Werden Daten von mehreren nationalen Datensatzkatalogen benötigt, müssen nicht mehrere Anträge an alle Zugangsstellen gestellt werden, sondern nur an die nationale Zugangsstelle des Antragstellers oder eine der Zugangsstellen der angeforderten Datensätze. Diese leitet den

²⁴ Darin kann der wesentliche Unterschied zwischen DGA und EHDS erblickt werden.

²⁵ *Wehde/Brandenberg in Hoeren/Sieber/Holznagel*, Handbuch Multimedia-Recht (Werkstand: 61. EL März 2024), Teil 16.8 Sekundärnutzung von Gesundheitsdaten, Rz 18.

²⁶ Art 2 Abs 2 lit v EHDS.

²⁷ *Öhlinger/Potacs*, EU-Recht und staatliches Recht⁷ (2020), 160.

²⁸ Alle nationalen Datensatzkataloge werden gem Art 79 Abs 1 EHDS in einem öffentlich einsehbaren Datensatzkatalog der Kommission („EU-Datensatzkatalog“) gesammelt.

Antrag sodann an alle betroffenen Zugangsstellen weiter.²⁹ Die Zugangsstelle, an die der Antrag gestellt wurde, bleibt jedoch verfahrensrechtlich nicht alleine zuständig, wie es beispielsweise die federführende Aufsichtsbehörde im System der DSGVO gem Art 56 DSGVO tut. Art 68 Abs 5 EHDS schließt einen solchen One-Stop-Shop für die Sekundärnutzung aus, indem normiert wird, dass die einzelnen Zugangsstellen jeweils für Entscheidungen betreffend ihrer nationalen Datensatzkataloge zuständig sind. Lediglich eine Informationspflicht der einzelnen Zugangsstellen über ihre jeweiligen Entscheidungen ist vorgesehen. Für Antragsteller bedeutet dies bei Datenanträgen betreffend mehrerer nationalen Datensatzkatalogen einen erheblichen Mehraufwand, da diese nicht nur den jeweiligen nationalen verfahrensrechtlichen Bestimmungen entsprechen müssen, sondern auch materiell-rechtliche Divergenzen zu berücksichtigen haben.³⁰ Es kann somit durchaus der Fall eintreten, dass bei demselben Antrag manche Daten pseudonymisiert bereitgestellt werden, während andere nur anonymisiert oder gar nicht zur Verfügung gestellt werden.

Dadurch wird jedoch die Praxis des Forum Shoppings abgeschwächt, bei der von Antragstellern federführende Zuständigkeiten bewusst ausgenutzt werden könnten, indem der Antrag bei derjenigen Zugangsstelle gestellt würde, welche für den Antragssteller mutmaßlich das beste Ergebnis sicherstellt.³¹ Die Möglichkeit solcher Praktiken im System des EHDS wurde in der Literatur teilweise befürchtet,³² ist aber in der aktuellen Version des EHDS durch die parallelen Zuständigkeiten nur in der abgeschwächten Form erhalten geblieben, dass Datennutzer zwar nationale Datensätze aus günstigeren Rechtsordnungen

²⁹ Art 67 Abs 3 EHDS.

³⁰ für das Beispiel der Anonymisierung siehe 2.2.2.2.

³¹ Wäre die Zugangsstelle, an die der Datenantrag gestellt wird, federführend für die Datenaufbereitung und Datenbereitstellung zuständig, so könnte das Inkludieren eines einzigen Datensatzes einer Rechtsordnung mit lockererem Ansatz alle angeforderten Datensätze begünstigen. Würden beispielsweise französische Datensätze benötigt, so könnten durch das Inkludieren eines Datensatzes aus einem anderen Mitgliedstaat die notorisch strengen Anonymisierungsvoraussetzungen der französischen Datenschutzbehörde, denen dann wohl auch die französische Zugangsstelle folgen würde, umgangen werden.

³² *Marelli et al.*, The European health data space: Too big to succeed?, Health policy 2023, 104861 (2).

anfordern können,³³ jedoch keine günstigere Zugangsstelle federführend für alle Datensätze zuständig gemacht werden kann.

Zur besseren Abstimmung der Mitgliedsstaaten im Bereich der Sekundärnutzung dient die von der Kommission gem Art 75 EHDS einzurichtende Plattform HealthData@EU, welche insbesondere die für die grenzüberschreitende Bereitstellung von elektronischen Gesundheitsdaten nötige IT-Infrastruktur schafft. Weiters soll dadurch gem Art 75 Abs 5 EHDS auch die Möglichkeit der Einbeziehung von Datensatzkatalogen aus Drittländern und internationalen Organisationen gegeben sein.

2.1.2 Inhalt

Der Datenantrag muss den in Art 67 Abs 2 EHDS normierten Inhalt aufweisen:

1. Angaben über die Identität des Antragstellers und natürliche Personen, welche Zugriff auf die Daten haben sollen (Art 67 Abs 2 lit a EHDS);³⁴
2. die beabsichtigte Verwendung der elektronischen Gesundheitsdaten inklusive Zweck gem Art 53 Abs 1 EHDS (Art 67 Abs 2 lit b EHDS);³⁵
3. eine detaillierte Beschreibung der geplanten Verarbeitungsschritte und der daraus erhoffte Nutzen, auch in Bezug auf die Zwecke gem Art 53 Abs 1 EHDS (Art 67 Abs 2 lit c EHDS);
4. eine Beschreibung der angefragten elektronischen Gesundheitsdaten inklusive des gewünschten Formats; bei Datenanträgen betreffend Datensätzen aus mehreren Mitgliedsstaaten auch die geografische Abdeckung (Art 67 Abs 2 lit d EHDS);
5. die Angabe, ob die elektronischen Gesundheitsdaten in anonymisierter oder pseudonymisierter Form bereitgestellt werden sollen, inklusive Begründung bei Antrag von pseudonymisierten Daten (Art 67 Abs 2 lit e EHDS);³⁶

³³ *Cimina*, The Proposal for a European Health Data Space: between pursued objectives and data protection challenges, ERA Forum 2023, 343 (358).

³⁴ inklusive Angaben über die fachliche Qualifikation des Antragstellers in Bezug auf ethische Praxis und geltende Rechts- und Verwaltungsvorschriften gem Art 68 Abs 1 lit d EHDS.

³⁵ Näheres sogleich unter 2.1.3.

³⁶ Näheres unter 2.2.2.1.

6. eine Beschreibung von zusätzlichen, eigenen Datensätzen, welche in der sicheren Verarbeitungsumgebung benötigt werden (Art 67 Abs 2 lit f EHDS);³⁷
7. eine Beschreibung der Schutzmaßnahmen, welche Missbrauch der elektronischen Gesundheitsdaten verhindern und die Rechte und Interessen der Datennutzer und Betroffenen schützen sollen. Insbesondere sollen bei der Zurverfügungstellung anonymisierter elektronischer Gesundheitsdaten Schutzmaßnahmen gegen Re-Identifizierung angeführt werden (Art 67 Abs 2 lit g EHDS);
8. eine Schätzung des Zeitraums, in dem die elektronischen Gesundheitsdaten in der sicheren Verarbeitungsumgebung zur Verfügung gestellt werden sollen (Art 67 Abs 2 lit h EHDS);
9. eine Beschreibung der für ein sicheres Umfeld erforderlichen Instrumente und Rechenressourcen (Art 67 Abs 2 lit i EHDS);³⁸
10. Informationen über die Bewertung ethischer Aspekte der Verarbeitung gemäß nationalem Recht (Art 67 Abs 2 lit j EHDS);
11. bei Stützen auf die Opt-Out Gegen Ausnahme von Art 71 Abs 4 EHDS eine Erklärung der Erfüllung der Voraussetzungen der nationalrechtlichen Durchführungsbestimmung (Art 67 Abs 2 lit j EHDS);
12. bei Beantragung pseudonymisierter Daten die Verarbeitungsgrundlage gemäß Art 6 Abs 1 DSGVO (Art 67 Abs 4 EHDS).³⁹

Insbesondere die genaue Beschreibung der geplanten Verarbeitungsschritte wird für den Erfolg des Datenantrags von entscheidender Bedeutung sein. Daher sollten zum Zweck der Abgrenzung auch nicht geplante Verarbeitungsschritte beschrieben werden.⁴⁰ Eine Orientierungshilfe für Datenanträge wurde auch von dem Forschungsprojekt HealthData@EU Pilot ausgearbeitet.⁴¹

³⁷ Näheres unter 2.2.1.

³⁸ Näheres unter 2.2.1.

³⁹ Näheres unter 2.2.3.

⁴⁰ *Quinn/Elyyne/Yao*, Computer Law & Security Review 54, 105993 (9).

⁴¹ *HealthData@EU Pilot*, D7.1, https://ehds2pilot.eu/wp-content/uploads/2024/04/HealthData@EU-Pilot-Deliverable-7.1_FIN.docx-1-1.pdf (abgefragt am 14.4.2025).

2.1.3 Zweck der Verarbeitung

Eine Datengenehmigung wird nur für bestimmte, in Art 53 Abs 1 EHDS aufgelistete Zwecke erteilt. Die Datennutzer müssen ihre geplante Datenverarbeitung einem oder mehreren⁴² dieser Zwecke zuordnen und diesen im Datenantrag angeben. Die Fülle und teilweise Überschneidung dieser Zwecke im Erstentwurf des EHDS hatte das Potential, Antragsteller zu überfordern.⁴³ Insbesondere für das Training von KI-Modellen zur wissenschaftlichen Forschung war in Art 34 EHDS-E unklar, welche Zwecke angegeben werden sollen. So gab der Entwurf sowohl den breiter formulierten Zweck der wissenschaftlichen Forschung in Art 34 Abs 1 lit e EHDS-E, als auch den engeren Zweck des Trainings von Algorithmen in KI-Systemen in Art 34 Abs 1 lit g EHDS-E und der personalisierten Gesundheitsversorgung in Art 34 Abs 1 lit h vor. Nun ist das Trainieren, Erproben und Bewerten von Algorithmen in KI-Systemen als Unterpunkt der wissenschaftlichen Forschung in Art 53 Abs 1 lit e EHDS vorgesehen, weswegen sich Forschende, die diesen Zweck im Zuge von wissenschaftlicher Forschung verfolgen, auf diese Bestimmung stützen können. Der Begriff der wissenschaftlichen Forschung ist grundsätzlich verordnungsautonom auszulegen. Der EHDS legt dabei einen breiten Forschungsbegriff zu Grunde. Darunter sollen sowohl Grundlagenforschung als auch die Weiterentwicklung bestehender Technologien wie Algorithmen fallen.⁴⁴

Da das Trainieren von KI-Modellen nun jedoch als Unterpunkt der wissenschaftlichen Forschung behandelt wird, ist davon auszugehen, dass bei Abschluss der Forschungstätigkeit zu einem KI-Modell, welches nicht mehr weiterentwickelt werden soll, der Zweck von Art 53 Abs 1 lit e EHDS nicht mehr als Datenzugangsgrundlage zusteht. Dabei könnte aber insbesondere das Up-to-Date halten dieser Modelle weiteren Datenzugang auf elektronische Gesundheitsdaten über den EHDS erfordern. Hierfür müssen also andere Zwecke gefunden werden, wobei beim Einsatz der Modelle für personalisierte Medizin Art 53 Abs 1 lit h EHDS eine mögliche Grundlage bilden könnte.

⁴² Art 68 Abs 1 lit b EHDS: „die angeforderten Daten sind in Bezug auf die im Antrag auf Zugang zu Gesundheitsdaten beschriebenen *Zwecke* erforderlich, angemessen und verhältnismäßig [...]“.

⁴³ für eine ausführliche Beschreibung aller Zwecke siehe *Quinn/Elyyne/Yao*, Will the GDPR Restrain Health Data Access Bodies Under the European Health Data Space (EHDS)?, Computer Law & Security Review 54, 105993 (4).

⁴⁴ ErwGr 61 EHDS.

Die Auswahl des Zwecks ist nicht nur für den Datenzugang an sich relevant, sondern auch in weiterer Folge bedeutsam und sollte daher mit Bedacht gewählt werden. Insbesondere ist zu beachten, dass, da die Datengenehmigung auf der Grundlage der Zwecke von Art 53 Abs 1 EHDS erteilt wird, der Datennutzer auch an diese während der gesamten Verarbeitungstätigkeit gebunden ist.⁴⁵

Darüber hinaus ist zu beachten, dass die Erteilung einer Datengenehmigung einer Verhältnismäßigkeitskontrolle gem Art 68 Abs 1 lit b EHDS unterliegt. Die Verarbeitung der angefragten Datensätze muss demnach notwendig sein, um den angegebenen Zweck zu erreichen und muss zu diesem in einem angemessenen Verhältnis stehen. Diese Verhältnismäßigkeitskontrolle ist auch auf die Bereitstellung anonymisierter Daten anwendbar, weswegen sie nicht ohne Weiteres mit der Interessenabwägung gem Art 6 Abs 1 lit f DSGVO gleichzusetzen ist.

Werden Daten in einem pseudonymisierten Format beantragt und soll die Interessenabwägung gem Art 6 Abs 1 lit f DSGVO für deren Verarbeitung als Verarbeitungsgrundlage gem Art 67 Abs 4 EHDS dienen,⁴⁶ ist zu beachten, dass der angegebene Zweck über die Verhältnismäßigkeitskontrolle von Art 68 Abs 1 lit b EHDS hinaus auch der Maßstab ist, an dem das überwiegende Interesse des Datennutzers zur Datenverarbeitung gemessen wird.⁴⁷

Zuletzt ist noch Art 54 EHDS zu beachten, der wiederum bestimmte Verarbeitungsvorgänge von der Sekundärnutzung ausschließt, welche grundsätzlich unter die Zwecke von Art 53 Abs 1 EHDS fallen könnten. Im medizinischen Forschungskontext relevant scheinen insbesondere Art 54 Abs 1 lit a und e EHDS. Art 54 Abs 1 lit a EHDS schließt Verarbeitungsvorgänge der angeforderten Gesundheitsdaten aus, welche zu Entscheidungen führen, die einer natürlichen Person oder einer Gruppe von Personen schaden und auf der Grundlage ihrer elektronischen Gesundheitsdaten getroffen werden. Verboten wird hier nicht das Training von KI-Modellen, welche eventuell zu schädlichen Entscheidungen führen können, sondern nur direkte Entscheidungen. Art 35 Abs 1 lit e EHDS ist eine Generalklausel, welche Verarbeitungsvorgänge ausschließt, die sich in

⁴⁵ Art 68 Abs 10 lit b iVm Art 68 Abs 11 und Art 61 Abs 1 EHDS.

⁴⁶ Näheres unter 2.2.3.2.

⁴⁷ *Wehde/Brandenberg*, Teil 16.8 Sekundärnutzung von Gesundheitsdaten in *Hoeren/Sieber/Holznagel*, Handbuch Multimedia-Recht (Werkstand: 61. EL März 2024), Rz 48.

Konflikt mit nationalen Ethikvorschriften befinden. Für die Genehmigung klinischer Studien müssten derartige Vorschriften jedoch ohnehin eingehalten werden.

2.1.4 Opt-Out

Gem Art 71 Abs 1 EHDS können Betroffene im System der Sekundärnutzung der Verarbeitung ihrer elektronischen Gesundheitsdaten jederzeit und ohne Angabe von Gründen widersprechen („Opt-Out“). Die Aufnahme dieser Möglichkeit in das System der Sekundärnutzung war einer der wesentlichen Streitpunkte in den Verhandlungen zum EHDS⁴⁸ und kann als Ersatz für die informierte Einwilligung als Verarbeitungsgrundlage gesehen werden.⁴⁹ Den Prozess hierfür müssen gem Art 72 Abs 2 EHDS die Mitgliedstaaten vorgeben. Wie genau dieser für Österreich aussehen wird, ist demnach noch nicht klar, wobei eine zentrale Opt-Out Stelle die naheliegende Lösung darstellt. Eine solche ist gem Art 10 Abs 1 EHDS auch für ein Opt-Out bezüglich Primärnutzungsbestimmungen des EHDS vorgesehen. Dort soll, wenn dies die Mitgliedsstaaten vorsehen, über den Zugangsdienst für elektronische Gesundheitsdaten die Möglichkeit des Opt-Out bestehen.

Die Mitgliedsstaaten können gem Art 71 Abs 4 EHDS jedoch vorsehen, dass unter bestimmten Umständen auch elektronische Gesundheitsdaten, für welche das Opt-Out Recht in Anspruch genommen wurde, für die Sekundärnutzung freigegeben werden können. Diese Gegen Ausnahme ist auf bestimmte Körperschaften, dazu zählen sowohl Behörden als auch private Körperschaften die öffentliche Aufgaben ausführen, und auf die in Art 71 Abs 4 lit a-c EHDS genannten Bedingungen beschränkt, welche wegen des beträchtlichen Eingriffs in die informationelle Selbstbestimmungen der Betroffenen hohe Anforderungen vorschreiben. So ist der Datenzugang trotz Opt-Out gem Art 71 Abs 4 lit b EHDS nur zulässig, wenn die gewünschten Datensätze nicht zeitnahe durch alternative Mittel und unter gleichen Bedingungen zugänglich gemacht werden können. Zusätzlich ist die Verarbeitung gem Art 71 Abs 4 lit a EHDS auf die Zwecke von Art 53 Abs 1 lit a-c EHDS – hierzu zählt die Verarbeitung zum Schutz der öffentlichen Gesundheit, Unterstützung regulatorischer Vorhaben und Gesundheitsstatistiken – und

⁴⁸ *Sokol*, European Health Data Space, Use of Data and Data Subjects’ Control over Their Own Health Data: Can an Opt-Out Restore the Balance?, *European Journal of Health Law* 2024, 365.

⁴⁹ *Afra*, An Assessment on Innovator’s Ability for Consent-Free Health Data Reuse, In the Context of the GDPR and EHDS: The Netherlands Case Study, *European Journal of Health Law* 2024, 475 (491).

wissenschaftliche Forschung aufgrund wichtiger öffentlicher Interessen beschränkt. Die Nennung wichtiger öffentlicher Interessen deutet darauf hin, dass an die Verarbeitung höhere Ansprüche als die bloße Verwendung für „gewöhnliche“ wissenschaftliche Forschungszwecke gestellt werden. Dabei wird in den Erwägungsgründen explizit die Deckung von medizinischem Bedarf, insbesondere bei seltenen Krankheiten und neu auftretenden Gesundheitsbedrohungen, erwähnt.⁵⁰

Die Einigung auf ein Opt-Out System im Trilogverfahren des EHDS ist aus Perspektive der Datennutzer prinzipiell zu begrüßen, da dies Bias in den Datensätzen eher verhindern kann als das verworfene Opt-In System.⁵¹ Durch die Möglichkeit des Opt-Out wird gleichzeitig der Wesensgehalt des Datenschutzrechts insofern gewahrt, als Betroffenen das Mitspracherecht bezüglich Verarbeitung ihrer elektronischen Gesundheitsdaten nicht gänzlich entzogen wird und die informationelle Selbstbestimmung weiter bei ihnen liegt.⁵² Somit scheint das System des Opt-Out den Optimalpunkt zwischen Grundrechtsschutz der Betroffenen und Nützlichkeit für Datennutzer darzustellen.

Die Gegen Ausnahme zur Verarbeitung trotz Opt-Out gem Art 71 Abs 4 EHDS und ihre konkrete Ausgestaltung ist jedoch aus grundrechtlicher Perspektive kritisch zu sehen. Die Möglichkeit des Umgehens des Opt-Out führt bei Betroffenen zu falschen Vorstellungen von der von ihnen ausgeübten Kontrolle über ihre elektronischen Gesundheitsdaten. In diesem Bereich kann nicht, wie Art 1 Abs 3 EHDS konstatiert, davon ausgegangen werden, dass die DSGVO durch den EHDS gänzlich unberührt belassen wird. Die ausnahmsweise Verarbeitung trotz Opt-Out steht insbesondere mit dem Grundsatz der Verarbeitung nach Treu und Glauben gem Art 5 Abs 1 lit a DSGVO in einem Spannungsverhältnis.⁵³ Dieser ordnet, trotz vagen normativen Gehalts, eine Fairnessklausel an, welche garantieren soll, dass Betroffene nicht in den vernünftigen Erwartungen enttäuscht werden, welche sie an die Datenverarbeitung auf der Grundlage ihrer Beziehung zu dem Verantwortlichen

⁵⁰ ErwGr 54 EHDS.

⁵¹ *Hermus et al.*, Opt-In versus opt-out for the secondary use of routinely recorded health data: A randomized controlled trial, *European Journal of Internal Medicine* 2025, 100.

⁵² *Raji*, 120.5 European Health Data Space in *Taeger/Pohle*, Computerrechts-Handbuch (Werkstand: 39. EL April 2024), Rz 30.

⁵³ *Raji*, 120.5 European Health Data Space in *Taeger/Pohle*, Computerrechts-Handbuch, Rz 32.

haben.⁵⁴ Um das durch die Opt-Out-Gegenausnahme geschaffene Erwartungsdefizit der Betroffenen auszugleichen, ist eine ausführlichere Information der Betroffenen über die Inanspruchnahme dieser Ausnahme essentiell. Eine solche ist im normativen Text des EHDS nicht vorgesehen, sollte jedoch, wie auch Art 71 Abs 4 EHDS andeutet, neben anderen Maßnahmen zum Schutz der Betroffenen in der nationalen Ausgestaltung der Gegenausnahme vorgesehen werden.

2.1.5 Datenschutzrechtliche Rollenverteilung

Gewisse datenschutzrechtliche Rollenverteilungen können den Abschluss von Vereinbarungen vor den geplanten Datenverarbeitungsvorgängen notwendig machen. Werden von zwei oder mehreren datenschutzrechtlich Verantwortlichen iSv Art 4 Z 7 DSGVO gemeinsam Entscheidungen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten getroffen, so ist von diesen eine Vereinbarung zwischen gemeinsam Verantwortlichen (Joint Controller Agreement) gem Art 26 Abs 1 DSGVO über die dort normierten Rechte und Pflichten der Verantwortlichen zu schließen. Bedient sich der Verantwortliche eines Auftragsverarbeiters iSv Art 4 Z 8 DSGVO, also einer rechtlich eigenständigen, natürlichen oder juristischen Person, welche im Auftrag des Verantwortlichen personenbezogene Daten ohne wesentliche eigene Entscheidungsbefugnis über Mittel und Zwecke dieser Verarbeitung verarbeiten soll, ist ein Auftragsverarbeitervertrag (Data Processing Agreement) gem Art 28 Abs 3 DSGVO über die Pflichten des Auftragsverarbeiters zu schließen. Gem ErwGr 72 EHDS sollen die Zugangsstellen beim Aufbereiten der elektronischen Gesundheitsdaten als Verantwortliche zu sehen sein, während Datennutzer bei Zurverfügungstellung von anonymisierten Daten aufgrund der Nichtanwendbarkeit der DSGVO keine datenschutzrechtliche Rolle übernehmen sollen. Somit ist bei Zurverfügungstellung von anonymisierten Daten keine Vereinbarung zwischen Datennutzern und der Zugangsstelle nötig. Werden pseudonymisierte Daten in der sicheren Verarbeitungsumgebung bereitgestellt, sollen gem ErwGr 79 EHDS für diesen Datenverarbeitungsprozess die Zugangsstellen als Auftragsverarbeiter der Datennutzer gelten. Diese Rollenverteilung wurde nicht nur in den nicht direkt rechtsverbindlichen Erwägungsgründen vorgesehen, sondern auch in den unmittelbar verbindlichen Rechtsvorschriften normiert. So gibt Art 74 Abs 1 EHDS diese Rollenverteilung auch rechtsverbindlich wieder.

⁵⁴ *Hötendorfer/Tschohl/Kastelitz* in *Knyrim*, *DatKomm* Art 5 DSGVO Rz 16 (Stand 7.5.2020, rdb.at).

Die rechtliche Normierung einer faktischen Beziehung und nicht deren Folgen, wie es Art 26 und Art 28 DSGVO eigentlich vorsehen,⁵⁵ führt vor allem bei den Datennutzern zur Rechtssicherheit, mag auf den Einzelfall jedoch nicht immer zutreffen. Wie schwierig die Normierung dieser faktischen Beziehung auch für die europäischen Rechtssetzer ist, zeigt der Vergleich zwischen dem Kommissionsvorschlag zum EHDS und der finalen Version deutlich. Während in Art 51 Abs 1 EHDS-E, im Einklang mit der betroffenenfreundlichen, weiten Definition der gemeinsamen Verantwortlichkeit,⁵⁶ noch die gemeinsame Verantwortlichkeit von Zugangsstelle und Datennutzer für alle Datenverarbeitungsschritte vorgesehen war,⁵⁷ soll die Zugangsstelle gemäß der finalen Version von Art 74 Abs 1 EHDS nun als bloßer Auftragsverarbeiter für die Bereitstellung der elektronischen Gesundheitsdaten fungieren. Ungeachtet dieser Überlegungen sollte ein Antragsteller die durch den EHDS normierte Rollenverteilung akzeptieren und mit der Zugangsstelle einen Auftragsverarbeitervertrag gem Art 28 Abs 3 DSGVO abschließen. Hierfür kann die Kommission gem Art 74 Abs 3 EHDS Muster zur Verfügung stellen. Der Abschluss dieses Vertrags ist gem Art 67 EHDS zwar nicht explizit Voraussetzung für eine Datengenehmigung, ist aber datenschutzrechtlich vor den Verarbeitungsvorgängen in der sicheren Verarbeitungsumgebung geboten. Zusätzlich könnte der Abschluss von Lizenzverträgen oder Geheimhaltungsvereinbarungen notwendig sein.⁵⁸

⁵⁵ Pachinger, Datenschutz-Verträge³ (2024), Rz 3.

⁵⁶ EuGH 5.6.2018, C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rz 28.

⁵⁷ Tschammler/Uecker, Verordnungsentwurf zur Schaffung eines Europäischen Gesundheitsdatenraums – erster Überblick mit Fokus auf die Nutzung von Gesundheitsdaten für Forschungs- und Entwicklungsvorhaben, ZD-Aktuell 2022, 01265.

⁵⁸ Näheres unter 3.2.2.

2.2 Datenverarbeitung

2.2.1 Sichere Verarbeitungsumgebung

Das institutionalisierte Ermöglichen der Sekundärnutzung von elektronischen Gesundheitsdaten im Rahmen des EHDS wirft naturgemäß grundrechtliche Bedenken auf. Die europäischen Rechtssetzer sind bei diesem Unterfangen insbesondere an Art 7 und 8 GRC und die DSGVO gebunden, welche den Rahmen hierfür vorgeben. Um datenschutzrechtlichen Bedenken entgegenzukommen, werden als Ausweg aus dem „Zielkonflikt zwischen Datenhunger und Datenschutzrecht“⁵⁹ Garantien zum Schutz der Betroffenen normiert. Diese sollen durch die Bereitstellung der elektronischen Gesundheitsdaten in einer sicheren Verarbeitungsumgebung gem Art 73 EHDS sichergestellt werden.

Das Konzept der sicheren Verarbeitungsumgebung, welche die Verarbeitung sensibler Daten durch Sicherheitsmaßnahmen ermöglichen soll, beschäftigt Forschende schon länger.⁶⁰ Auch Art 5 Abs 3 DGA schreibt für den Datenzugang die Bereitstellung in einer sicheren Verarbeitungsumgebung vor. Diese soll gem Art 2 Z 20 DGA der umfassenden Gewährleistung einer rechtssicheren Datenverarbeitung, insbesondere aus dem Blickwinkel des Datenschutzrechts, des geistigen Eigentums und des Geschäftsgeheimnisschutzes, dienen. Der DGA verweist hierfür in ErwGr 7 auf die Verordnung (EU) Nr. 557/2013,⁶¹ welche in Art 8 die Möglichkeit der Akkreditierung von Zugangseinrichtungen für den Zugang zu Eurostat-Daten der Europäischen Kommission vorsieht. Auch diese mussten gem Art 8 Abs 3 *leg cit* bereits hohe Standards in Bezug auf Datensicherheit und Datenmanagement erfüllen. Auf nationaler Ebene stellt insbesondere das AMDC bei Antrag auf Zugang zu Bundesstatistikdaten oder Registerdaten eine sichere Verarbeitungsumgebung zur Verfügung. Diese besteht bei Remote-Access gem § 31 Abs 3 Bundesstatistikgesetz aus einer virtuellen Desktop-Infrastruktur (VDI) mit einer Zwei-

⁵⁹ *Schneeberger*, KI-Assistenzsysteme in der Medizin, RdM 2021, 139 (140).

⁶⁰ *Specht-Riemenschneider/Heineking*, Datenverarbeitung in sicheren Verarbeitungsumgebungen am Beispiel von MRT-Gehirnscans, DuD 2024, 110.

⁶¹ Verordnung (EU) Nr. 557/2013 der Kommission vom 17. Juni 2013 zur Durchführung der Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates über europäische Statistiken in Bezug auf den Zugang zu vertraulichen Daten für wissenschaftliche Zwecke und zur Aufhebung der Verordnung (EG) Nr. 831/2002 der Kommission, ABl. L 164, 16.

Faktor-Authentifizierung und lückenloser Zugriffs-Protokollierung. Daneben gibt es auch die Möglichkeit, das Safe-Center vor Ort für den Zugang zu Mikrodaten zu nutzen.⁶²

Die grundlegenden Sicherheitsanforderungen für die sichere Verarbeitungsumgebung im EHDS werden in Art 73 Abs 1 EHDS dargelegt. Demnach soll beispielsweise gem Art 73 Abs 1 lit e EHDS die Führung von Zugangsprotokollen verpflichtend erfolgen. Zusätzlich soll die Kommission gem Art 73 Abs 5 EHDS bis zum 26. März 2027 genauere technische und organisatorische Anforderungen an die Zugangsstellen durch Durchführungsrechtsakte festlegen. Die Zugangsstelle muss den Datennutzer gem Art 68 Abs 10 lit f EHDS über technische Merkmale der sicheren Verarbeitungsumgebung in Kenntnis setzen und angeben, welche Instrumente in dieser Verarbeitungsumgebung zur Verfügung stehen.

Gem Art 67 Abs 2 lit f EHDS können Datennutzer unter Umständen auch eigene Datensätze in die sichere Verarbeitungsumgebung einbringen. Soll dies geschehen, müssen diese im Datenantrag beschrieben werden. Zusätzlich sollen Datennutzer gem Art 67 Abs 2 lit i EHDS auch bereits im Datenantrag angeben, welche Instrumente und Ressourcen sie für die Verarbeitung in der sicheren Verarbeitungsumgebung benötigen.

2.2.2 Anonymisierung und Pseudonymisierung

2.2.2.1 Vorgaben im EHDS

Eng verbunden mit den Überlegungen zur sicheren Verarbeitungsumgebung ist die Verpflichtung zur Datenminimierung⁶³ durch Pseudonymisierung und Anonymisierung der elektronischen Gesundheitsdaten.⁶⁴ Der EHDS schließt den Zugang zu Rohdaten explizit aus und ordnet dabei Pseudonymisierung als Mindestmaß an Entfernung des Personenbezugs an. Zugang zu pseudonymisierten Daten gem Art 66 Abs 3 iVm Art 68 Abs 1 lit c EHDS wird nach dem Prinzip der Verhältnismäßigkeit jedoch nur gewährt, wenn anonymisierte Daten für die Verarbeitungszwecke der Datennutzer nicht ausreichen.

Aus dem normativ verbindlichen Teil der Verordnung geht keine eindeutige Zuständigkeit für den konkreten technischen Akt der Entfernung des Personenbezugs hervor. Auch gem ErwGr 72 S 6 EHDS sollen sowohl Dateninhaber als auch Zugangsstellen in der Lage sein,

⁶² *Austrian Micro Data Center*, <https://www.statistik.at/services/tools/services/amdc-mikrodaten-fuer-die-wissenschaft/safe-center> (abgefragt am 14.4.2025).

⁶³ Näheres unter 2.2.4.

⁶⁴ ErwGr 72 S 2 EHDS.

die Pseudonymisierung beziehungsweise Anonymisierung durchzuführen. Dem Grundsatz der Datenminimierung folgend scheint aus datenschutzrechtlicher Sicht jedoch eine möglichst frühe Entfernung des Personenbezugs erforderlich und diese daher schon bei den Dateninhabern geboten.⁶⁵

Für die Dateninhaber bestünde bei dieser Sichtweise neben der technischen Herausforderung insbesondere rechtliche Unklarheit. Sie würden zwar nicht entscheiden, ob die elektronischen Gesundheitsdaten in einem pseudonymisierten oder anonymisierten Format bereitgestellt werden, ihnen obläge jedoch die schwierig zu treffende Beurteilung der technisch-rechtlichen Grenze zwischen Anonymisierung und Pseudonymisierung im Einzelfall. Zusätzlich geht aus dem Verordnungstext durch die fehlende Verpflichtung einer konkreten Stelle zur Durchführung der Anonymisierung beziehungsweise Pseudonymisierung nicht eindeutig hervor, auf welche datenschutzrechtliche Verarbeitungsgrundlage, sofern mit der hM die Notwendigkeit einer solchen bejaht wird,⁶⁶ diese von den Dateninhabern gestützt werden könnte. Die oben getroffene Überlegung zum möglichst frühen Handeln auf der Grundlage des Grundsatzes der Datenminimierung erfüllt wohl kaum die strengen Anforderungen einer Erforderlichkeit der Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung gem Art 6 Abs 1 lit c DSGVO an die Dateninhaber.⁶⁷

Die durchaus schwierig zu treffende Entscheidung⁶⁸ über das Format der bereitgestellten elektronischen Gesundheitsdaten wird jedoch in letzter Konsequenz von den Zugangsstellen selbst getroffen, indem sie den Datenantrag abweisen oder positiv über ihn durch Erlass der Datengenehmigung absprechen. Gem Art 68 Abs 3 EHDS haben die Zugangsstellen auch die dritte Möglichkeit, den Datenantrag bei Aussichtslosigkeit einer Datengenehmigung in das aliud der (Gesundheits-)Datenanfrage gem Art 69 EHDS

⁶⁵ *Gabauer*, Sekundärnutzung von elektronischen Gesundheitsdaten auf Grundlage des Entwurfs einer Verordnung über den Europäischen Raum für Gesundheitsdaten (EHDS) in *Janisch/Krempelmeier/Mader/Staudegger/Thiele*, Am Glasfaserpuls – Festschrift für Dietmar Jähnel (2025), 201 (227).

⁶⁶ *Stürmer*, Löschen durch Anonymisieren?, ZD 2020, 626; *Hornung/Wagner*, Anonymisierung als datenschutzrelevante Verarbeitung?, ZD 2020, 223; aA *Thüsing/Rombey*, Anonymisierung an sich ist keine rechtfertigungsbedürftige Datenverarbeitung, ZD 2021, 548.

⁶⁷ *Frenzel* in *Paal/Pauly*, DS-GVO BDSG³ (2021) Art 6 DSGVO Rz 16.

⁶⁸ *Forgó*, Der European Health Data Space im Kontext der MMR, MMR 2023, 3 (4).

umzudeuten, wenn die dort normierten Voraussetzungen erfüllt sind. Bei der Datenanfrage wird kein direkter Zugang zu elektronischen Gesundheitsdaten gewährt, sondern diese bloß in einem statistischen Format bereitgestellt. Für eine solche Umdeutung muss gem Art 68 Abs 3 EHDS jedoch die Zustimmung des Antragstellers eingeholt werden. Eine ähnliche Vorgehensweise, bei der ein Datenantrag bezüglich bloß pseudonymisierter Daten in einen Datenantrag bezüglich anonymisierter Daten umgedeutet werden kann, ist im EHDS nicht vorgesehen. Daher empfiehlt sich für Antragsteller, welche Zugang zu pseudonymisierten Daten suchen, in eventu auch die Bereitstellung anonymisierter Daten zu begehren.

Während pseudonymisierte Daten in der sicheren Verarbeitungsumgebung verbleiben müssen und nur dort zu den angegebenen Zwecken verarbeitet werden können, soll es gem Art 73 Abs 2 EHDS möglich sein, anonymisierte Daten herunterzuladen. Ob das Herunterladen die Verarbeitung anonymisierter Gesundheitsdaten über die gem Art 68 Abs 10 lit e EHDS von den Zugangsstellen vorgegebene Genehmigungsdauer erlaubt, ist fraglich. Die Überprüfung eines eventuellen Verstoßes würde sich jedoch äußerst schwierig gestalten.⁶⁹ Darüber hinaus werden im EHDS keine Einschränkungen an die Daten-Governance der Datennutzer für anonymisierte Daten gestellt, mit der Ausnahme, dass gem Art 61 Abs 3 EHDS eine Re-Identifizierung anonymisierter Gesundheitsdaten verboten sein soll.

Weitreichende Konsequenzen für die Daten-Governance der Datennutzer könnte jedoch Art 61 Abs 2 EHDS haben. Diese Bestimmung verbietet es, nicht in der Datengenehmigung genannten Dritten Zugang zu elektronischen Gesundheitsdaten bei Verarbeitung in der sicheren Verarbeitungsumgebung zu verschaffen. Die Bestimmung stellt nicht auf eine Unterscheidung zwischen pseudonymisierten und anonymisierten Daten ab und scheint daher vor allem der Verhinderung der Umgehung des Datenantragsprozesses gem Art 68 EHDS zu dienen. Aufgrund dieser Überlegung wäre es jedoch systemwidrig, nur die Zugangsverschaffung in der sicheren Verarbeitungsumgebung zu verbieten und nicht die Umgehung dieses Verbots durch Herunterladen anonymisierter Daten und anschließender Zurverfügungstellung. Datennutzer wären demnach vorerst gut beraten, gegen den Wortlaut von Art 61 Abs 2 EHDS davon auszugehen, dass auch heruntergeladene, anonymisierte Gesundheitsdaten nicht weitergegeben werden dürfen.

⁶⁹ Denga, Die Nutzungsgovernance im European Health Data Space als Problem eines Immaterialgütermarkts, EuZW 2023, 25 (30).

2.2.2.2 Anforderungen an Datennutzer

Der EHDS gibt keine verordnungsautonome Anonymisierungsdefinition vor. Daher müssen für die Gewährleistung datenschutzrechtlicher Standards die Vorgaben anderer datenschutzrechtlicher Rechtsgrundlagen, insbesondere die der DSGVO, der Rechtsprechung des EuGH und der nationalen Behörden und Gerichte, herangezogen werden.

Die Rechtsrahmen des EHDS und der DSGVO stellen hierbei große Anforderungen an Datennutzer. Sie müssen in einem ersten Schritt selbst beurteilen, ob anonymisierte Daten für die gewünschten Verarbeitungszwecke ausreichend sind oder ob pseudonymisierte Daten verlangt werden sollen. Diese Entscheidung erfordert neben einem Bewusstsein über die notwendigen Verarbeitungsschritte insbesondere ein klares Verständnis der datenschutzrechtlichen Unterscheidung zwischen Anonymisierung und Pseudonymisierung.

Bei pseudonymisierten Daten handelt es sich gem Art 4 Z 5 DSGVO um Daten, die „[...] ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“. Bei der Pseudonymisierung sollen also personenbezogene Daten und deren Identitätsmerkmale getrennt werden – technisch, organisatorisch und logisch.⁷⁰ Bei der Pseudonymisierung besteht jedoch weiterhin die Möglichkeit der Identifizierung der betroffenen Personen. Im Kontext des EHDS kann dies jederzeit durch die Zugangsstellen beziehungsweise in der sicheren Verarbeitungsumgebung geschehen.⁷¹

Anonymisierte Daten sind hingegen solche, bei denen eine Re-Identifizierung grundsätzlich ausgeschlossen ist. Wurde in der Vergangenheit noch teilweise ein absoluter Ansatz vertreten, der personenbezogene Daten erst dann als rechtlich anonymisiert betrachtete, wenn niemand unter welchem Aufwand auch immer in der Lage gewesen wäre,

⁷⁰ *Burghoff*, Praxisgerechter Umgang mit der Verfremdung personenbezogener Daten, ZD 2023, 658 (659).

⁷¹ *Hödl* in *Knyrim*, DatKomm Art 4 DSGVO Rz 57 (Stand 1.12.2018, rdb.at).

eine einzelne Person in diesen Daten zu identifizieren,⁷² wird mittlerweile, gestützt auf ErwGr 26 DSGVO und die Rechtsprechung,⁷³ ein relativer Ansatz vertreten. Hierbei werden nur Personen und deren verfügbare Mittel in Betracht gezogen, welche vernünftigerweise eingesetzt werden könnten, um eine Person aus einem Datensatz zu bestimmen.⁷⁴ Eine rechtlich wirksame Anonymisierung sei gem der Rechtsprechung daher auszuschließen, wenn die Identifizierung daher „einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung de facto vernachlässigbar“ erscheine.⁷⁵ Hierbei wird gewöhnlich auf den Stand der Technik und erwerbbares Zusatzwissen der Beteiligten abgestellt.⁷⁶ Zu erwähnen ist, dass bei Gesundheitsdaten eine rechtskonforme Anonymisierung per se in Zweifel gezogen wird.⁷⁷

Die Notwendigkeit der Auseinandersetzung mit Anonymisierung endet jedoch nicht mit dem Erhalt der Datengenehmigung. Werden die gewünschten elektronischen Gesundheitsdaten anonymisiert von den Datennutzern aus der sicheren Verarbeitungsumgebung heruntergeladen, sind einige Herausforderungen in Hinblick auf Daten-Governance zu beachten, welche so im Verordnungstext des EHDS keine Beachtung finden.

Insbesondere ist zu berücksichtigen, dass eine bereits erfolgte Anonymisierung nicht zwangsweise permanent wirkt. Im System der relativen Anonymisierung, in dem ein Restrisiko der Re-Identifizierung bestehen kann, ist diese naturgemäß möglich. Der EHDS

⁷² *Art.-29-Datenschutzgruppe*, WP 216 Stellungnahme 5/2014 zu Anonymisierungstechniken, angenommen am 10. 4. 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf (abgefragt am 14.4.2025).

⁷³ EuGH 7.3.2024, C-604/22, *IAB Europe*, ECLI:EU:C:2024:214; EuGH 9.11.2023, C-319/22, *Scania*, ECLI:EU:T:2022:48; EuGH 19.10.2016, C-582/14, *Breyer*, ECLI:EU:C:2016:779; EuG 26.4.2023, T-557/20, *SRB/EDS*, ECLI:EU:T:2023:219.

⁷⁴ EuGH *Breyer* Rz 42.

⁷⁵ EuGH *Breyer* Rz 46.

⁷⁶ *Roßnagel/Geminn*, Vertrauen in Anonymisierung, ZD 2021, 487 (488).

⁷⁷ statt vieler *Jäger/Meier/Möhring/Ferrolli/Nida-Rümelin/Peters*, Von der Sackgasse der Anonymisierung zu Lösungsansätzen für den Datenschutz der Zukunft, ZD 2024, 490.

begegnet diesem Risiko zunächst mit dem mit höherer Strafe⁷⁸ versehenen Verbot der bewussten Re-Identifizierung anonymisierter Daten.⁷⁹

Daneben besteht aber durchaus auch ein Risiko der unbewussten Re-Identifizierung der anonymisierten Daten. Im Einklang mit ErwGr 26 DSGVO muss der Stand der Technik, damit sind insbesondere Re-Identifizierungstechniken gemeint, zu denen anonymisierte Daten verarbeitende Stellen Zugang haben, ständig verfolgt werden. Durch technischen Fortschritt kann eine bereits erfolgte Anonymisierung daher rechtlich hinfällig werden. Weiters muss das dem Datennutzer verfügbare Zusatzwissen beachtet werden, was Fragen über die Sicherheit der Anonymisierung aufwirft, da dieses Kriterium ex ante, insbesondere von den Zugangsstellen, schwer zu beurteilen ist.⁸⁰ Das führt insbesondere bei der langfristigen Aufbewahrung von Forschungsdaten, wie es mitunter die gute wissenschaftliche Praxis gebietet, zu großem Compliance-Aufwand, da deren fortdauernde Anonymisierung periodisch überprüft werden müsste.⁸¹ Der Umstand, dass elektronische Gesundheitsdaten im System der Sekundärnutzung durch Zugangsstellen bereitgestellt werden, wirkt nicht haftungsbefreiend und ändert nichts an dieser Notwendigkeit.

Somit ist zu befürchten, dass insbesondere das Risiko der Re-Identifizierung anonymisiert geglaubter elektronischer Gesundheitsdaten von Datennutzern nicht ausreichend beachtet wird. Dieses Risiko müsste von den Zugangsstellen bei der Bereitstellung dieser Daten offen kommuniziert werden. ErwGr 72 EHDS erwähnt zwar eben jenes Risiko der Re-Identifizierung und verweist auf die Möglichkeit der Kommission, delegierte Rechtsakte auf der Grundlage von Art 5 Abs 13 DGA DGA zu erlassen, welche Vorschriften beinhalten können, die zur Reduzierung des Risikos der Re-Identifizierung anonymisierter Daten führen sollen. Diese Ermächtigung bezieht sich jedoch nur auf Risiken, welche beim Transfer der Daten in Drittländer, also Staaten außerhalb der Europäischen Union und des Geltungsbereichs der DSGVO, auftreten. Dass der Kern des Problems ein technischer ist

⁷⁸ siehe auch ErwGr 106 EHDS.

⁷⁹ Art 61 Abs 3 iVm Art 64 Abs 5 lit c EHDS.

⁸⁰ *Mayrhofer/Leitner/Stadlbauer*, Datenschutzrechtliche Aspekte der Nutzung von Krankenhausinformationssystemen für Forschungszwecke, ZTR 2022, 207 (214); *Haimberger*, Datenschutz in der medizinischen und pharmazeutischen Forschung (2021), 196; *Fuchs*, Anonymisierende Wirkung der Verschlüsselung, Dako 2019, 55.

⁸¹ *Conrad/Folkerts*, Anonyme Daten unter der DSGVO - Risiko statt Vorteil?, KuR 2023, 89 (92).

und auch bei Staaten mit denselben rechtlichen Rahmenbedingungen auftreten kann, wird im EHDS nicht ausreichend abgebildet.

Daher sei Datennutzern empfohlen, bei Bezug anonymisierter Daten eine periodische Überprüfung der aufrechten Anonymisierung der übernommenen Gesundheitsdaten vorzusehen, oder aber diese gleich in der sicheren Verarbeitungsumgebung zu belassen, um dieses Risiko gar nicht erst entstehen zu lassen. Ein solches periodisches Überprüfungsregime sollte auch gem Art 67 Abs 2 lit g EHDS bei dem Datenantrag angegeben werden.

2.2.3 Verarbeitungsgrundlage pseudonymisierter Daten

Mehr noch als bei der Verarbeitung anonymisierter Daten und den damit einhergehenden Herausforderungen wird bei der Verarbeitung pseudonymisierter Daten die Beziehung zum Datenschutzrecht ersichtlich.⁸²

Da pseudonymisierte Daten sehr wohl personenbezogene Daten darstellen,⁸³ ist für deren Verarbeitung eine Verarbeitungsgrundlage gem Art 6 Abs 1 DSGVO notwendig. Zusätzlich handelt es sich bei elektronische Gesundheitsdaten um sensible Daten gem Art 9 Abs 1 DSGVO, weswegen kumulativ die Identifizierung eines Ausnahmetatbestandes gem Art 9 Abs 2 DSGVO erforderlich ist. Üblicherweise wird bei der Primärnutzung insbesondere im Forschungskontext der Verarbeitungsgrundlage der informierten Einwilligung gem Art 6 Abs 1 lit a DSGVO der Vorzug gegeben.⁸⁴ Das System der Sekundärnutzung im EHDS richtet sich jedoch bewusst gegen diese Verarbeitungsgrundlage, deren Einsatz nicht praktikabel wäre.⁸⁵ Es soll durch den EHDS gerade ein umfassender und vollständiger Zugang zu Gesundheitsdaten, auch nach der ursprünglichen Datenverarbeitung erfolgen.⁸⁶ Dieser wäre durch das bloße Abstellen auf die informierte Einwilligung nicht gegeben.

⁸² *Shabani/Yilmaz*, Lawfulness in secondary use of health data, *Technology and Regulation* 2022, 128.

⁸³ Art 4 Z 5 DSGVO.

⁸⁴ *Veil*, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, *NVwZ* 2018, 686 (688).

⁸⁵ *Becker/Chokoshvili/Dove*, Legal bases for effective secondary use of health and genetic data in the EU: time for new legislative solutions to better harmonize data for cross-border sharing?, *International Data Privacy Law* 2024, 6.

⁸⁶ ErwGr 53 EHDS.

Der EHDS gibt teilweise Verarbeitungsgrundlagen für Datenverarbeitungsschritte im System der Sekundärnutzung vor. So soll die Übermittlung der elektronischen Gesundheitsdaten an die Zugangsstellen durch die Dateninhaber als Erfüllung einer rechtlichen Verpflichtung von der Verarbeitungsgrundlage in Art 6 Abs 1 lit c DSGVO iVm den Ausnahmebestimmungen in Art 9 Abs 2 lit i und j DSGVO gedeckt sein. Die von den Zugangsstellen gesetzten Verarbeitungsschritte zur Aufbereitung und Zurverfügungstellen der Daten sind als Erfüllung einer öffentlichen Aufgabe von Art 6 Abs 1 lit e DSGVO iVm Art 9 Abs 2 lit g DSGVO gedeckt.⁸⁷

Eine der zentralen Frage für Datennutzer im System des EHDS ist, ob durch die Verordnung selbst bzw durch das Erfüllen der Anforderungen an den Datenantrag gem Art 67 EHDS eine Verarbeitungsgrundlage gem Art 6 Abs 1 DSGVO gegeben sein soll. Hier wäre insbesondere daran zu denken, dass der europäische Rechtssetzer den EHDS gem Art 6 Abs 1 lit e iVm Art 6 Abs 3 lit a DSGVO als eine eigene Verarbeitungsgrundlage für Datennutzer deklariert.⁸⁸ Gem ErwGr 52 S 6 EHDS sollen Datennutzer jedoch selbständig eine Verarbeitungsgrundlage gem Art 6 Abs 1 DSGVO vorweisen können.

Die Datennutzer können und sollen daher aus mehreren Verarbeitungsgrundlagen wählen, welche bereits im Datenantrag gem Art 67 Abs 4 EHDS anzugeben sind. Der EHDS gibt hier keine bestimmte Verarbeitungsgrundlage vor, legt den Datennutzern in ErwGr 52 jedoch die Verarbeitungsgrundlagen in Art 6 Abs 1 lit e und f DSGVO nahe.⁸⁹

2.2.3.1 Art 6 Abs 1 lit e DSGVO – Öffentliches Interesse

Art 6 Abs 1 lit e DSGVO schafft für sich genommen keine Verarbeitungsgrundlage, sondern erlaubt im Zusammenspiel mit Art 6 Abs 2 und 3 DSGVO die Verarbeitung personenbezogener Daten, welche für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Die Verarbeitungsgrundlage des öffentlichen Interesses gem Art 6 Abs 1 lit e DSGVO muss somit erst gem Art 6 Abs 3 DSGVO in nationales Recht oder Unionsrecht gegossen werden.

⁸⁷ kritisch *Raji*, Datenräume in der Europäischen Datenstrategie am Beispiel des European Health Data Space, ZD 2023, 3 (7).

⁸⁸ *Albers/Veit in Wolff/Brink/von Ungern-Sternberg*, BeckOK Datenschutzrecht⁵¹ Art 6 DS-GVO Rz 90 (Stand 1.2.2025, beck-online.beck.de).

⁸⁹ ErwGr 52 S 10 EHDS.

Im Kontext des EHDS sind Verarbeitungsgrundlagen im öffentlichen Interesse, ob rechtmäßig oder nicht konkret auf Art 6 Abs 1 lit e DSGVO iVm Art 6 Abs 2 und 3 DSGVO gestützt,⁹⁰ insbesondere in den nationalen datenschutzrechtlichen Forschungsprivilegien zur Datenverarbeitung zu sehen.

In Österreich kommen hierfür vor allem die Verarbeitungsgrundlagen in FOG und DSG⁹¹ in Betracht. Zum Verhältnis von FOG und DSG ist voranzustellen, dass die wahrscheinlich hM in der Literatur die Verarbeitungsgrundlagen im FOG als speziellere Normen iSd lex specialis Doktrin ansieht.⁹² Dies Einordnung würde den Verarbeitungsgrundlagen im DSG auch im Kontext des EHDS den sachlichen Anwendungsbereich nehmen. Andererseits soll auch betont werden, dass die Datenschutzbehörde diesen Überlegungen zum Trotz weiterhin § 7 Abs 3 DSG anwendet und somit scheinbar von einer gewissen Parallelität von FOG und DSG ausgeht.⁹³

Im DSG finden sich in § 7 Abs 1 DSG drei Verarbeitungsgrundlagen, welche prima facie für Datenverarbeitung im Kontext des EHDS geeignet wären. § 7 Abs 1 Z 1 DSG erlaubt die Verarbeitung von öffentlich zugänglichen Daten, wobei hierunter jedoch nur allgemein zugängliche Daten, wie solche aus öffentlichen Verzeichnissen oder im Internet veröffentlichte Daten zu verstehen sind.⁹⁴ Diese Verarbeitungsgrundlage kann daher nicht

⁹⁰ *Gabauer*, Nationale Regelungsspielräume im Zusammenhang mit Datenverarbeitungen zu wissenschaftlichen Forschungszwecken in *Jahnel/Krempelmeier/Schmid*, Wissenschaft und Datenschutz (2024), 63.

⁹¹ Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl Nr. 165/1999.

⁹² *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, Datenschutzgesetz (2018) §7 Rz 10; *Haimberger*, Datenschutz, 21; *Feiler/Forgó*, EU-DSGVO, 527; *Jahnel*, Kommentar zur Datenschutz-Grundverordnung (2021), Art 89 DSGVO, Rz 23;

aA *Gabauer*, Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken (2019), 119; *Pinggera/Stadler* in *Bramshuber/Blasch*, Jahrbuch Sozialversicherungsrecht (2022), Von verantwortungsvollen Verantwortlichen, 101; *Lachmayer/Souhrada-Kirchmayer*, Datenschutzrecht in der wissenschaftlichen Forschung, zfhr 2018, 153 (157); *Kotschy*, Die Zulässigkeitsvoraussetzungen für Forschungsdatenverarbeitungen nach dem FOG – eine kritische Analyse in *Jahnel*, Datenschutzrecht (2020), 281 (307).

⁹³ DSB 7.6.2018, DSB-D202.207/0001-DSB/2018.

⁹⁴ *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, Datenschutzgesetz §7 Rz 12.

in Anspruch genommen werden, um pseudonymisierte elektronische Gesundheitsdaten Rahmenwerk des EHDS zu verarbeiten, da zwar der Datensatzkatalog der Allgemeinheit zugänglich ist, jedoch nicht die einzelnen Gesundheitsdaten selbst. § 7 Abs 1 Z 2 DSG erlaubt eine zweckändernde Datenverarbeitung für Daten, welche für andere Zwecke bereits zulässigerweise ermittelt wurden. Diese Bestimmung ermöglicht jedoch nur Datenverarbeitung, wenn primäre Erhebung und zweckändernde Verarbeitung von demselben Verantwortlichen durchgeführt werden⁹⁵ und stellt somit auch keine taugliche Verarbeitungsgrundlage, wie von Art 67 Abs 4 EHDS gefordert, dar.

§ 7 Abs 1 Z 3 DSG erlaubt jedoch die Verarbeitung von personenbezogenen Daten, welche für den Verantwortlichen pseudonymisiert sind, sofern dieser die Identität der betroffenen Person mit rechtlich zulässigen Mitteln nicht bestimmen, den direkten Personenbezug also nicht wiederherstellen, kann. Diese Verarbeitungsgrundlage erlaubt somit die Sekundärnutzung von pseudonymisierten, auch sensiblen Gesundheitsdaten zu wissenschaftlichen Forschungszwecken durch Dritte.⁹⁶ Die Wiederherstellung des direkten Personenbezugs ist für Datennutzer durch die Konzeption der sicheren Verarbeitungsumgebung gem Art 73 Abs 1 EHDS nicht möglich. Somit können sich Datennutzer, unter der Voraussetzung der Anwendbarkeit des DSG, auf § 7 Abs 1 Z 3 DSG stützen, um die Datenverarbeitung im EHDS zu legitimieren.

Daneben hat der österreichische Gesetzgeber mit § 2d Abs 2 Z 1 FOG eine umfassende Verarbeitungsgrundlage für Forschungszwecke geschaffen. Damit soll gemäß den Gesetzesmaterialien zum FOG eine „ausdrückliche und generelle Rechtsgrundlage“ geschaffen werden, welche Forschungsprojekten zugutekommen soll.⁹⁷ Anwendbar ist diese Verarbeitungsgrundlage auf jegliche Datenverarbeitung einer wissenschaftlichen Einrichtung. Diese werden gem § 2b Z 12 FOG bewusst weit definiert als „natürliche Personen, Personengemeinschaften sowie juristische Personen, die Zwecke gemäß Art. 89 Abs. 1 DSGVO verfolgen, d.h. insbesondere Tätigkeiten der Forschung und experimentelle Entwicklung (Z 10) vornehmen“. Somit kann von dieser Norm privilegierte Forschung sowohl im betrieblichen, als auch im universitären oder außeruniversitären Rahmen stattfinden und umfasst daher auch kommerziell tätige Unternehmen, solange die konkrete

⁹⁵ Löffler in Knyrim, DatKomm Art 89 DSGVO Rz 66 (Stand 1.12.2023, rdb.at).

⁹⁶ Gabauer, Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken, 106.

⁹⁷ ErläutRV 68 BlgNR 26. GP 33.

Forschungstätigkeit gem § 2c Abs 3 Z 3 FOG neuartig, schöpferisch, ungewiss in Bezug auf das Endergebnis, systematisch und übertrag- oder reproduzierbar ist.⁹⁸ Im Gegenzug müssen die weitreichenden Sicherheitsmaßnahmen von § 2d Abs 1 FOG bei der Datenverarbeitung eingehalten und die in § 2d Abs 2 Z 1 FOG normierten Schranken beachtet werden. Die einzelnen Litera von § 2d Abs 2 Z 1 FOG stellen dabei Alternativvoraussetzungen dar, welche von den Verantwortlichen erfüllt werden müssen, um die weitreichende Verarbeitungsgrundlage in Anspruch zu nehmen. Hierbei bietet sich insbesondere § 2d Abs 2 Z 1 lit b FOG an. Diese Bestimmung erlaubt jegliche Datenverarbeitung, solange die Daten nur in einem pseudonymisierten Format verarbeitet werden. Genau das wird gem Art 66 Abs 3 iVm Art 68 Abs 1 lit c EHDS in der sicheren Verarbeitungsumgebung garantiert.

Wegen der weitreichenden Erlaubnis zur Datenverarbeitung müssen Verantwortliche bei Inanspruchnahme des Forschungsprivilegs auch die beispielhaft⁹⁹ aufgezählten geeigneten Garantien zum Schutz der Betroffenen gem § 2d Abs 1 FOG beachten. Diese stellen in der Praxis die größte Hürde zur Inanspruchnahme dieser Verarbeitungsgrundlage dar und werden teilweise auch als überschießend kritisiert.¹⁰⁰ Im Kontext des EHDS werden jedoch die meisten Sicherheitsmaßnahmen gem § 2d Abs 1 FOG bereits durch die sichere Verarbeitungsumgebung erfüllt. Diese schreibt gem Art 73 Abs 1 lit e EHDS beispielsweise ein Zugriffsprotokoll vor, welches auch gem § 2d Abs 1 Z 1 FOG erforderlich ist. Auch die Begrenzung des Zugangs für in der Datengenehmigung genannten Personen gem Art 73 Abs 1 lit a EHDS spiegelt in Verbindung mit dem Verbot des Verfügbarmachens der elektronischen Gesundheitsdaten an Dritte gem Art 61 Abs 2 EHDS das Datengeheimnis gem § 2d Abs 1 Z 2 FOG wider. Nach erstem Vergleich der Sicherheitsmaßnahmen in § 2d Abs 1 FOG und denen des EHDS, insbesondere der Anforderungen an die sichere Verarbeitungsumgebung gem Art 73 Abs 1 EHDS, kann festgehalten werden, dass Datennutzer für die Anwendbarkeit von § 2d Abs 2 Z 1 lit b FOG insbesondere zwei Sicherheitsmaßnahmen ergreifen müssen, welche nicht explizit im EHDS vorgesehen sind. Sie haben gem § 2d Abs 1 Z 5 lit f FOG ihre Mitarbeiter nachweislich über Datenschutz- und Datensicherheitsvorschriften zu belehren und gem § 2d Abs 1 Z 5 lit a FOG im Internet

⁹⁸ Haimberger, Datenschutz, 22.

⁹⁹ Gem § 2d Abs 1 FOG sollen „insbesondere folgende angemessene Maßnahmen“ zur Anwendung kommen.

¹⁰⁰ Kotschy, Zulässigkeitsvoraussetzungen in Jahnke, Datenschutzrecht, 281 (297).

öffentlich einsehbar auf die Inanspruchnahme dieser Rechtsgrundlage hinzuweisen. Zur Erfüllung letzterer Maßnahme können Synergien mit der Publikationspflicht der Resultate der Sekundärnutzung gem Art 61 Abs 4 EHDS genutzt werden.¹⁰¹

Zusammengefasst sind somit zwei Verarbeitungsgrundlagen in der österreichischen Rechtsordnung auszumachen, welche gem Art 6 Abs 1 lit e DSGVO der Datenverarbeitung von pseudonymisierten Daten in der sicheren Verarbeitungsumgebung des EHDS dienlich sein können. § 7 Abs 1 Z 3 DSG scheint auf diese Situation besonders zugeschnitten und erlaubt Datenverarbeitung, solange die personenbezogenen Daten für den Verantwortlichen pseudonymisiert sind und dieser den Personenbezug mit rechtlich zulässigen Mitteln nicht wiederherstellen kann. Der Nachteil dieser Verarbeitungsgrundlage liegt in der unsicheren Beziehung zum FOG und in der Frage, ob § 7 Abs 1 Z 3 DSG in diesem Lichte überhaupt anwendbar ist. Somit bietet sich insbesondere die Verarbeitungsgrundlage in § 2d Abs 2 Z 1 lit b FOG für die Verarbeitung elektronischer Gesundheitsdaten im Rahmen des EHDS an. Deren Anwendbarkeit ist gewiss, hat üblicherweise in der Praxis jedoch den Nachteil der Voraussetzung hoher Datensicherheitsmaßnahmen gem § 2d Abs 1 FOG. Das Gros eben jener Maßnahmen wird im System des EHDS jedoch schon durch die Vorgaben der sicheren Verarbeitungsumgebung garantiert.

Neben den oben skizzierten Normen sollten Datennutzer auch Entwicklungen betreffend neuen unionalen und insbesondere nationalen Verarbeitungsgrundlagen im Auge behalten. Die Möglichkeit der Mitgliedsstaaten, auf der Basis von Art 6 Abs 1 lit e DSGVO iVm Art 6 Abs 2 und 3 DSGVO eigene Verarbeitungsgrundlagen im öffentlichen Interesse zu schaffen, möglicherweise sogar eigens für Datenverarbeitungen im Zuge der Sekundärnutzung im EHDS, bedeutet im Zusammenspiel mit der Neutralität des EHDS gegenüber den Verarbeitungsgrundlagen der Datennutzer jedoch das Potential der Zersplitterung dieses Rahmenwerks durch nationale Divergenzen im Datenschutzrecht.¹⁰²

¹⁰¹ Näheres unter 2.3.3.

¹⁰² *Gabauer*, Sekundärnutzung von elektronischen Gesundheitsdaten in *Janisch/Krempelmeier/Mader/Staudegger/Thiele*, Am Glasfaserpuls, 201 (255).

2.2.3.2 Art 6 Abs 1 lit f DSGVO – Berechtigtes Interesse

Art 6 Abs 1 lit f DSGVO erlaubt die Verarbeitung personenbezogener Daten, wenn diese zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist und die schutzwürdigen Interessen der Betroffenen nicht überwiegen. Hieraus ergibt sich ein dreigliedriges Prüfungsschema, welches von EuGH¹⁰³, OGH¹⁰⁴ und der DSB¹⁰⁵ für die Prüfung der Rechtmäßigkeit einer Datenverarbeitung auf der Grundlage von Art 6 Abs 1 lit f DSGVO herangezogen wird. Das Prüfungsschema stellt sich als analog der Verhältnismäßigkeitsprüfung eines Grundrechtseingriffs dar:

1. Wahrnehmung eines berechtigten Interesses des Verantwortlichen oder eines Dritten
2. Erforderlichkeit der Verarbeitung der personenbezogenen Daten zur Verwirklichung dieses berechtigten Interesses
3. Kein Überwiegen der Interessen oder Grundrechte der Betroffenen gegenüber dem berechtigten Interesse des Verantwortlichen oder des Dritten

Wissenschaftliche Forschung wurde schon unter der Datenschutzrichtlinie¹⁰⁶ von der *Art-29-Datenschutzgruppe* als übliche Fallgruppe eines berechtigten Interesses betrachtet.¹⁰⁷ Das Kriterium der Erforderlichkeit ist erfüllt, wenn es keine weniger stark in die Interessen und Grundrechte der Betroffenen eingreifende Mittel zum Erreichen des verfolgten berechtigten Interesses gibt.¹⁰⁸ Das Hauptaugenmerk dieses Schemas liegt jedoch bei der Interessenabwägung von Punkt 3. Betroffenen kommen insbesondere die Grundrechte betreffend Datenschutz und Privatsphäre gem Art 7 und 8 GRC zugute, während sich Verantwortliche auf die Wichtigkeit der von Ihnen durchgeführten wissenschaftlichen Forschung und das öffentliche Interesse daran stützen können. Durch zusätzliche

¹⁰³ EuGH 11.12.2019, C-708/18, *Asociația de Proprietari bloc M5A-ScaraA*, ECLI:EU:C:2019:1064 Rz 40.

¹⁰⁴ OGH 27.11.2019, 6 Ob 150/19f.

¹⁰⁵ DSB 26.6.2020, 2020-0.349.984.

¹⁰⁶ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

¹⁰⁷ *Artikel-29-Datenschutzgruppe*, Stellungnahme zum Begriff des berechtigten Interesses (WP217), https://dsb.gv.at/sites/site0344/media/downloads/wp251rev01_de.pdf, 32 (abgefragt am 14.4.2025).

¹⁰⁸ *Artikel-29-Datenschutzgruppe*, WP217, 70.

Schutzmaßnahmen, wie Datenminimierung, Privacy by Design und Zugangsbeschränkungen kann das Gleichgewicht zugunsten des Verantwortlichen verschoben werden.¹⁰⁹

Diese Verarbeitungsgrundlage eignet sich prima facie hervorragend für die Verarbeitung im Zuge der wissenschaftlichen Forschung, weil hier einerseits das berechtigte Interesse der Forschenden als Verantwortliche als hoch einzuschätzen ist und andererseits bereits standardmäßig taugliche Schutzmaßnahmen vorliegen, welche für wissenschaftliche Forschung ohnehin vorgeschrieben sind.¹¹⁰ Spezifisch für medizinische Forschung ist sie jedoch nicht immer praktikabel, da die Forschung mit Gesundheitsdaten als besondere Kategorie personenbezogener Daten zusätzlich das Vorliegen eines Ausnahmetatbestandes gem Art 9 Abs 2 DSGVO erfordert. Ein unmittelbar anwendbarer, Art 6 Abs 1 lit f DSGVO äquivalenter Ausnahmetatbestand existiert jedoch nicht.

Das vom EHDS geschaffene Sekundärnutzungssystem bewirkt nun zweierlei: Einerseits soll der EHDS gem ErwGr 52 EHDS einen Ausnahmetatbestand gem Art 9 Abs 2 DSGVO bilden. Insbesondere in der Einbeziehung von Zugangsstellen, dem Zurverfügungstellen der Daten in der sicheren Verarbeitungsumgebung und den Modalitäten der Datengenehmigung sollen ausreichende Schutzmaßnahmen erblickt werden, welche als „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ einen unionsrechtlich vorgesehenen Ausnahmetatbestand gem Art 9 Abs 2 lit g-j DSGVO rechtfertigen. Auf welcher der Ausnahmetatbestände von Art 9 Abs 2 lit g-j DSGVO dies genau geschieht, geht aus ErwGr 52 EHDS nicht eindeutig hervor, was auch von EDSA und EDSB in ihrer gemeinsamen Stellungnahme zum EHDS-Entwurf kritisiert wurde.¹¹¹ Jedenfalls sollen sensible Gesundheitsdaten wie „normale“ personenbezogene Daten behandelt werden und im Rahmen des EHDS somit das berechtigte Interesse, insbesondere auch für kommerzielle Forschung, als Verarbeitungsgrundlage ermöglichen. Zusätzlich bietet das System der Sekundärnutzung,

¹⁰⁹ *Artikel-29-Datenschutzgruppe*, WP217, 71.

¹¹⁰ Art 89 Abs 1 DSGVO.

¹¹¹ *EDSA/EDSB*, Gemeinsame Stellungnahme 3/2022 des EDSA und des EDSB zum Vorschlag für eine Verordnung über den europäischen Raum für Gesundheitsdaten, Rz 84, https://www.edpb.europa.eu/system/files/2023-04/edpb_edps_jointopinion_202203_europeanhealthdataspace_de.pdf (abgefragt am 14.4.2025).

unter anderem durch das Vorschreiben von Pseudonymisierung,¹¹² die verpflichtende Beschreibung von Schutzmaßnahmen im Datenantrag gem Art 67 Abs 2 lit g EHDS und insbesondere die Bereitstellung der Daten in einer sicheren Verarbeitungsumgebung gewichtige Argumente für das Überwiegen der berechtigten Interessen des Verantwortlichen bzw des Datennutzers in der oben beschriebenen Interessenabwägung.

Das Ergebnis der Interessenabwägung wird demnach nicht vorweggenommen, was nach der Rechtsprechung des EuGH auch unzulässig wäre.¹¹³ Die Interessenabwägung bleibt somit eine Einzelfallentscheidung,¹¹⁴ womit einige Unsicherheiten für Datennutzer bezüglich Rechtmäßigkeit der Datenverarbeitung bestehen bleiben. Es ist jedoch zu erwähnen, dass die Gewährung des Datenzugangs eine gewisse Sicherheit für sie darstellt, da die Zugangsstellen gem Art 68 Abs 1 lit c EHDS bereits die Rechtmäßigkeit der von den Datennutzern im Datenantrag gem Art 67 Abs 4 EHDS angegebenen Interessenabwägung prüfen.

2.2.4 Zweckbindung und Datenminimierung

Auch wenn die Rechtmäßigkeit der Datenverarbeitung gegeben ist, muss aufgrund des „unberührt“ gelassenen datenschutzrechtlichen Rahmens bei der Verarbeitung pseudonymisierter elektronischer Gesundheitsdaten den Grundsätzen der Datenverarbeitung gem Art 5 DSGVO Genüge getan werden. Hierbei stechen insbesondere die Grundsätze der Zweckbindung gem Art 5 Abs 1 lit b DSGVO und der Datenminimierung gem Art 5 Abs 1 lit c DSGVO hervor.

Dabei ist gem Art 5 Abs 1 lit b DSGVO einerseits dafür zu sorgen, dass bereits vor Beginn der Verarbeitung personenbezogener Daten deren Zwecke eindeutig, konkret und damit möglichst eng festgelegt werden müssen und dass diese Daten nur in einer mit diesen Zwecken vereinbaren Weise verwendet werden dürfen. Andererseits sollen gem Art 5 Abs 1 lit c DSGVO auch nicht mehr personenbezogene Daten verwendet werden, als für die

¹¹² EDSA, Guidelines 01/2025 on Pseudonymisation (Adopted on 16 January 2025), Rz 55, https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf (abgefragt am 14.4.2025).

¹¹³ EuGH 24.11.2011, C-468/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)*, ECLI:EU:C:2011:777 Rz 47.

¹¹⁴ Hacker, A Legal Framework for AI Training Data - From First Principles to the Artificial Intelligence Act, Law, Innovation and Technology 2020, 257 (285).

Verarbeitung unbedingt benötigt werden. Üblicherweise wird der KI-Forschung im Big Data Bereich ein Spannungsverhältnis mit diesen Grundsätzen attestiert.¹¹⁵ Dieser Befund ergibt sich aus der Notwendigkeit der Verarbeitung großer Datenmengen in einem ergebnisoffenen Bereich wie der wissenschaftlichen Forschung.

Zweckbindung und Datenminimierung müssen auch im Sekundärnutzungssystem des EHDS eingehalten werden. Es soll jedoch festgehalten werden, dass der EHDS selbst bereits einige Maßnahmen hierfür vorsieht. So müssen primär die Zugangsstellen bei Prüfung des Datenantrags gem Art 68 Abs 1 lit b EHDS auf diese Grundsätze Bedacht nehmen. Weiters können in der verpflichteten Pseudonymisierung beziehungsweise Anonymisierung sowie sogar in der Bereitstellung der elektronischen Gesundheitsdaten in der sicheren Verarbeitungsumgebung Maßnahmen zur Datenminimierung erblickt werden.¹¹⁶ Zweckbindung wird gem Art 54 EHDS insbesondere durch das Verbot der Verarbeitung bereitgestellter elektronischer Gesundheitsdaten außerhalb des im Datenantrag verpflichtend anzugebenden¹¹⁷ und in der Datengenehmigung ersichtlichen Zwecks erzielt. Forschende haben demnach zu berücksichtigen, dass das Sekundärnutzungssystem des EHDS in Bezug auf den Grundsatz der Zweckbindung strenger als die allgemeinen datenschutzrechtlichen Vorgaben ist und diesen im Rahmen des EHDS als *lex specialis* vorgeht. Der EHDS erlaubt somit keine zweckändernde Verarbeitung von personenbezogenen Daten, welche für andere Zwecke ermittelt oder zugänglich gemacht wurden, wie sonst in der wissenschaftlichen Forschung auf der Basis von Art 5 Abs 1 lit b iVm Art 89 Abs 1 DSGVO¹¹⁸ oder nationalen Bestimmungen wie § 2d Abs 2 Z 1 FOG mitunter möglich. Darüber hinaus trifft das Verbot einer zweckändernden Verarbeitung, anders als nach allgemeinen datenschutzrechtlichen Grundsätzen, auch anonymisierte Daten.

¹¹⁵ *Graf/van Hövell/Stoppe*, Künstliche Intelligenz in der Medizin. Datenschutz und Haftungsfragen in der Schnittstelle zwischen KI-VO und MDR, PharmR 2025, 77 (80); *Alon*, KI in der Gesundheitstechnologie: Die Datenschutz-Challenge, GRCaktuell 2023, 93 (94).

¹¹⁶ *Kogut-Czarkowska/Shabani*, Federated networks and secondary uses of health data in *Slokenberga/Ó Cathaoir/Shabani*, The European Health Data Space (2025), 238.

¹¹⁷ Näheres unter 2.1.3.

¹¹⁸ *Hötzendorfer/Tschohl/Kastelitz* in *Knyrim*, DatKomm Art 5 DSGVO Rz 32.

2.3 Pflichten der Datennutzer nach erfolgter Verarbeitung

2.3.1 Betroffenenrechte

Das Kapitel III der DSGVO beinhaltet subjektive Rechte Betroffener, welche ihnen bei Verarbeitung ihrer personenbezogenen Daten zustehen. Zunächst kann festgehalten werden, dass die Betroffenen diese Rechte gegenüber jedem Verantwortlichen geltend machen können. Dies betrifft im Kontext der Sekundärnutzung neben den Zugangsstellen und den Dateninhabern auch die Datennutzer, sofern diese die Gesundheitsdaten nicht anonymisiert verarbeiten. Es ist festzuhalten, dass auch diese Rechte vom Regelungssystem des EHDS weitgehend unberührt gelassen werden.

Unter den Betroffenenrechten ist im Kontext des EHDS insbesondere das Widerspruchsrecht gem Art 21 Abs 1 DSGVO hervorzuheben. Dieses besteht für die Verarbeitung personenbezogener Daten auf der Basis von Art 6 Abs 1 lit e oder f DSGVO, somit für die Hauptfälle einwilligungsloser Datenverarbeitung, welche auch im EHDS als Grundlage für die Verarbeitung pseudonymisierter Gesundheitsdaten vorgesehen sind. Betroffene können durch das Widerspruchsrecht bei „Gründen, die sich aus ihrer besonderen Situation ergeben“¹¹⁹ eine grundsätzlich rechtmäßige Datenverarbeitung untersagen, solange der Verantwortliche keine zwingenden schutzwürdigen Gründe für die Verarbeitung nachweisen kann, welche die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.¹²⁰ In der Praxis des EHDS wird dieses Recht jedoch nicht von großer Bedeutung sein, weil der EHDS ein autonomes Recht auf Opt-Out aus dem Sekundärnutzungssystem vorsieht, welches ohne Angabe von Widerspruchsgründen auskommt und daher eher Verwendung finden würde.¹²¹ Ein Anwendungsfall für das Widerspruchsrecht könnte daher insbesondere beim Fall der Datenverarbeitung trotz Opt-Out gem Art 71 Abs 4 EHDS bleiben, da sich Betroffene trotz EHDS-autonomen Widerspruch mit der Verarbeitung ihrer Gesundheitsdaten konfrontiert sehen. Betroffene könnten daher versuchen, eine einzelne, auf Art 71 Abs 4 EHDS gestützte Datenverarbeitung auf der Grundlage des Widerspruchsrechts gem Art 21 Abs 1 DSGVO zu verhindern. Da für die Ausnahme gem Art 71 Abs 4 EHDS jedoch ohnehin wichtige öffentliche Interessen vorliegen müssen, wäre der positive Ausgang dieses Vorhabens für

¹¹⁹ zu diesem Begriff siehe EuGH 13.5.2014, C-131/12, *Google Spain*, ECLI:EU:C:2014:317 Rz 80.

¹²⁰ *Haidinger* in *Knyrim*, *DatKomm* Art 21 DSGVO Rz 1 (Stand 1.12.2022, rdb.at).

¹²¹ Näheres unter 2.1.4.

Betroffene schon aus diesem Grund zweifelhaft. Weiters wird auch vertreten, dass das Recht auf Opt-Out gem Art 71 Abs EHDS im Anwendungsbereich des EHDS das allgemeine Widerspruchsrecht gem Art 21 DSGVO als speziellere Norm verdrängt und damit für dieses ohnehin kein Anwendungsbereich bleibt.¹²²

Darüber hinaus ist schon fraglich, inwiefern die Ausübung von Betroffenenrechten in der Praxis überhaupt möglich sein könnte. Von den drei Akteuren, welche personenbezogene Daten verarbeiten, haben nur die Zugangsstellen sowohl die Möglichkeit der Identifizierung der Betroffenen als auch Einblick in die Zwecke der Weiterverarbeitung durch Datennutzer. Dateninhaber bekommen zwar die Aufforderung zur Bereitstellung ihrer elektronischen Gesundheitsdaten gem Art 60 Abs 1 EHDS, haben jedoch keinen Einblick in die genauen Schritte der Verarbeitung durch die Datennutzer. Diese können wiederum nur in der sicheren Verarbeitungsumgebung gem Art 73 EHDS auf die elektronischen Gesundheitsdaten zugreifen und keinen direkten Personenbezug herstellen.

ErwGr 66 S 4 EHDS spricht jedoch davon, dass sich die Zugangsstellen gegenüber Betroffenen unter Umständen auf die Ausnahme der Informationspflicht in Art 14 Abs 5 DSGVO berufen können. Insbesondere Art 14 Abs 5 lit b DSGVO sieht hierfür eine Ausnahme bei Datenverarbeitung für wissenschaftliche Forschungszwecke vor. In Art 38 Abs 6 EHDS-E war noch eine generelle Ausnahme von diesem Recht im rechtsverbindlichen Verordnungsteil vorgesehen,¹²³ welche jedoch in der Letztversion der Verordnung nicht mehr vorhanden ist. Gem ErwGr 66 EHDS sollen insbesondere die allgemeinen Berichtspflichten der Zugangsstellen gem Art 59 EHDS die konkreten Informationspflichten gegenüber Betroffenen ersetzen.

Somit bleibt kaum Möglichkeit für die Ausübung der Betroffenenrechte,¹²⁴ wodurch auch Datennutzer nicht mit Auskunftsbegehren konfrontiert werden sollten. Sind sie es doch, können sie den Betroffenenrechten bei Verarbeitung anonymisierter Daten die Nichtanwendbarkeit der DSGVO entgegenhalten. Verarbeiten sie pseudonymisierte Daten

¹²² *Gabauer*, Sekundärnutzung von elektronischen Gesundheitsdaten in *Janisch/Krempelmeier/Mader/Staudegger/Thiele*, Am Glasfaserpuls, 201 (252).

¹²³ *Fähraeus/Reichell/Slokenberga*, The European Health Data Space: Challenges and Opportunities, <https://uu.diva-portal.org/smash/get/diva2:1845108/FULLTEXT01.pdf>, 9 (abgefragt am 14.4.2025).

¹²⁴ *Raji*, Datenräume in der Europäischen Datenstrategie am Beispiel des European Health Data Space, ZD 2023, 3 (7); *Denga*, Nutzungsgovernance, EuZW 2023, 25 (30).

in der sicheren Verarbeitungsumgebung, können sie auf der Basis von Art 11 Abs 2 beziehungsweise Art 12 Abs 2 DSGVO einwenden, dass sie alleine nicht in der Lage sind, die betroffene Person zu identifizieren und somit nicht tätig werden. Somit erscheinen auch die oben getroffenen Überlegungen zum Recht auf Widerspruch gem Art 21 DSGVO von geringer praktischen Relevanz zu sein. Insbesondere wegen der fehlenden Einwilligung der Betroffenen in die Zurverfügungstellung ihrer Gesundheitsdaten und dem abgeschwächten Opt-Out System, welches unter bestimmten Umständen die Möglichkeit der Bereitstellung von elektronischen Gesundheitsdaten trotz Opt-Out vorsieht, wäre die Aufrechterhaltung der Betroffenenrechte jedoch wichtig.¹²⁵

2.3.2 Information der Betroffenen über klinisch signifikante Resultate

Art 61 Abs 5 EHDS normiert den einzigen direkten Nutzen der Sekundärnutzungsbestimmungen des EHDS für Betroffene. Sie sollen über gesundheitlich wesentliche Befunde, die sich aus der Sekundärdatennutzung ihrer elektronischen Gesundheitsdaten ergeben, informiert werden. Datennutzer müssen hierfür in einem ersten Schritt die Zugangsstelle von potentiell klinisch signifikanten Resultaten informieren, da sie selbst schließlich keine direkt personenbezogenen Daten verarbeiten. Die Zugangsstelle soll gem Art 58 Abs 3 EHDS diese Information sodann weiterleiten. Dazu soll zuerst der Dateninhaber von den Resultaten in Kenntnis gesetzt werden, welcher dann wiederum mit dem Betroffenen nach einem Prozess, welcher nationalstaatlich näher definiert werden soll, Kontakt aufnehmen soll. Das kann gem Art 58 Abs 3 auch über die die betreffende natürliche Person behandelnden Angehörige der Gesundheitsberufe geschehen.

Die Pflicht zur Kommunikation dieser sogenannten Incidental Findings („Zufallsbefunde“) wird im Forschungskontext schon länger diskutiert.¹²⁶ Durch das Normieren einer solchen Pflicht für Datenverarbeitung im Rahmen der Sekundärnutzung im EHDS wird jedenfalls Rechtssicherheit für Datennutzer in diesem Bereich geschaffen. Die diesbezüglich notwendige Verarbeitung von Gesundheitsdaten kann als Erfüllung einer rechtlichen Verpflichtung auf Art 6 Abs 1 lit c DSGVO iVm den Ausnahmebestimmungen in Art 9 Abs 2 lit i DSGVO gestützt werden.

¹²⁵ *Staunton et al.*, Ethical and social reflections on the proposed European Health Data Space, *European Journal of Human Genetics* 2024, 498.

¹²⁶ *Wolf et al.*, Managing Incidental Findings in Human Subjects Research: Analysis and Recommendations, *Journal of Law, Medicine & Ethics* 2008, 219.

Fraglich bleibt jedoch, was als wesentlicher Befund gelten soll und wie die Datennutzer zu diesem Ergebnis kommen sollen, wenn sie keinen Zugriff auf die gesamte Krankengeschichte der Betroffenen haben. Informationen über die Wesentlichkeit von Befunden gem Art 94 Abs 2 lit c EHDS sollen jedenfalls vom EHDS-Ausschuss in Konsultation mit Interessenvertreter aus Medizin, Wissenschaft und von Patientenseite ausgearbeitet werden, was zu mehr Klarheit in diesem Bereich führen wird.

Positiv zu werten ist, dass mit dieser Bestimmung durch eine Art „Recht auf Gefundenwerden“¹²⁷ der Nutzen von wissenschaftlicher Forschung für den Einzelnen ersichtlich wird. Andererseits ist an diesem System insbesondere zu kritisieren, dass Betroffene selbst kein Mitspracherecht bezüglich der Frage haben, über welche konkreten Resultat sie informiert werden sollen.¹²⁸ Art 58 Abs 3 EHDS normiert lediglich ein generelles Opt-Out aus der Informationserteilung, wobei wohl die Mitgliedstaaten das diesbezügliche Verfahren festlegen können.

2.3.3 Veröffentlichung und Publikation der Ergebnisse

Spätestens binnen 18 Monaten nach erfolgter Verarbeitung der elektronischen Gesundheitsdaten müssen Datennutzer die Ergebnisse dieser Verarbeitung gem Art 61 Abs 4 EHDS öffentlich machen. Der Bericht soll weiters auch auf der Website der zuständigen Zugangsstelle veröffentlicht werden. Es ist davon auszugehen, dass für beide Zwecke derselbe Bericht veröffentlicht werden kann und dass für die eigene Veröffentlichung ein Eintrag auf der Website des Datennutzers genügen sollte. Zu beachten ist, dass keine personenbezogenen Daten in diesem Bericht veröffentlicht werden dürfen und der EHDS hierfür auch keine Verarbeitungsgrundlage liefert. Darüber hinaus gibt es in der Verordnung keine Anhaltspunkte und Hilfestellungen für Datennutzer in Bezug auf den Inhalt dieses Berichts, außer, dass gem ErwGr 66 EHDS auch Laien als Zielgruppe angesprochen werden sollen. Die Informationspflicht gem Art 61 Abs 4 EHDS könnte demnach zu nicht zu unterschätzendem Mehraufwand für Datennutzer führen. Zusätzlich scheinen damit einhergehende Eingriffe in Immaterialgüterrechte und

¹²⁷ von Kalle, Digitalisierung für Patient:innen denken: Vom Recht auf Gefundenwerden, https://e-health-com.de/fileadmin/user_upload/dateien/Downloads/Vision_Zero_2024_Recht_auf_Gefundenwerden.pdf (abgefragt am 14.4.2025).

¹²⁸ *Staunton et al.*, Ethical and social reflections on the proposed European Health Data Space, *European Journal of Human Genetics* 2024, 498 (502).

Geschäftsgeheimnisse, im Gegenteil zur Bereitstellung der elektronischen Gesundheitsdaten durch Dateninhaber,¹²⁹ keine Beachtung zu finden.

Der Umstand, dass diese Informationen bereitgestellt werden müssen, bedeutet weiters einen Eingriff in die Publikationsstrategie der Datennutzer. Zwar berührt die Veröffentlichungspflicht gem Art 61 Abs 4 EHDS ausdrücklich nicht Veröffentlichungsrechte in wissenschaftlichen Fachzeitschriften oder einer anderen wissenschaftlichen Veröffentlichung. Je nach geforderter Genauigkeit des Berichts und Beschreibung der angewandten Methodik und Resultate könnten Ergebnisse, welche sonst für Publikationen geeignet wären, durch diese Pflicht jedoch vorweggenommen werden. In Art 61 Abs 4 EHDS wird diesem Problem mit der Möglichkeit der Zugangsstellen begegnet, insbesondere bei geplanter Publikation eine Verlängerung der 18-monatigen Frist zu gewähren. Sowohl die Gewährung der Verlängerung als auch deren Länge liegen dabei im Ermessen der Zugangsstellen.

Ein Konflikt mit dieser Bestimmung könnte für Datennutzer durch von Förderverträgen auferlegten Pflichten zur, auch kommerziellen, Ergebnisverwertung entstehen. Förderverträge beinhalten regelmäßig derartige Verpflichtungen. Die Verwertung erfordert wiederum oft einen langwierigen Prozess, insbesondere bei großen Konsortien, in welchen komplexe Verhandlungen über Rechte an Ergebnissen geführt werden müssen. Dieser Umstand kann als Begründung einer Fristverlängerung gem Art 61 Abs 4 EHDS dienen. Andernfalls könnten die Ergebnisse auch nur auf einer Metaebene beziehungsweise in aggregierter Form veröffentlicht werden, was ihrer Verwertung nicht im Weg stünde. Da Artikel 61 Abs 4 EHDS vorschreibt, dass die Resultate oder Ergebnisse ohnehin nur anonyme Daten enthalten dürfen, ist die Veröffentlichung der Ergebnisse in aggregierter Form naheliegend. Dies könnte die in ErwGr 66 EHDS geforderte Transparenz über die Ergebnisse der Sekundärnutzung ermöglichen, ohne die Verwertung von Ergebnissen nach einem längeren Zeitraum unmöglich zu machen. Demnach dient diese Verpflichtung primär dem Zweck der Transparenz über Datenverarbeitungen und der Sichtbarkeit des EHDS. Eine Verpflichtung der Datennutzer, Ergebnisse in ihrer Gänze öffentlich zur Verfügung zu stellen, ist dadurch nicht intendiert. Ähnliche Regelungen finden sich auch bei anderen Datenräumen.¹³⁰ So verpflichtet beispielsweise auch § 31 Abs 6 Z 4

¹²⁹ Näheres unter 3.2.2.

¹³⁰ *Towards European Health Data Space*, Description of steps in accessing individual-level data for national and EU researchers in a selection of centralised systems and decentralised systems

Bundesstatistikgesetz die Nutzer des AMDC zur Veröffentlichung der Hauptergebnisse des Forschungsvorhabens über das Internet.¹³¹

Zusätzlich ist zu beachten, dass gem Art 61 Abs 4 EHDS sowohl der Umstand der Verwendung von elektronischen Gesundheitsdaten im Rahmen des EHDS als auch deren Quelle bei wissenschaftlichen Publikationen und anderer Verwendung angegeben werden müssen. Die rechtsverpflichtende Angabe des ursprünglichen Dateninhabers ist insbesondere bei Verwendung von Datensätzen zu begrüßen. Deren Sammlung und Annotation geht üblicherweise mit einem hohen Aufwand einher, weswegen das Überlassen jener Datensätze die Akzeptanz des Sekundärnutzungssystems bei Forschenden in Frage stellen könnte. Die Verpflichtung zur Nennung der Quelle kann diesen jedoch trotz verpflichtetem Teilen ihrer Datensätze zu gewisser akademischen Gratifikation verhelfen.

2.3.4 Begleichen der Kosten

Datennutzern werden in der Datengenehmigung gem Art 68 Abs 10 lit g EHDS sowohl die Kosten der Zugangsstelle als auch die Kosten des Dateninhabers unter einem in Rechnung gestellt. Bereits vor Ausstellen der Datengenehmigung soll den Datennutzern gem Art 62 Abs 5 EHDS eine Einschätzung der erwartbaren Gebühren übermittelt werden. Jedoch kann selbst nach erteilter Datengenehmigung noch eine Verhandlung über den Gebührenteil der Dateninhaber erfolgen, wobei die Zugangsstellen bei deren Scheitern eine verhältnismäßige Gebühr festlegen können. Forschende, öffentliche Stellen und Kleinunternehmer sollten zusätzlich überprüfen, ob der für die Datengenehmigung zuständige Mitgliedsstaat eine Gebührenermäßigung gem Art 62 Abs 1 EHDS für die Bereitstellung der elektronischen Gesundheitsdaten vorgesehen hat. Durch gezieltes Anfordern von Datensätzen in Mitgliedsstaaten, welche diese Gebührenermäßigung vorsehen, können insbesondere im kostensensiblen Bereich der öffentlich finanzierten Forschung Einsparungen erzielt werden.¹³²

<https://tehdas.eu/app/uploads/2022/04/tehdas-report-description-of-steps-in-accessing-individual-level-data-for-national-and-eu-researchers-in-a-selection-of-centralised-systems-and-decentralised-systems.pdf>, 27 (abgefragt am 14.4.2025).

¹³¹ siehe auch *Austrian Micro Data Center*, Vertragsmuster für die Nutzung des AMDC, https://www.statistik.at/fileadmin/pages/1805/Vertragsmuster_AMDC.pdf, § 5 Abs 7 (abgefragt am 14.4.2025).

¹³² Näheres unter 3.4.

3 Dateninhaber

3.1 Datenabfrage

Datenanträge betreffen andererseits auch Dateninhaber gem Art 2 Abs 2 lit t EHDS. Das sind natürliche oder juristische Personen oder öffentliche Stellen oder Behörden, welche die Pflicht oder das Recht haben, elektronische Gesundheitsdaten für bestimmte Zwecke einschließlich der Gesundheitsversorgung und Forschung zu verarbeiten.¹³³ Ihre zentrale Aufgabe im Sekundärnutzungssystem ist es, den Zugangsstellen auf Anfrage gem Art 60 Abs 1 EHDS gewisse Kategorien elektronischer Gesundheitsdaten zur Verfügung zu stellen. Dabei ist die Definition elektronischer Gesundheitsdaten für sich genommen nicht ausreichend, um ihr einen sinnvollen Inhalt beizumessen. Art 2 Abs 2 lit c EHDS definiert elektronische Gesundheitsdaten zirkulär als „personenbezogene oder nicht personenbezogene elektronische Gesundheitsdaten“.¹³⁴ Somit ist umso mehr Augenmerk auf die einzelnen Kategorien der zur Verfügung zu stellenden elektronischen Gesundheitsdaten zu legen.

Diese Kategorien werden in Art 51 Abs 1 EHDS aufgezählt. Insbesondere elektronische Gesundheitsdaten aus EHR gem Art 51 Abs 1 lit a EHDS nehmen in der Sekundärnutzung eine zentrale Rolle ein. Insofern setzen auch die Sekundärnutzungsbestimmung im EHDS auf den Primärnutzungsbestimmungen auf. Die anderen bereitzustellenden Datensätze umfassen einerseits bestimmte Datenarten, welche unabhängig von deren Erhebung zur Verfügung gestellt werden müssen. Hier sind insbesondere Verwaltungsdaten zur Gesundheitsversorgung gem Art 51 Abs 1 lit e EHDS und genetische, epigenomische und genomische Daten gem Art 51 Abs 1 lit f EHDS zu erwähnen. Andererseits müssen auch Datensätze nach bestimmten Erhebungsformen zur Verfügung gestellt werden. Darunter fallen gem Art 51 Abs 1 lit m EHDS, für Forschende relevant, insbesondere Daten von Studien und Prüfungen gem der Clinical Trials Regulation,¹³⁵ der SOHO,¹³⁶ der

¹³³ Näheres zu Begriffsdefinitionen unter 1.2.

¹³⁴ kritisch *Detting*, Was sind Daten in der Arzneimittelentwicklung und im neuen Datennutzungsrecht (Data Act und European Health Data Space)?, *PharmR* 2024, 473 (488).

¹³⁵ Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG, ABl L 158/1.

¹³⁶ Verordnung (EU) 2024/1938 des Europäischen Parlaments und des Rates vom 13. Juni 2024 über Qualitäts- und Sicherheitsstandards für zur Verwendung beim Menschen bestimmte Substanzen

Medizinproduktverordnung¹³⁷ und der IVDR¹³⁸. Gem Art 51 Abs 1 lit p EHDS unterliegen auch gesundheitsbezogene Daten aus Forschungskohorten, Fragebögen und Erhebungen der Pflicht zur Bereitstellung, dies jedoch nur nach Erstpublikation der Ergebnisse. Mitgliedstaaten können gem Art 51 Abs 2 EHDS weitere Kategorien elektronischer Gesundheitsdaten zur Sekundärnutzung durch eine Öffnungsklausel freigeben. Insbesondere die Einbeziehung elektronischer Gesundheitsdaten sogenannter Wellness-Anwendungen¹³⁹ gem Art 51 Abs 1 lit i EHDS wurde von EDSA und EDSB wegen Bedenken bezüglich Datenqualitätsanforderungen und möglichen Rückschlüssen auf andere sensible Informationen kritisiert.¹⁴⁰

Zu beachten ist, dass keine zeitliche Begrenzung der Bereitstellungsverpflichtung dieser Datensätze im EHDS vorgesehen ist. Dateninhaber müssen demnach nach Anwendbarkeit der Bestimmungen ihre derzeitigen Datenbestände auf relevante Datensätze gem Art 52 Abs 1 EHDS überprüfen.

Wurde dieses Basislevel an Datensätzen identifiziert, muss gem Art 60 Abs 3 EHDS eine allgemeine Beschreibung davon an die nationale Zugangsstelle übermittelt werden. Bezüglich des Inhaltes der Beschreibung kann auf Durchführungsrechtsakte der Europäischen Kommission gem 77 Abs 4 EHDS verwiesen werden, welche zur näheren Ausgestaltung erlassen werden sollen. Zusätzlich ist bei Datensätzen, welche in Projekten

menschlichen Ursprungs und zur Aufhebung der Richtlinien 2002/98/EG und 2004/23/EG, ABl L 2024/1938.

¹³⁷ Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates, ABl L 117/1.

¹³⁸ Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission, ABl L 117/176.

¹³⁹ Das ist gem Art 2 Abs 2 lit a EHDS Software oder eine Kombination aus Software und Hardware, welche vom Hersteller für die Verwendung durch eine natürliche Person bestimmt ist, elektronische Gesundheitsdaten verarbeitet und speziell der Bereitstellung von Informationen über die Gesundheit natürlicher Personen oder der Leistung von Pflege zu anderen Zwecken als der Gesundheitsversorgung dient.

¹⁴⁰ EDSA/EDSB, Gemeinsame Stellungnahme 3/2022, Rz 35.

mit Förderung auf europäischer oder nationaler Ebene erhoben werden, ein Qualitäts- bzw. Nutzungslabel mit dem in Art 78 Abs 3 vorgeschriebenen, sehr ausführlichen, Inhalt verpflichtend anzubringen. Dateninhaber sind gem Art 60 Abs 3 EHDS dazu verpflichtet, die Beschreibung ihrer Datensätze im Katalog der Zugangsstellen mindestens einmal jährlich zu überprüfen.

Wird ein Datenantrag von der Zugangsstelle positiv bewertet und eine Datengenehmigung ausgestellt, wird diese an den Dateninhaber weitergeleitet. Der Dateninhaber soll der darin enthaltenen Aufforderung zur Bereitstellung der elektronischen Gesundheitsdaten gem Art 60 Abs 2 EHDS in einer angemessenen Zeit nachkommen, wobei im Normalfall drei Monate hierfür die Obergrenze bilden. Die Angemessenheit der Frist wird wohl nach dem Umfang des Datenantrags zu beurteilen sein. Der Dateninhaber muss spätestens zu diesem Zeitpunkt Rechte an seinen Datensätzen identifiziert haben, um diese auch effektiv in diesem System geltend machen zu können.

3.2 Geistiges Eigentum und Geschäftsgeheimnisse

3.2.1 Rechte an Daten

Um die Notwendigkeit des rechtlichen Schutzes von medizinischen Datensätzen aufzeigen zu können, soll zunächst die Schutzfähigkeit von Daten als Rechtsgut geklärt werden. Daten haben einen mitunter monetär ausdrückbaren Wert,¹⁴¹ den es zu schützen gilt. In Bezug auf Schutzmaßnahmen kann grundsätzlich zwischen technischen und rechtlichen Schutz unterschieden werden.¹⁴²

Für gewöhnlich werden Daten rein technisch geschützt – durch den physischen Verbleib in der Sphäre der Verarbeitenden ist die Zuordnungsfrage geklärt.¹⁴³ Über rechtliche Schutzmaßnahmen, i.e. Rechte an Daten, informieren sich die Verarbeitenden regelmäßig aufgrund fehlender Notwendigkeit nicht. Im System des EHDS müssen vorhandene Gesundheitsdaten jedoch unter Umständen zur Verfügung gestellt werden.¹⁴⁴ Dies durchbricht rein technische Schutzmaßnahmen und erfordert eine nähere Auseinandersetzung mit rechtlichen Schutzmechanismen.

Daten sind an sich, entgegen der Bezeichnung „Dateninhaber“ im System des EHDS, dem Sachenrecht nicht zugänglich. Somit gibt es auch kein Eigentum an Daten im sachenrechtlichen Sinn.¹⁴⁵ Die „Befugniß, mit der Substanz und den Nutzungen einer Sache nach Willkür zu schalten, und jeden Andern davon auszuschließen“¹⁴⁶ wird vielmehr durch punktuelle Rechte an Daten und Datensätzen ersetzt. Diese müssen in anderen Regelwerken außerhalb des Kernzivilrechts gesucht werden. Gesetzlich angeordnet ist hierbei primär das Datenschutzrecht, welches einzelne Rechtspositionen und rechtliche Ansprüche von Betroffenen über ihre personenbezogenen Daten normiert. Im gegenständlich relevanten Fall sind jedoch Dateninhaber und Betroffener zwei

¹⁴¹ *Fiske/Degelsegger-Márquez/Marsteurer/Prainsack*, Value-creation in the health data domain: a typology of what health data help us do, *BioSocieties* 2022, 473.

¹⁴² *Horeth*, Intellectual Property in Innovationskooperationen (2021), 345.

¹⁴³ *Straub*, Datenhoheit und Datenschutz aus Nutzer-, Verbraucher- und Patientenperspektive in *Rohde/Bürger/Peneva/Mock*, Datenwirtschaft und Datentechnologie (2022), 167.

¹⁴⁴ kritisch *Roos/Maddaloni*, Regulierter Datenaustausch zur Gesundheitsforschung, *RDi* 2023, 225 (229).

¹⁴⁵ *Holzner* in *Rummel/Lukas*, ABGB⁴ § 285 Rz 4.

¹⁴⁶ § 354 ABGB.

verschiedene Personen. Dateninhabern können hierbei im Wesentlichen zwei Rechtsinstrumente zugutekommen: Urheberrecht bzw verwandte Schutzrechte und der Geschäftsgeheimnisschutz.¹⁴⁷

3.2.1.1 Datenbankschutz durch Urheberrecht und verwandte Schutzrechte

Rechte an Daten können durch die Identifizierung immaterialgüterrechtlicher Positionen sichergestellt werden. Insbesondere das Urheberrecht eignet sich als Grundlage dafür. Zentraler Anknüpfungspunkt des urheberrechtlichen Schutzes ist dabei der Werkbegriff. Gem § 1 UrhG¹⁴⁸ liegt ein Werk bei einer eigentümlichen geistigen Schöpfung auf den Gebieten der Literatur, der Tonkunst, der bildenden Künste oder der Filmkunst vor. Das anthropozentrische Urheberrecht schützt somit den dem Werk zugrundeliegenden Denkprozess einer natürlichen Person und nicht etwa den Informationsgehalt eines Objekts. Aus diesem Grund steht Rohdaten¹⁴⁹ und bloßen Erkenntnissen wissenschaftlichen Erhebungen ohne bestimmte Formung¹⁵⁰ auch kein urheberrechtlicher Schutz zu. Die im üblichen Behandlungsprozess einer Krankenanstalt anfallenden Gesundheitsdaten und quantitative Forschungsdaten sind daher grundsätzlich nicht urheberrechtlich geschützt.¹⁵¹ Eine Weiterverarbeitung dieser Daten kann jedoch durchaus rechtlich begrenzt sein. Hierfür ist nicht primär auf die üblichen Werkkategorien Literatur, Tonkunst, bildende Kunst und Filmkunst in § 1 Abs 1 UrhG Bedacht zu nehmen,¹⁵² sondern auf den Schutz als Datenbankwerk gem § 40f Abs 2 UrhG beziehungsweise auf den sui generis Schutz der schlichten Datenbank gem § 76c UrhG.

¹⁴⁷ *Dürager*, Sind Daten ein schutzfähiges Gut?, ÖBl 2018, 260.

¹⁴⁸ Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz), BGBl. Nr. 111/1936.

¹⁴⁹ *Humer*, Schutz für KI-Trainingsdaten sowie Rohdaten, *ecolex* 2024, 467; *Ciresa*, *Praxishandbuch Urheberrecht*³ (2022), 63.

¹⁵⁰ OGH 9. 11. 1999, 4 Ob 282/99w.

¹⁵¹ *Baumann/Krahn/Lauber-Rönsberg*, *Forschungsdatenmanagement und Recht* (2021), 27.

¹⁵² für CT- und MRT-Scans siehe jedoch 3.2.1.2.

Basierend auf der DatenbankRL¹⁵³ und völkerrechtlichen Vorgaben¹⁵⁴ wurden Datenbanken als eigener Schutzgegenstand in das nationale Urheberrecht eingeführt. Gemäß der Definition von § 40f Abs 1 UrhG und der Rechtsprechung des EuGH¹⁵⁵ müssen folgende Faktoren für die grundlegende Einordnung als Datenbank vorliegen: die Unabhängigkeit der einzelnen Elemente, die systematische oder methodische Anordnung derselben und die einzelne Zugänglichkeit der Elemente. Kann somit einer Anordnung von Elementen eine Logik bzw Struktur entnommen werden, welche dazu führt, dass einzelne Elemente identifiziert und entnommen werden können, ohne, dass der Wert ihres informativen Inhalts dadurch beeinträchtigt wird, liegt eine Datenbank gem § 40f Abs 1 UrhG vor.¹⁵⁶ Dabei ist zu beachten, dass sich der Datenbankschutz nur auf die Anordnung der Daten, nicht aber auf die enthaltenen Elemente selbst erstreckt.¹⁵⁷

Wurde eine Datenbank gem § 40f Abs 1 UrhG identifiziert, sollte zuerst geprüft werden, ob ein Datenbankwerk gem § 40f Abs 2 UrhG vorliegt. Ein Datenbankwerk stellt systematisch eine Untergruppe des Sammelwerks gem § 6 UrhG dar, bei dem urheberrechtlicher Schutz für die durch Auswahl oder Anordnung des Stoffs erzielte schöpferische Eigenart einer Sammlung, insbesondere bei literarischen und wissenschaftlichen Werken, gewährt wird.¹⁵⁸ Eine ausreichende Originalität einer Datenbank liegt vor, wenn „[...] der Urheber über die Auswahl oder Anordnung der in ihr enthaltenen Daten seine schöpferischen Fähigkeiten in eigenständiger Weise zum Ausdruck bringt, indem er freie und kreative Entscheidungen trifft.“¹⁵⁹ Hingegen soll kein urheberrechtlicher Schutz bestehen, wenn die „[...] Herstellung der Datenbank durch

¹⁵³ Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken, ABl L 1996/77, 20.

¹⁵⁴ Art 10 Abs 2 Agreement on Trade-Related Aspects of Intellectual Property Rights as Amended by the 2005 Protocol Amending the TRIPS Agreement.

¹⁵⁵ EuGH 9.11.2004, C-444/02, *Fixtures Marketing*, ECLI:EU:C:2004:697.

¹⁵⁶ Thiele, Urheberrechtliche Fragen der Weitergabe und Veröffentlichung von personenbezogenen Daten in der Forschung in *Jahnel/Krempelmeier/Schmid*, Wissenschaft und Datenschutz (2024), 160.

¹⁵⁷ Nägele/Apel, Immaterialgüterrecht in *Kaulartz/Braegelman*, Rechtshandbuch Artificial Intelligence und Machine Learning (2020), Rz 28.

¹⁵⁸ Schumacher in *Handig/Hofmarcher/Kucsko*, urheber.recht³ (2023) § 6 UrhG Rz 7.

¹⁵⁹ EuGH 1.3.2012, C-604/10, *Football Dataco v Yahoo*, ECLI:EU:C:2012:115 Rz 38.

technische Erwägungen, Regeln oder Zwänge bestimmt wird, die für künstlerische Freiheit keinen Raum lassen [...].“¹⁶⁰ Insbesondere bei der Aufarbeitung von Rohdaten für wissenschaftliche Zwecke wie dem Training von KI-Modellen wird das schöpferische Element durch die Auswahl der Daten und der dahinterliegenden Kreativität zu bejahen sein, vor allem, wenn in origineller Weise neue und unkonventionelle Datenquellen für das Training miteinbezogen werden.¹⁶¹ Hingegen wird bei Datenbanken zur internen Verwaltung die notwendige Originalität wegen der technischen und inhaltlichen Vorgaben eher zu verneinen sein.

Daneben besteht noch die Möglichkeit des sui generis Schutzes als schlichte Datenbank gem § 76c UrhG. Hierfür muss zu den oben beschriebenen grundlegenden Datenbankkriterien gem § 40f Abs 1 UrhG eine wesentliche Investition hinzutreten. Die Abgrenzung der berücksichtigungswerten Investitionen und deren geforderte Wesentlichkeit stellt die zentrale Frage für den Datenbankschutz dar. Berücksichtigungswert sind nur Investitionen in die Beschaffung, Überprüfung oder Darstellung des Inhalts der Datenbank und nicht, da Daten an sich eben nicht geschützt werden sollen, in die Datenerzeugung.¹⁶² Richtet sich eine Investition daher primär auf andere Zwecke als den Aufbau der Datenbank, soll sie keine Berücksichtigung finden.¹⁶³ Dieser Punkt ist insbesondere bei der Systematisierung elektronischer Gesundheitsdaten von Relevanz, da hierfür regelmäßig beträchtliche Investitionen finanzieller und personeller Natur in die Datenerhebung fließen, welche jedoch für den sui generis Schutz schlichter Datenbanken unbeachtlich sind. Inhaltlich können Investitionen sowohl personeller, finanzieller und technischer Natur sein, was vor allem bedeutet, dass eine Investition nicht unbedingt in Geldwert ausdrückbar sein muss, um von Relevanz zu sein. Investitionen können demnach je nach Bezifferbarkeit sowohl quantitativer als auch qualitativer Natur sein.¹⁶⁴ Bei Datenbanken, welche aus ausgewählten und aufbereiteten Rohdaten bestehen, um etwa dem Training von ML-Modellen zu dienen, sollte dieses Kriterium, auch wegen des personellen Aufwandes, in der Regel erfüllt sein. Zu beachten

¹⁶⁰ EuGH *Football Dataco v Yahoo* Rz 39.

¹⁶¹ *Hacker*, Immaterialgüterrechtlicher Schutz von KI-Trainingsdaten, GRUR 2020, 1025 (1028).

¹⁶² OGH 4 Ob 206/14v jusIT 2015, 184 (*Staudegger*) = ecolex 2015, 798 (*Tonninger*).

¹⁶³ *Woller* in *Handig/Hofmarcher/Kucsko*, urheber.recht³ § 76c UrhG Rz 24.

¹⁶⁴ *Dokalik* in *Dokalik/Zemann*, Urheberrecht⁸ (2022) Art 7 Datenbanken-RL E 6.

ist, dass die Rechte an Datenbankwerken und der sui generis Schutz schlichter Datenbanken durch die voneinander getrennten Schutzzwecke des Schutzes geistiger Schöpfungen auf der einen Seite und Investitionen auf der anderen Seite, voneinander unabhängig sind und daher auch gemeinsam bestehen können.¹⁶⁵

Der Schutz des Datenbankwerks gem § 40f Abs 2 UrhG kommt dem Schöpfer der Datenbank zugute. Dieser ist gemäß dem Schöpferprinzip von § 10 UrhG derjenige, welcher die Datenbank als eigentümliche geistige Schöpfung geschaffen hat. Eine Urheberschaft juristischer Personen, etwa der Universität oder des Unternehmens, für welche die Datenbank zusammengestellt wird, ist im anthropozentrischen Urheberrecht nicht vorgesehen. Dieser Grundsatz wird jedoch durch die mittels Arbeitsvertrag abänderbare, verpflichtenden Einräumung eines Werknutzungsrechts für im Zuge der Tätigkeit als Dienstnehmer geschaffenen Datenbankwerken an den Dienstgeber gem § 40f Abs 3 iVm § 40b UrhG abgeschwächt.¹⁶⁶

Die Schutzrechte an schlichten Datenbanken kommen hingegen gem § 76c Abs 1 UrhG ihrem Hersteller zugute. Das ist gem § 76d Abs 1 derjenige, der die geforderte wesentliche Investition getätigt hat. Hierfür wird nicht auf eine kreative, menschliche Schöpfungsleistung abgestellt, sondern auf diejenige juristische oder natürliche Person, welche die Initiative zur Schaffung der Datenbank ergreift und das Investitionsrisiko im Sinne der Gefahr der Nicht-Amortisierung trägt.¹⁶⁷ Bei Forschungsinstituten ist dies demnach regelmäßig das Institut selbst als juristische Person und nicht die dazugehörigen Arbeitnehmer.¹⁶⁸

Geschützt ist bei beiden Datenbankkategorien ein Bündel an Ausschließlichkeit vermittelnden Verwertungsrechten, welches für Datenbankwerke kraft Werkeigenschaft aus dem dritten Abschnitt des UrhG zu entnehmen ist, während es für schlichte Datenbanken in § 76c Abs 1 UrhG nachgebildet wird. Im Kontext der Zurverfügungstellung von Datensätzen im Rahmen des EHDS ist insbesondere das dem Urheber beziehungsweise dem Hersteller vorbehaltene Recht auf Vervielfältigung gem §

¹⁶⁵ EuGH *Football Dataco v Yahoo* Rz 27.

¹⁶⁶ siehe beispielsweise OGH 4 Ob 58/04i MR 2004, 331 (*Walter*).

¹⁶⁷ *Woller* in *Handig/Hofmarcher/Kucsko*, urheber.recht³ § 76d UrhG Rz 4.

¹⁶⁸ ErwGr 41 DatenbankRL.

15 UrhG von Relevanz, da die Bereitstellung der Datensätze schon in einem ersten Schritt der Übermittlung an die Zugangsstellen in dieses Ausschließungsrecht eingreift.

In dieses Recht wird, in europarechtskonformer Interpretation des § 15 UrhG im Lichte von Art 5a DatenbankRL bei Datenbankwerken bereits eingegriffen, wenn bloß ein Teil der Datenbank vervielfältigt wird. Bei schlichten Datenbanken ist primär die Entnahme von Datensätzen, welche einen qualitativ oder quantitativ wesentlichen Teil derselben ausmachen, geschützt. Ein qualitativ wesentlicher Teil liegt vor, wenn der wirtschaftliche Wert des entnommenen Teils im Verhältnis zum Wert des Gesamtinhalts entweder in Hinblick auf den verursachten Schaden oder anhand des Investitionsaufwandes gegeben ist,¹⁶⁹ wobei ein Teil jedenfalls als wesentlich anzusehen ist, wenn in ihm alleine eine wesentliche Investition verkörpert ist.¹⁷⁰ Liegt beispielsweise eine Datenbank mit KI-Trainingsdaten aus retrospektiven und eigens für das KI-Training durchgeführten prospektiven Studien vor, welche dafür mit großem Personalaufwand aufbereitet wurden, wird auch die bloße Entnahme der prospektiven Daten die Entnahme eines qualitativ wesentlichen Teils der Datenbank gem § 76d Abs 1 UrhG darstellen. Daneben ist auch die Entnahme eines unwesentlichen Teils einer Datenbank als Eingriff zu werten, solange diese wiederholt und systematisch erfolgt.¹⁷¹ Dieser Auffangtatbestand soll vermeiden, dass eine Entnahmehandlung in mehrere kleinere Handlungen aufgeteilt wird, um so den Schutz zu umgehen.¹⁷²

Ein Eingriff in ein urheberrechtlich geschütztes Ausschließungsrecht bedeutet per se noch keine Verletzung dieses Rechts. Eingriffe können entweder als freie Werknutzungen gem des siebten Abschnitts UrhG gerechtfertigt sein oder durch Lizenzverträge gem § 24 UrhG ermöglicht werden. Freie Werknutzungen sind gesetzlich bestimmte Verwertungsarten, welche trotz urheberrechtlichem beziehungsweise verwandtem Schutz zulässig sind. Hierbei ist die Unterscheidung zwischen Datenbankwerken und schlichten Datenbanken besonders bedeutsam, da für beide Datenbankarten verschiedene freie (Werk-)Nutzungen möglich sind.

¹⁶⁹ OGH 4 Ob 25/04m ecolex 2004, 722 (*Beck*).

¹⁷⁰ OGH 4 Ob 206/14v jusIT 2015, 184 (*Staudegger*) = ecolex 2015, 798 (*Tonninger*).

¹⁷¹ *Zemann* in *Dokalik/Zemann*, Urheberrecht⁸ § 76d UrhG E 11.

¹⁷² *Woller* in *Handig/Hofmarcher/Kucsko*, urheber.recht³ § 76d UrhG Rz 28.

Bei Datenbankwerken ist insbesondere auf die freie Werknutzung gem § 40h Abs 2 UrhG iVm § 42 Abs 2 UrhG Bedacht zu nehmen. Diese erlaubt die Vervielfältigung einzelner Datenbankwerke beziehungsweise Teile davon zum eigenen Gebrauch zu Zwecken der nicht kommerziellen Forschung auf jeglichem Trägermedium. Nicht kommerzielle Forschung ist sowohl in naturwissenschaftlicher- als auch geisteswissenschaftlicher¹⁷³ grundlagen- und anwendungsorientierter Forschung zu sehen.¹⁷⁴ Die Wortfolge „zum eigenen Gebrauch“ in § 42 Abs 2 UrhG soll ausdrücken, dass es gem § 42 Abs 5 UrhG zu keiner Verbreitung des Vervielfältigungsstücks in die Öffentlichkeit kommen soll. Sie beschränkt jedoch nicht die Anwendung der freien Werknutzung auf natürliche Personen und umfasst daher auch juristische Personen und allgemein Forschungseinrichtungen aller Art. Beachtung ist daher eher der Einschränkung der freien Werknutzung auf nicht kommerzielle Zwecke zu schenken. Die Kommerzialität des Forschungszwecks ist konkret auf das jeweilige Forschungsvorhaben einzelfallbezogen zu beurteilen. Unter „nicht kommerziellen Zwecken“ ist primär das Fehlen einer Gewinnerzielungsabsicht zu verstehen, wobei eine Finanzierung beziehungsweise Mitfinanzierung durch Drittmittel ebenso wenig schadet wie die vergütete Publikation der Forschungsergebnisse.¹⁷⁵ Insgesamt wird durch diese Ausnahme dennoch eine vergleichsweise breite Nutzung urheberrechtlich geschützter Datenbanken ermöglicht.¹⁷⁶ Datennutzer, welche über den EHDS Forschung zur Gewinnerzielungsabsicht betreiben wollen, etwa zur Entwicklung von Lifestyle-Apps, müssen demnach jedoch beachten, dass sie keine freie Werknutzung für den Zugang zu Datenbankwerken in Anspruch nehmen können und daher auf die Zustimmung des Urhebers durch Lizenzvertrag gem § 24 UrhG angewiesen sind.

Die freie Nutzung schlichter Datenbanken gem § 76d Abs 3 Z 2 UrhG erlaubt analog zu der oben angeführten freien Werknutzung zu Forschungszwecken die Vervielfältigung eines wesentlichen Teils der Datenbank. Diese Nutzung ist jedoch zweifach begrenzt. Einerseits ist auch sie nur ohne Erwerbszweck zulässig, andererseits ist sie nur anwendbar auf gem § 8 UrhG veröffentlichte Datenbanken. Die Veröffentlichung gem § 8 UrhG setzt das freiwillige Zugänglichmachen gegenüber der Allgemeinheit beziehungsweise einem

¹⁷³ ErwGr 36 DatenbankRL.

¹⁷⁴ *Zemann in Handig/Hofmarcher/Kucsko*, urheber.recht³ § 42 UrhG Rz 24.

¹⁷⁵ *Ciresa in Ciresa*, Österreichisches Urheberrecht (24. Lfg 2024) § 42 UrhG Rz 39.

¹⁷⁶ siehe beispielsweise die urheberfreundlichere Regelung in § 60c deutsches UrhG.

breiten Publikum voraus.¹⁷⁷ Dieses fehlt im Kontext des EHDS jedoch offensichtlich, da Dateninhaber durch Bescheid zur Bereitstellung verpflichtet sind und daher keine freiwillige Veröffentlichung vorliegt. Das Ergebnis wäre ein weitergehender Schutz von schlichten Datenbanken im Vergleich mit Datenbankwerken, was prima facie als wertungswidrig erscheint. Unter Umständen wäre aus diesem Grund im Anwendungsbereich des EHDS eine teleologische Reduktion des Öffentlichkeitsbegriffs in § 76d Abs 3 Z 2 UrhG angebracht. Andernfalls sei es Dateninhabern empfohlen, sich aufgrund der Parallelität der Rechte aus Datenbankwerken und schlichten Datenbanken auf letztere zu berufen.

Ist keine freie Werknutzung für die Verwertung eines durch Urheberrecht geschützten Werks anwendbar, kann der Eingriff dennoch gem § 26 UrhG durch Vertrag zwischen Urheber und Eingreifenden ermöglicht werden. Dieser Vertrag unterliegt der zivilrechtlichen Vertragsfreiheit.

3.2.1.2 Sonstige geschützte elektronische Gesundheitsdaten

Ähnliche Überlegungen wie jene zu schlichten Datenbanken können punktuell zu anderen elektronischen Gesundheitsdaten getroffen werden. So sind beispielsweise CT- und MRT-Scans als schlichte Lichtbilder zu qualifizieren, da ihnen zwar nicht die nötige Schöpfungshöhe für ein Lichtbildwerk zukommt, jedoch kraft ihres Lichtbildcharakters dennoch ein gewisser Schutz gem § 74 UrhG zugutekommt. Der Hersteller, bei in Krankenanstalten aufgenommenen CT- und MRT-Scans ist dies der Krankenanstaltsträger, hat insbesondere das alleinige Recht auf Vervielfältigung und Verbreitung dieser Lichtbilder,¹⁷⁸ worin durch die Bereitstellung im EHDS auch eingegriffen wird.

Die oben zu Datenbankwerken getroffenen Überlegungen zur freien Werknutzung sind qua Verweis in § 74 Abs 7 UrhG auch bei schlichten Lichtbildern von Relevanz. Im Ergebnis führt die Anwendung von § 74 Abs 7 UrhG iVm § 42 Abs 2 UrhG demnach wie bei Datenbankwerken zum Ergebnis einer freien Werknutzung für nicht-gewinnorientierte Zwecke. Auch diese Divergenz zwischen Lichtbildern und anderen elektronischen Gesundheitsdaten läuft dem intendierten Zweck des EHDS zum möglichst freien Datenaustausch prima facie zuwider.

¹⁷⁷ *Ciresa in Ciresa*, Österreichisches Urheberrecht (20. Lfg 2018) § 8 UrhG Rz 14.

¹⁷⁸ *Herda*, Die Verwendung von Patientenbildern durch die Krankenanstalt: Zustimmungserfordernis für Patienten?, RdM 2024, 137.

3.2.1.3 Geschäftsgeheimnisschutz

Neben Urheberrechten und verwandten Schutzrechten kann auch Geschäftsgeheimnissen gem der RL zum Schutz von Geschäftsgeheimnissen¹⁷⁹ rechtlicher Schutz zugutekommen. Ein Geschäftsgeheimnis ist gem § 26b UWG¹⁸⁰ eine „Information, die

1. geheim ist, weil sie weder in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen zu tun haben, allgemein bekannt noch ohne weiteres zugänglich ist,
2. von kommerziellem Wert ist, weil sie geheim ist, und
3. Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen durch die Person ist, welche die rechtmäßige Verfügungsgewalt über diese Informationen ausübt.“

Durch den Geschäftsgeheimnisschutz kann demnach ein Recht an Daten durch faktische Exklusivität begründet werden.¹⁸¹ Darin ist im Sinne eines Zugangsschutzes der rechtswidrige Erwerb von Geschäftsgeheimnissen und somit die Zwischenstufe am Weg zum „echten“, absoluten Immaterialgüterrecht, wie dem Patent- und Urheberrecht, geschützt. Der Geschäftsgeheimnisschutz ist daher insbesondere im Forschungs- und Entwicklungsbereich Bedeutung von Relevanz und schützt dort technologisches Know-How.¹⁸²

Einer Information kommt Geheimnischarakter gem § 26b Abs 1 Z 1 UWG zu, wenn sie sowohl hinsichtlich ihrer Gesamtheit als auch ihrer genauen Anordnung und Zusammensetzung keine allgemeine Bekanntheit in den relevanten Verkehrskreisen genießt. Dabei ist auch auf Experten des Verkehrskreises abzustellen.¹⁸³ Der allgemeinen Bekanntheit ist gleichzuhalten, dass die Information ohne Weiteres zugänglich ist, also

¹⁷⁹ Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABI L 157/1.

¹⁸⁰ Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG, BGBl. Nr. 448/1984.

¹⁸¹ Kornmeier/Baranowski, Das Eigentum an Daten - Zugang statt Zuordnung, BB 2019, 1219 (1223).

¹⁸² Zinober/Bogensberger, Praxishandbuch Know-how und Geschäftsgeheimnisse (2020), 8.

¹⁸³ Thiele in Wiebe/Kodek, UWG² § 26b Rz 12.

ohne erheblichen Aufwand und Einsatz an Zeit, Mühe, Kosten und/oder Geschick mit ansonsten lauterer Mitteln erlangt werden kann.¹⁸⁴ Das Teilen von Datensätzen im Konsortium eines wissenschaftlichen Forschungsprojekts schließt bei dem üblichen Abschluss von Vertraulichkeitsvereinbarungen (Non Disclosure Agreements) den Geheimnischarakter einer Information nicht aus beziehungsweise spricht gerade die Notwendigkeit solcher Vereinbarungen für die Einordnung als geheime Information.

Weiters muss die Information gem § 26b Abs 1 Z 2 UWG einen zumindest mittelbaren kommerziellen Wert haben und somit geschäftsrelevant sein. Die Wettbewerbsposition des berechtigten Inhabers muss durch die unbefugte Verwendung der geheimen Information bedroht werden, weswegen ein ideeller Wert alleine nicht ausreicht. Insgesamt ist hier ein großzügiger Maßstab anzulegen.¹⁸⁵

Die Geheimhaltungsmaßnahmen gem § 26b Abs 1 Z 3 UWG sollen angemessen und den Umständen entsprechend sein. Hier ist insbesondere auf Branchenusancen zurückzugreifen und auf die konkreten Möglichkeiten und Ressourcen der Geheimnisinhaber Bedacht zu nehmen, wodurch an KMUs vergleichsweise geringere Anforderungen gestellt werden.¹⁸⁶

Es ist zu betonen, dass eine Unternehmereigenschaft für den Geschäftsgeheimnisschutz nicht zwingend notwendig ist, weswegen auch Universitäten und nicht-kommerzielle Forschungseinrichtungen davon profitieren können, sofern die oben beschriebenen, allgemeinen Voraussetzungen gegeben sind.¹⁸⁷

3.2.2 Abwägungen im EHDS

Im Sekundärnutzungssystem des EHDS treffen die oben genannten Rechte an Daten auf den Wunsch nach Nutzung derselben. Dem europäischen Rechtssetzer ist diese Kollision bewusst und überantwortet das Treffen dieser Abwägung im Einzelfall den jeweiligen Zugangsstellen bei der Prüfung des Datenantrags.¹⁸⁸

¹⁸⁴ OGH 4 Ob 188/20f ecolex 2021, 450 (*Hofmarcher*).

¹⁸⁵ *Thiele in Wiebe/Kodek*, UWG² § 26b Rz 14.

¹⁸⁶ *Hofmarcher*, Schutzgegenstand und Inhaber Was und wen schützt das neue Gesetz?, ipCompetence 2019 H 21, 10 (14).

¹⁸⁷ *Görg in Görg*, Kommentar zum UWG (2020) § 26b UWG Rz 83.

¹⁸⁸ ErwGr 60 EHDS.

Die Ersteinschätzung überlässt der EHDS jedoch den Dateninhabern selbst. Diese müssen gem Art 52 Abs 2 EHDS spätestens bei Übermittlung des Datenantrags tätig werden und der jeweiligen Zugangsstelle die Rechte an ihren elektronischen Gesundheitsdaten mitteilen. Da zu diesem Zeitpunkt jedoch bereits eine Datengenehmigung vorliegen sollte, sei den Dateninhabern zur Vermeidung eines prozessualen Aufwandes empfohlen, Rechte an ihren Daten bereits bei der Übermittlung der Datensatzbeschreibung gem Art 60 Abs 2 EHDS zu identifizieren und die Zugangsstellen somit davon rechtzeitig in Kenntnis zu setzen. Dabei ist insbesondere zu bedenken, dass die oben beschriebenen Rechtsinstrumente keiner Eintragung in ein Register bedürfen und deren Identifizierung somit auch ad hoc geschehen kann.

Betrifft ein Datenantrag elektronische Gesundheitsdaten, an denen Rechte der Zugangsstelle gemeldet wurden, so hat diese gem Art 52 Abs 3 EHDS zu beurteilen, ob diese Rechte tatsächlich bestehen und gegebenenfalls nötige Maßnahmen zu treffen, um die Verarbeitung der Daten trotzdem zu ermöglichen. Diese Maßnahmen können technischer, organisatorischer oder rechtlicher Natur sein, wobei vertragliche Vereinbarungen und die Vorverarbeitung der zur Verfügung gestellten Daten als besonders geeignet angesehen werden.¹⁸⁹ Bei vertraglichen Vereinbarungen ist insbesondere an Vertraulichkeitsvereinbarungen, gekoppelt mit Lizenzvereinbarungen, zu denken. Somit geht auch der Geschäftsgeheimnisschutz nicht alleine durch Zugang im Rahmen der Sekundärnutzung verloren, da der Kreis der mitwissenden Personen durch die Zurverfügungstellung der Daten in der sicheren Verarbeitungsumgebung und das Verbot der Zugangsverschaffung Dritter gem Art 61 Abs 2 EHDS unter Kontrolle gehalten werden kann.

Bei der Beurteilung des rechtlichen Schutzes der elektronischen Gesundheitsdaten sollten auch freie (Werk-)Nutzungen berücksichtigt werden, wobei hierfür die Beweislast bei den Datennutzern liegt. Nach den oben getroffenen Überlegungen sind diese insbesondere bei nicht-gewinnorientierter Forschung zu überprüfen. Wie die Zugangsstellen mit den oben angesprochenen Wertungswidersprüchen in Bezug auf schlichte Datenbanken und Datenbankwerken beziehungsweise Lichtbildern und elektronischen Gesundheitsdaten im Textformat umgehen, ist abzuwarten. In letzter Konsequenz können Dateninhaber jedenfalls ihre Zustimmung zum Datenzugang geben, wobei die genauen Bedingungen

¹⁸⁹ ErwGr 62 EHDS.

hierfür scheinbar nicht zwingend von der Zugangsstelle vorgegeben sind und daher auch in einer zweiseitig, frei vereinbarten, mitunter monetären Gegenleistung liegen könnten.¹⁹⁰

Können die elektronischen Gesundheitsdaten nach Einschätzung der Zugangsstelle nicht zur Verfügung gestellt werden ohne Rechte der Dateninhaber zu verletzen, hat sie den Datenantrag gem Art 52 Abs 5 EHDS abzulehnen. Gegen eine Erledigung der Zugangsstelle steht beiden Parteien bei dargelegtem rechtlichen Interesse, das auch in der konkreten Ausgestaltung der von der Zugangsstelle getroffenen Schutzmaßnahmen liegen kann, das Rechtsmittel der Bescheidbeschwerde offen.

Die Regelungen des EHDS in Bezug auf Rechte an Daten wurde insbesondere vonseiten der Industrie mehrfach kritisiert.¹⁹¹ Konkret wurde befürchtet, dass Unternehmen den Datenantrag dafür missbrauchen könnten, um auf Geschäftsgeheimnisse ihrer Mitbewerber zuzugreifen.¹⁹² Diese Problematik wurde jedenfalls durch Beschränkung des direkten Datenantrags¹⁹³ etwas abgemildert.

Insgesamt bleibt jedoch der Befund einer radikal neuen IP Governance im EHDS.¹⁹⁴ Außerdem ist anzumerken, dass auch auf die Zugangsstellen ein nicht zu unterschätzender administrativer Aufwand zukommen wird, indem sie über die oben angeführten Rechte entscheiden müssen.

¹⁹⁰ Näheres zur Vergütung unter 3.4.

¹⁹¹ statt vieler *Bundesverband der Arzneimittel-Hersteller e.V. (BAH)*, Stellungnahme zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten (COM 2022/0140 (COD)) 20220407-EHDS for Decide (003) (europa.eu), https://www.pharmadeutschland.de/index.php?id=1&type=565&file=redakteur_filesystem/public/Stellungnahmen_und_Positionspapiere/20220728_BAH_Stellungnahme_zum_Verordnungsvorschlag_EHDS.pdf (abgefragt am 14.4.2025).

¹⁹² *Kertesz*, Collaboration in Healthcare: Implications of Data Sharing for Secondary Use in the European Union, *European Journal of Health Law* 2024, 497; zu ähnlichen Befürchtungen im Rahmenwerk des Data Acts siehe *Bruchbacher/Hinterberger*, Geschäftsgeheimnisschutz: rechtlicher Rahmen und Spannungsverhältnis zu Datenauskunfts- und Datenzugangsrechten, *GRC aktuell* 2025, 24.

¹⁹³ Näheres sogleich unter 3.3.

¹⁹⁴ *Rak*, Anonymisation, Pseudonymisation and Secure Processing Environments Relating to the Secondary Use of Electronic Health Data in the European Health Data Space (EHDS), *European Journal of Risk Regulation* 2024, 928 (935).

3.3 Vertrauenswürdige Dateninhaber

Der EHDS eröffnet neben dem herkömmlichen Verfahren der Bereitstellung elektronischer Gesundheitsdaten über die Zugangsstellen auch die Option der direkten Bereitstellung durch bestimmte Dateninhaber. Gem Art 72 EHDS ist dieser vereinfachte Vorgang für den Zugang zu Daten eines designierten vertrauenswürdigen Gesundheitsdateninhabers vorgesehen.

Erhält eine Zugangsstelle einen Datenantrag, welcher nur die Daten eines vertrauenswürdigen Dateninhabers betrifft, kann sie den Datenantrag gem Art 72 Abs 1 iVm Art 72 Abs 3 EHDS an diesen weiterleiten. Der vertrauenswürdige Dateninhaber hat den Datenantrag sodann gem Art 72 Abs 4 EHDS nach denselben Kriterien wie die Zugangsstelle zu prüfen¹⁹⁵ und eine Empfehlung auszusprechen. Dafür hat er gem Art 72 Abs 5 EHDS zwei Monate Zeit. Die Letztentscheidung bleibt, wohl auch aufgrund von Rechtsschutzgründen, bei den Zugangsstellen. Hierfür haben diese wiederum zwei Monate nach Erhalt der Einschätzung des vertrauenswürdigen Dateninhaber Zeit. An diese Einschätzung sind sie bei ihrer Entscheidungsfindung explizit nicht gebunden.

Die Vereinfachung, die durch das System des direkten Datenantrags bei den vertrauenswürdigen Dateninhabern eintreten soll,¹⁹⁶ ist im nächsten Schritt auszumachen. Gem Art 72 Abs 6 EHDS sollen die vertrauenswürdigen Dateninhaber selbst die Aufgaben der Zugangsstellen gem Art 57 Abs 1 lit a sublit i EHDS und Art 57 Abs 1 lit b EHDS übernehmen. Das beinhaltet sowohl die Datenaufbereitung inklusive Anonymisierung beziehungsweise Pseudonymisierung¹⁹⁷ als auch die Bereitstellung der elektronischen Gesundheitsdaten in einer sicheren Verarbeitungsumgebung.¹⁹⁸ Überraschend ist das Fehlen eines Verweises auf Art 52 Abs 3 EHDS. Somit bleibt die Kompetenz für das Ergreifen von Schutzmaßnahmen zugunsten von Dateninhabern, welche Rechte an Daten geltend machen,¹⁹⁹ bei den Zugangsstellen selbst.

¹⁹⁵ Näheres unter 2.1.2.

¹⁹⁶ ErwGr 76 EHDS.

¹⁹⁷ Näheres unter 2.3.1.

¹⁹⁸ Näheres unter 2.2.2.

¹⁹⁹ Näheres unter 2.2.1.

Sowohl öffentliche als auch private Institutionen können als vertrauenswürdige Dateninhaber deklariert werden, wobei dies bei Institutionen der Europäischen Union gem Art 72 Abs 7 EHDS auch einseitig geschehen kann. Von dieser Ausnahme abgesehen, liegt die Initiative hierfür bei den Institutionen selbst. Da von den vertrauenswürdigen Dateninhabern für die Erfüllung der ihnen übertragenen Aufgaben eine große Expertise zu verlangen ist, soll jedoch ein striktes Auswahlverfahren hierfür etabliert werden. Dieses liegt gem Art 72 Abs 2 EHDS grundsätzlich in den Händen der Mitgliedsstaaten, wobei der EHDS jedoch Rahmenbedingungen vorgibt. So sollen vertrauenswürdige Dateninhaber folgende Kriterien erfüllen:

1. Sie können Datennutzern durch eine sichere Verarbeitungsumgebung gem Art 73 EHDS Zugriff auf elektronische Gesundheitsdaten verschaffen
2. Sie haben die nötige Expertise, um Datenanträge zu bewerten
3. Sie garantieren auch sonst die Einhaltung der Bestimmungen des EHDS

Diese Kriterien sind von der jeweils zuständigen Zugangsstelle zu bewerten und regelmäßig zu überprüfen. Zu erwähnen ist jedoch, dass Mitgliedstaaten keine Verpflichtung trifft, einen derartigen Prozess und somit das Institut der vertrauenswürdigen Dateninhaber überhaupt einzuführen.

Die zuständige Zugangsstelle soll vertrauenswürdige Dateninhaber nach positiver Beurteilung und Designation derselben im Datensatzkatalog gem Art 77 EHDS auflisten. Hierbei handelt es sich um eine Form der Kennzeichnung der Datensatzkataloge.

Fraglich ist, welche Motivation für Institutionen besteht, sich als vertrauenswürdiger Dateninhaber zu registrieren. Die Designation als vertrauenswürdiger Dateninhaber ist keineswegs eine Voraussetzung, um Daten zur Verfügung stellen zu können und führt für Dateninhaber durch die verpflichtende Abgabe der Evaluierung und der Übernahme der Aufbereitungs- und Bereitstellungspflichten zu großem Aufwand. Vertrauenswürdigen Dateninhaber sind gem Art 74 Abs 2 EHDS auch als Verantwortliche iSv Art 4 Z 7 DSGVO für die Verarbeitung elektronischer Gesundheitsdaten zur Aufbereitung, inklusiver Pseudonymisierung beziehungsweise Anonymisierung und die Bereitstellung in der sicheren Verarbeitungsumgebung zu betrachten. Somit erhöht sich für vertrauenswürdige Dateninhaber der Grad der Verantwortung und demnach rechtliche Risiken erheblich.

Die Kontrolle der Dateninhaber über ihre elektronischen Gesundheitsdaten wird durch die Übernahme der Verpflichtungen als vertrauenswürdige Dateninhaber nicht wesentlich

gestärkt, bleibt doch sowohl der Schutz der Rechte an den Datensätzen als auch die finale Entscheidung über die Gewährung des Datenzugangs bei den Zugangsstellen.

Da die Vergütungsbestimmungen bloß Kostendeckung garantieren sollen,²⁰⁰ stellt die Möglichkeit gem Art 62 Abs 1 EHDS, den Aufwand durch die Vorschreibung von Gebühren auf den Datennutzer zu überwälzen, auch keinen großen Anreiz für Dateninhaber dar, die Rolle als vertrauenswürdige Dateninhaber zu übernehmen.

²⁰⁰ Näheres sogleich unter 3.4.

3.4 Vergütung

Gem Art 62 Abs 1 EHDS können Zugangsstellen und vertrauenswürdige Dateninhaber den Datennutzern Gebühren für die Durchführung ihrer Aufgaben im Rahmen des EHDS verrechnen. Diese Gebühren sollen verhältnismäßig zu ihren Kosten sein und den Wettbewerb nicht behindern. Sie sollen Teile der Kosten oder die kompletten Kosten für den gesamten Vorgang der Aufbereitung und Zurverfügungstellung der elektronischen Gesundheitsdaten abbilden und sollen dabei gem Art 62 Abs 3 EHDS transparent, das heißt für die Datennutzer nachvollziehbar, sein. Die verrechneten Gebühren sollen den Zugangsstellen helfen, ihre operationalen Kosten zu decken.²⁰¹

Zusätzlich können auch Dateninhaber Gebühren für ihre Aufwendungen geltend machen. Dies geschieht jedoch, mit der Ausnahme der vertrauenswürdigen Dateninhaber, nicht direkt, sondern über die Zugangsstellen. Hierfür müssen sie den Zugangsstellen gem Art 62 Abs 2 EHDS eine Schätzung der angefallenen Kosten übermitteln. Diese schreiben die Kosten den Datennutzern in einer Rechnung vor und zahlen den Dateninhabern ihren Teil aus.

Durchaus kritikwürdig ist, dass nicht klarer aus dem Verordnungstext hervorgeht, welche Kosten hierbei berücksichtigt werden können. Gem Art 62 Abs 2 EHDS können Dateninhaber zwar explizit Kosten für das Zusammenstellen und Aufbereitung der Datensätze für die Sekundärnutzung geltend machen. Der genaue Umfang geht jedoch nicht alleine aus dem Wortlaut der Bestimmung hervor. Gedeckt scheinen nach dem Wortlaut von Art 62 Abs 2 EHDS die Kosten für die konkrete Bereitstellung des angeforderten Datensatzes wie die Entfernung des Personenbezugs, soweit dies vom Dateninhaber selbst durchgeführt wird. Der Wortlaut „Schätzung dieser Kosten“ in Art 62 Abs 2 EHDS legt dabei nahe, dass Dateninhaber einen gewissen Spielraum bei der Festsetzung dieser Kosten haben. Jedoch scheinen weder die Kosten für die Primärerhebung, noch für die allgemeine Beschreibung der Datensätze für den Datensatzkatalog gem Art 60 Abs 3 EHDS von Art 62 Abs 2 EHDS umfasst zu sein.²⁰²

²⁰¹ ErwGr 70 EHDS.

²⁰² Kuss/Moers, Die Europäische und nationale Datenstrategie im Gesundheitswesen am Beispiel des European Health Data Space und des Gesundheitsdatennutzungsgesetzes: Ein Durchbruch für die Forschung? in Hoffberger-Pippan/Ladeck/Ivankovics, Digitalisierung und Recht (2024), 350.

Gem Art 62 Abs 5 EHDS soll die Zugangsstelle die Datennutzer vor Ausstellung der Datengenehmigung von den erwarteten Gebühren in Kenntnis setzen und sie von der Möglichkeit informieren, den Datenantrag zurückzuziehen. In diesem Fall ist von dem Antragssteller nur eine Gebühr für die bereits entstandenen Kosten zu entrichten.

Art 62 Abs 4 EHDS sieht weiters eine Art Verhandlung über Gebühren zwischen den Dateninhabern und Datennutzern vor, welche auch nach Ausstellung der Datengenehmigung erfolgen kann. Führt diese binnen einem Monat nach Ausstellung der Datengenehmigung zu keiner Einigung, soll die Zugangsstelle eine verhältnismäßige Gebühr für die Aufwendungen der Dateninhaber festlegen können. Prima facie widerspricht die Möglichkeit der Verhandlung nach erteilter Datengenehmigung dem bisher erläuterten System – die Zugangsstellen sollen die Gebühren gem Art 62 Abs 2 iVm Art 68 Abs 10 lit g EHDS ja gesammelt, also auch inklusive der Gebühr des Dateninhabers, in der Datengenehmigung angeben. Anscheinend soll die in der Datengenehmigung angegebene Gebühr zumindest betreffend den Teil des Dateninhabers jedoch vorerst nicht rechtsverbindlich sein, sondern nur der Information der Datennutzer dienen und auch noch danach Verhandlungen zugänglich sein. Sollten Dateninhaber oder Datennutzer auch nach zwangsweiser Festsetzung der Gebühren weiterhin nicht einverstanden sein, sollen beide Parteien gem Art 62 Abs 4 EHDS Zugang zu einem Sonderregime zur Streitbeilegung gem Art 10 Data Act (DA)²⁰³ haben. Fraglich ist, ob Dateninhaber während dieser Zeit ihre elektronischen Gesundheitsdaten zurückhalten können oder diese ungeachtet der Uneinigkeit über die Gebühren trotzdem gemäß der Datengenehmigung bereitstellen müssen. Insgesamt schafft das skizzierte Verfahren der Gebührenfestsetzung Rechtsunsicherheit für beide Parteien.

Für Forschende ist zusätzlich die Öffnungsklausel in Art 62 Abs 1 EHDS von Interesse. Diese erlaubt Mitgliedsstaaten, für Datenanträge gewisser Datennutzer reduzierte Gebühren festzulegen. Beispielsweise genannt werden Kleinstunternehmen und universitäre Forschungseinrichtungen. Diese vergleichsweise weitgehende Öffnungsklausel muss jedoch erst auf nationalstaatlicher Ebene ausgestaltet werden.

Mehr Klarheit im Bereich der Gebührenvorschreibung soll durch die Europäische Kommission gem Art 62 Abs 6 EHDS mittels Durchführungsrechtsakten geschaffen

²⁰³ Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung), ABl L 2023/2854.

werden. Diese sollen Grundsätze für die Berechnung und Struktur der Gebühren festlegen. Insgesamt ist jedoch anzumerken, dass für die Gebührenberechnung wenig konkrete Vorgaben existieren und erneut weitreichende Entscheidungsbefugnis den Zugangsstellen übertragen wird. Möglichen anderen Regelungen, wie insbesondere der Festsetzung genauerer Kriterien durch die Mitgliedsstaaten, wie in Art 6 Abs 6 DGA vorgesehen, oder einem Fixpreismodell²⁰⁴ wird somit eine Absage erteilt. Letzteres für die gesamte Europäische Union zentral zu realisieren, wäre herausfordern, da durch die Gebühren ein Ausgleich für die Kosten der Zusammenstellung und Aufbereitung der elektronischen Gesundheitsdaten erzielt werden soll. Diese unterscheiden sich jedoch je nach Datenerhebungsprozess, nationalen Strukturen und Divergenzen in Personal- und Infrastrukturkosten. Aufgrund dieser Überlegungen könnte für Datennutzer neben den primären Erwägungen zur Datenqualität und Datenmenge auch ein Anreiz entstehen, Daten aus Mitgliedsstaaten mit niedrigeren Gebühren zu beantragen.

Die Möglichkeit, über die konkreten Bereitstellungskosten hinaus eine Vergütung in der Form der Berücksichtigung des Marktwerts der Daten zu verlangen, ist im System des EHDS nicht vorgesehen und würde den Zweck des gemeinwohlorientierten Datenzugangs konterkarieren. Das deckt sich auch mit den Regelungen in Art 6 DGA, unterscheidet das System des EHDS aber von dem des DA. Gem Art 9 Abs 1 und 2 DA können Dateninhaber und Datenempfänger eine Gegenleistung für die Bereitstellung der Daten vereinbaren, welche neben den konkret anfallenden Kosten auch, im Unterschied zu DGA und EHDS, die Kosten der Primärerhebung der Daten und eine Gewinnspanne beinhalten kann.

Diese grundlegende Divergenz verdeutlicht die unterschiedliche Zielsetzung dieser Rechtsakte. Der DA sieht Daten als marktwirtschaftliches Gut und soll Rahmenbedingungen zur Förderung von Wettbewerb und Wirtschaftswachstum schaffen.²⁰⁵ Dabei konzentriert sich diese Verordnung auf Regeln für Datenübertragbarkeit, stellt im Bereich des Datenzugangs jedoch keine wahre Revolution dar.²⁰⁶ Daher können Dateninhaber nach diesem System weiter die Nutzung des grundsätzlich nicht-rivalen und

²⁰⁴ so beispielsweise im finnischen Gesundheitsdatenraum Findata: Sosiaali- ja terveystieteiden ministeriön asetus Sosiaali- ja terveystietojen tietolupaviranomaisen suorittamien maksullisuudesta, 1147/2023, <https://www.finlex.fi/fi/laki/alkup/2023/20231147> (abgefragt am 14.4.2025).

²⁰⁵ ErwGr 2 DA.

²⁰⁶ *Ivanova/Reiter*, Horizontal-LL und Data Act, ÖBl 2023, 235 (237).

nicht-exklusiven Guts Daten²⁰⁷ durch technische Maßnahmen beschränken und somit deren Wert durch künstliche Verknappung steigern. Der DGA und der EHDS rücken Daten hingegen näher an das Konzept eines Gemeinguts, mit der Zielsetzung, Datenverarbeitung zu Zwecken, „die mit der Verwendung elektronischer Gesundheitsdaten im Gesundheitswesen und im Pflegesektor verbunden sind und der Gesellschaft zugutekämen“ zu fördern.²⁰⁸ Auch das oben beschriebene Gebührenprivileg für Forschende verdeutlicht die Gemeinwohlorientierung des EHDS. Rechtlich wird diese durch die Verankerung des Anspruchs der Datennutzer auf Datenzugang gem Art 68 Abs 3 EHDS in Verbindung mit der Rechtspflicht der Dateninhaber zur Bereitstellung der elektronischen Gesundheitsdaten gem Art 60 Abs 1 EHDS realisiert. Somit stellt der EHDS auch im Bereich des Datenzugangs eine Revolution dar, insbesondere da ein Rechtsanspruch auf Datenzugang auch bezüglich elektronischer Gesundheitsdaten von Privaten besteht. Die Integration von kommerziell agierenden Unternehmen als Datennutzer in das Sekundärnutzungssystem des EHDS betrifft die tiefergreifende Frage der Notwendigkeit der Unterscheidung zwischen gewinnorientierter und nicht-gewinnorientierter Forschung in Bezug auf ihre, insbesondere datenschutzrechtliche, Privilegierung.²⁰⁹ Der Kritik über fehlende Unterscheidung im System des EHDS wird dabei die Innovationskraft und diesbezügliche Notwendigkeit der Integration kommerzieller Forschung entgegengehalten.²¹⁰

²⁰⁷ Schwamberger, Der Data Act, ecolex 2024, 367.

²⁰⁸ ErwGr 1 EHDS.

²⁰⁹ Buchner, Forschungsdaten effektiver nutzen, DuD 2022, 555 (560).

²¹⁰ Gassner, Forschung und Innovation im europäischen Gesundheitsdatenraum DuD 2022, 739 (743).

4 Zusammenfassung und Fazit

Der EHDS soll einen Paradigmenwechsel im Bereich der datengetriebenen medizinischen Forschung darstellen. Interoperable Datenformate und Zugangsstellen als Datenintermediäre sollen insbesondere im Bereich von Big Data die derzeitige Herangehensweise von Nutzungsvereinbarungen zwischen Forschungsstellen und Dateninhabern ersetzen.²¹¹ Dabei bewegt sich der EHDS im Spannungsfeld zwischen dem Verlangen nach Datenzugang der Datennutzer, Bedenken des geistigen Eigentums und kommerzieller Interessen der Dateninhaber und Bedenken des Datenschutzes der Betroffenen.

Nach erster Analyse kann festgehalten werden, dass sich Dateninhaber insbesondere mit Blick auf geistiges Eigentum und Geschäftsgeheimnisse auf den EHDS vorbereiten müssen. Ihnen bleibt es überlassen, vor allem im jährlichen Reporting über die verfügbaren Datensätze ihnen zustehende Rechte an denselben auszumachen, zu dokumentieren und daraufhin effektiv durch Information der Zugangsstelle zu schützen. Durch das Durchstoßen von technischen Schutzmaßnahmen wird die Wichtigkeit der Identifizierung rechtlicher Schutzmaßnahmen wie beispielsweise Rechte an Datenbanken zunehmen. Dabei ist festzuhalten, dass nach österreichischer Rechtslage relevante freie Werknutzungen nur für Datenverarbeitung ohne Gewinnerzielungsabsicht bestehen und bei Nichtanwendbarkeit dieser ein Lizenzvertrag zwischen Dateninhaber und Datennutzer notwendig ist. In der Notwendigkeit der proaktiven Identifizierung von Rechten an Daten ist durchaus ein Paradigmenwechsel in der Daten- bzw IP-Governance von Dateninhabern zu sehen.

Das mitunter aus dem Grundsatz der Datenminimierung ableitbare möglichst frühe Entfernen des Personenbezugs schafft durch die fehlende ausdrückliche Verantwortlichkeit hierfür Unklarheit in Hinblick auf technische Machbarkeit und dafür anwendbare Rechtsgrundlagen. Zusätzlich besteht für Dateninhaber im Bereich der Gebührenordnung noch grundlegende Unklarheiten über Höhe der festsetzbaren Gebühren und des diesbezüglichen Verfahrens. Durch die Entscheidung des europäischen Rechtsetzers, nur die konkreten Kosten für Aufbereitung und Bereitstellung der elektronischen Gesundheitsdaten refundierbar zu machen, werden elektronische Gesundheitsdaten näher

²¹¹ Denga, Nutzungsgovernance, EuZW 2023, 25 (29).

an das Konzept eines Gemeinguts gerückt,²¹² welches insbesondere auch von Unternehmen zur gewinnorientierten Forschung gebraucht werden kann. Die konkret einzuholende informierte Einwilligung der Betroffenen verliert somit an Wichtigkeit. Auch darin ist ein Paradigmenwechsel zu sehen.

Datennutzern sei daher nahegelegt, sich mit Verarbeitungsgrundlagen abseits der informierten Einwilligung zu beschäftigen und deren Anwendbarkeit auf ihre Projekte zu analysieren. Für österreichische Forschende sind hierbei insbesondere die Verarbeitungsgrundlagen des berechtigten Interesses gem Art 6 Abs 1 lit f DSGVO und die nationalen Forschungsausnahmen in § 7 Abs 1 Z 3 DSG und § 2d Abs 2 Z 1 lit b FOG von Relevanz. Durch die Sicherheitsmaßnahmen der sicheren Verarbeitungsumgebung gem Art 73 EHDS kann insbesondere die Anwendung von § 2d Abs 2 Z 1 lit b FOG leichter als bisher ermöglicht werden. Daneben besteht weiterhin das Problem der Abgrenzung zwischen anonymisierten und pseudonymisierten Daten, welches durch die zentrale Rolle dieser Unterscheidung im Sekundärnutzungssystem des EHDS nur verstärkt wird. Auch mit dieser Abgrenzung sollten sich Forschende zukünftig noch intensiver auseinandersetzen, um als Datennutzer die Möglichkeiten des EHDS in Übereinstimmung mit den Bestimmungen des Datenschutzrechts auszuschöpfen. Bei und nach erfolgter Verarbeitung sollten insbesondere Art 61 Abs 5 EHDS, welcher die Pflicht zur Meldung von Incidental Findings normiert, und Art 61 Abs 4 EHDS, welcher Rahmenbedingungen für die Publikation der Ergebnisse der Datenverarbeitung verpflichtend vorschreibt, beachtet werden. Diese Publikation hat in einer zugänglichen, Laien ansprechenden, Sprache auf der Website der Zugangsstelle und zusätzlich auch vom Datennutzer selbst zu geschehen und dient insbesondere der Transparenz der Verarbeitung und als Werbemaßnahme für den EHDS. Aus ähnlichen Gründen müssen Datennutzer bei allen Publikationen gem Art 61 Abs 4 EHDS die Quellen der elektronischen Gesundheitsdaten und den Umstand, dass diese über den EHDS zur Verfügung gestellt wurde, offenlegen.

Neben diesen Werbemaßnahmen hängt die Akzeptanz des EHDS entscheidend von Dateninhabern und Betroffenen ab. Bei Dateninhabern muss für das Gelingen des EHDS ein Umdenken bezüglich der Sichtweise von Daten als exklusives Gut einsetzen, was jedoch unter Umständen ihren wirtschaftlichen Interessen widersprechen kann. Weiters sollten datenerhebende Institutionen vermehrt ein Augenmerk auf die Datenerhebung im

²¹² *Slokenberga*, Scientific Research Regime 2.0? How the proposed EHDS Regulation may change the GDPR Research Regime, *Technology and Regulation* 2022, 135 (145).

Lichte von Sekundärnutzung legen und diese idealerweise bei der Primärerhebung mitberücksichtigen. Hierbei sind sowohl die Mitgliedsstaaten als auch einzelne datenerhebende Institutionen angehalten, dies durch gemeinsame Standards und Interoperabilität zu ermöglichen. Hierfür ist jedoch ein Sinneswandel bis auf die unterste Ebene der datenerhebenden Institutionen erforderlich, welcher schwierig zu realisieren ist, da dieser unter Umständen auch mit einer effizienten Arbeitsweise konfligiert²¹³ und keine finanziellen Anreize hierfür im System des EHDS bestehen.

Betroffene könnten sich durch die Sekundärnutzungsbestimmungen im EHDS insbesondere in ihrer informationellen Selbstbestimmung verletzt sehen. In der finalen Version der Verordnung wird ihnen zwar ein leicht realisierbares Opt-Out ermöglicht, den Mitgliedsstaaten jedoch auch die Möglichkeit gegeben, dieses für vage umschriebene Zwecke zu umgehen. Die genaue Ausgestaltung dieser Ausnahme obliegt den Mitgliedsstaaten. Daher sollten bei Nutzung dieser Öffnungsklausel geeignete Garantien wie zusätzliche Maßnahmen zur technisch sicheren Entfernung des Personenbezugs und weitreichende Informationspflichten gegenüber den Betroffenen vorgesehen werden. Andernfalls würde die Akzeptanz des EHDS auf Betroffenenseite erheblich gefährdet. Diese sind nämlich üblicherweise bereit, ihre personenbezogenen Daten zu Forschungszwecken bereitzustellen, erwarten jedoch berechtigterweise die Wahrung ihrer informationellen Selbstbestimmung und geeignete Sicherheitsanforderungen an die Datenverarbeitung im Gegenzug.²¹⁴

²¹³ *EIT Health Austria*, Der Weg zum European Health Data Space in Österreich, https://eithealth.eu/wp-content/uploads/2024/10/Der-Weg-zum-EHDS-in-Osterreich-EIT-Health-Austria-Report-v1.2_300dpi.pdf, 19 (abgefragt am 14.4.2025).

²¹⁴ *Menager et. al.*, Qualitative study to assess citizens' perception of sharing health data for secondary use and recommendations on how to engage citizens in the EHDS, <https://tehda.eu/app/uploads/2023/03/tehda-study-to-assess-citizens-perception-of-sharing-health-data-for-secondary-use.pdf>, 4 (abgefragt am 14.4.2025).

5 Abstract

Gegenstand dieser Arbeit ist die eingehende Untersuchung der Sekundärnutzungsbestimmungen der Verordnung über den Europäischen Gesundheitsdatenraum (EHDS). Der EHDS soll durch Datenzugangsansprüche, insbesondere für Zwecke der, auch kommerziellen, Forschung als erster gemeinsamer Datenraum der EU-Datenstrategie einen Paradigmenwechsel im Umgang mit elektronischen Gesundheitsdaten einläuten. Diese Arbeit beschreibt die wesentlichen Sekundärnutzungsbestimmungen aus Sicht der Datennutzer und Dateninhaber, untersucht diese kritisch und geht insbesondere auf deren Zusammenspiel mit bestehenden datenschutzrechtlichen und urheberrechtlichen Bestimmungen ein.

This thesis presents an in-depth examination of the secondary use provisions of the European Health Data Space Regulation (EHDS). The EHDS intends to bring on a paradigm shift in the handling of electronic health data as the first common data space of the EU Data Strategy. This is to be achieved through right to data access, in particular for the purpose of research, including commercial research. This thesis critically examines the most important secondary use provisions from the perspective of data users and data holders and covers in particular their interaction with data protection and copyright provisions.

6 Literaturverzeichnis

Monografien, Sammelbände, Kommentare:

Albers/Veit in Wolff/Brink/von Ungern-Sternberg, BeckOK Datenschutzrecht⁵¹ Art 6 DS-GVO (Stand 1.2.2025, beck-online.beck.de).

Baumann/Krahn/Lauber-Rönsberg, Forschungsdatenmanagement und Recht (2021).

Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl, Datenschutzgesetz (2018).

Ciresa in Ciresa, Österreichisches Urheberrecht (20. Lfg 2018) § 8 UrhG.

Ciresa in Ciresa, Österreichisches Urheberrecht (24. Lfg 2024) § 42 UrhG.

Ciresa, Praxishandbuch Urheberrecht³ (2022).

Dokalik in Dokalik/Zemann, Urheberrecht⁸ Art 7 Datenbanken-RL.

Feiler/Forgó, EU-DSGVO² (2022).

Frenzel in Paal/Pauly, DS-GVO BDSG³ (2021) Art 6 DSGVO.

Gabauer, Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken (2019).

Görg in Görg, Kommentar zum UWG (2020) § 26b UWG.

Haidinger in Knyrim, DatKomm Art 21 DSGVO (Stand 1.12.2022, rdb.at).

Haimberger, Datenschutz in der medizinischen und pharmazeutischen Forschung (2021).

Hödl in Knyrim, DatKomm Art 4 DSGVO (Stand 1.12.2018, rdb.at).

Holzner in Rummel/Lukas, ABGB⁴ (2024) § 285.

Horeth, Intellectual Property in Innovationskooperationen (2021).

Hötzendorfer/Tschohl/Kastelitz in Knyrim, DatKomm Art 5 DSGVO (Stand 7.5.2020, rdb.at).

Humer, Schutz für KI-Trainingsdaten sowie Rohdaten, ecolex 2024, 467.

Jahnel, Kommentar zur Datenschutz-Grundverordnung (2021).

Knyrim/Urban, DGA, DMA, DSA, DA, AI-Act, EHDS - ein Überblick über die europäische Datenstrategie (Teil I), *Dako* 2023, 55.

Löffler in *Knyrim*, *DatKomm* Art 89 DSGVO (Stand 1.12.2023, *rdb.at*).

Öhlinger/Potacs, EU-Recht und staatliches Recht (2020).

Pachinger, Datenschutz-Verträge³ (2024).

Schumacher in *Handig/Hofmarcher/Kucsko*, *urheber.recht*³ (2023) § 6 UrhG.

Thiele in *Wiebe/Kodek*, *UWG*² (2024) § 26b.

Woller in *Handig/Hofmarcher/Kucsko*, *urheber.recht*³ (2023) § 76c UrhG.

Woller in *Handig/Hofmarcher/Kucsko*, *urheber.recht*³ (2023) § 76d UrhG.

Zemann in *Dokalik/Zemann*, *Urheberrecht*⁸ (2022) § 76d UrhG.

Zemann in *Handig/Hofmarcher/Kucsko*, *urheber.recht*³ § 42 UrhG Rz 24.

Zinober/Bogensberger, *Praxishandbuch Know-how und Geschäftsgeheimnisse* (2020).

Beiträge in Zeitschriften:

Afra, An Assessment on Innovator's Ability for Consent-Free Health Data Reuse, In the Context of the GDPR and EHDS: The Netherlands Case Study, *European Journal of Health Law* 2024, 475.

Alon, KI in der Gesundheitstechnologie: Die Datenschutz-Challenge, *GRCaktuell* 2023, 93.

Becker/Chokoshvili/Dove, Legal bases for effective secondary use of health and genetic data in the EU: time for new legislative solutions to better harmonize data for cross-border sharing?, *International Data Privacy Law* 2024, 6.

Böning, EHDS: Ein ambitioniertes Projekt mit Folgefragen, *ZD-Aktuell* 2024, 01695.

Bruchbacher/Hinterberger, Geschäftsgeheimnisschutz: rechtlicher Rahmen und Spannungsverhältnis zu Datenauskunfts- und Datenzugangsrechten, GRC aktuell 2025, 24.

Buchholtz/Schmalhorst/Brauneck, Der Gesetzgeber im Spannungsfeld zwischen Patientensouveränität und Forschungsinteressen – eine Bewertung der neuesten Gesetzgebungsaktivitäten auf EU-Ebene und nationaler Ebene, MedR 2024, 471.

Buchner, Forschungsdaten effektiver nutzen, DuD 2022, 555.

Burghoff, Praxisgerechter Umgang mit der Verfremdung personenbezogener Daten, ZD 2023, 658

Cimina, The Proposal for a European Health Data Space: between pursued objectives and data protection challenges, ERA Forum 2023, 343.

Conrad/Folkerts, Anonyme Daten unter der DSGVO - Risiko statt Vorteil?, KuR 2023, 89.

Denga, Die Nutzungsgovernance im European Health Data Space als Problem eines Immaterialgütermarkts, EuZW 2023, 25.

Detting, Was sind Daten in der Arzneimittelentwicklung und im neuen Datennutzungsrecht (Data Act und European Health Data Space)?, PharmR 2024, 473.

Dürager, Sind Daten ein schutzfähiges Gut?, ÖBl 2018, 260.

Fiske/Degelsegger-Márquez/Marsteurer/Prainsack, Value-creation in the health data domain: a typology of what health data help us do, BioSocieties 2022, 473.

Forgó, Der European Health Data Space im Kontext der MMR, MMR 2023, 3.

Fuchs, Anonymisierende Wirkung der Verschlüsselung, Dako 2019, 55.

Gassner, Forschung und Innovation im europäischen Gesundheitsdatenraum DuD 2022, 739.

Graf/van Hövell/Stoppe, Künstliche Intelligenz in der Medizin. Datenschutz und Haftungsfragen in der Schnittstelle zwischen KI-VO und MDR, PharmR 2025, 77.

Hacker, A Legal Framework for AI Training Data - From First Principles to the Artificial Intelligence Act, Law, Innovation and Technology 2020, 257.

- Hacker*, Immaterialgüterrechtlicher Schutz von KI-Trainingsdaten, GRUR 2020, 1025.
- Heinzke*, Ein neues Datenrecht für die EU: Digitaler Wandel zum Wohle aller?, BB 2022 H 18, 1.
- Herda*, Die Verwendung von Patientenbildern durch die Krankenanstalt: Zustimmungserfordernis für Patienten?, RdM 2024, 137.
- Hermus et al.*, Opt-In versus opt-out for the secondary use of routinely recorded health data: A randomized controlled trial, European Journal of Internal Medicine 2025, 100.
- Hofmarcher*, Schutzgegenstand und Inhaber Was und wen schützt das neue Gesetz?, ipCompetence 2019 H 21, 10.
- Hornung/Wagner*, Anonymisierung als datenschutzrelevante Verarbeitung?, ZD 2020, 223.
- Ivanova/Reiter*, Horizontal-LL und Data Act, ÖBl 2023, 235.
- Jäger/Meier/Möhring/Ferrolì/Nida-Rümelin/Peters*, Von der Sackgasse der Anonymisierung zu Lösungsansätzen für den Datenschutz der Zukunft, ZD 2024, 490.
- Kertesz*, Collaboration in Healthcare: Implications of Data Sharing for Secondary Use in the European Union, European Journal of Health Law 2024, 497.
- Kornmeier/Baranowski*, Das Eigentum an Daten - Zugang statt Zuordnung, BB 2019, 1219.
- Kotschy*, Registerforschung nach der Novelle 2021 zum FOG, zfhr 2022, 139.
- Lachmayer/Souhrada-Kirchmayer*, Datenschutzrecht in der wissenschaftlichen Forschung, zfhr 2018, 153.
- Löffler/Kastelitz*, Was ist der Europäische Raum für Gesundheitsdaten (EHDS)?, Dako 2023, 79.
- Marcelli et al.*, The European health data space: Too big to succeed?, Health policy 2023, 104861.
- Mayrhofer/Leitner/Stadlbauer*, Datenschutzrechtliche Aspekte der Nutzung von Krankenhausinformationssystemen für Forschungszwecke, ZTR 2022, 207.

- Mikl et al.*, A national evaluation analysis and expert interview study of real-world data sources for research and healthcare decision-making, *Scientific Reports* 2024, 9751.
- Quinn/Elyne/Yao*, Will the GDPR Restrain Health Data Access Bodies Under the European Health Data Space (EHDS)?, *Computer Law & Security Review* 54, 105993.
- Raji*, Datenräume in der Europäischen Datenstrategie am Beispiel des European Health Data Space, *ZD* 2023, 3.
- Rak*, Anonymisation, Pseudonymisation and Secure Processing Environments Relating to the Secondary Use of Electronic Health Data in the European Health Data Space (EHDS), *European Journal of Risk Regulation* 2024, 928.
- Roos/Maddaloni*, Regulierter Datenaustausch zur Gesundheitsforschung, *RDi* 2023, 225.
- Roßnagel/Geminn*, Vertrauen in Anonymisierung, *ZD* 2021, 487.
- Schneeberger*, KI-Assistenzsysteme in der Medizin, *RdM* 2021, 139.
- Schwamberger*, Der Data Act, *ecolex* 2024, 367.
- Shabani/Yilmaz*, Lawfulness in secondary use of health data, *Technology and Regulation* 2022, 128.
- Slokenberga*, Scientific Research Regime 2.0? How the proposed EHDS Regulation may change the GDPR Research Regime, *Technology and Regulation* 2022, 135.
- Sokol*, European Health Data Space, Use of Data and Data Subjects' Control over Their Own Health Data: Can an Opt-Out Restore the Balance?, *European Journal of Health Law* 2024, 365.
- Specht-Riemenschneider/Heineking*, Datenverarbeitung in sicheren Verarbeitungsumgebungen am Beispiel von MRT-Gehirnscans, *DuD* 2024, 110.
- Staunton et al.*, Ethical and social reflections on the proposed European Health Data Space, *European Journal of Human Genetics* 2024, 498.
- Stürmer*, Löschen durch Anonymisieren?, *ZD* 2020, 626.
- Terzis*, Compromises and Asymmetries in the European Health Data Space, *European Journal of Health Law* 2023, 345.

Thüsing/Rombey, Anonymisierung an sich ist keine rechtfertigungsbedürftige Datenverarbeitung, ZD 2021, 548.

Tschammler/Uecker, Verordnungsentwurf zur Schaffung eines Europäischen Gesundheitsdatenraums – erster Überblick mit Fokus auf die Nutzung von Gesundheitsdaten für Forschungs- und Entwicklungsvorhaben, ZD-Aktuell 2022, 01265.

Veil, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, NVwZ 2018, 686.

Wolf et al., Managing Incidental Findings in Human Subjects Research: Analysis and Recommendations, Journal of Law, Medicine & Ethics 2008, 219.

Beiträge in Sammelbänden:

Gabauer, Nationale Regelungsspielräume im Zusammenhang mit Datenverarbeitungen zu wissenschaftlichen Forschungszwecken in *Jahnel/Krempelmeier/Schmid*, Wissenschaft und Datenschutz (2024).

Gabauer, Sekundärnutzung von elektronischen Gesundheitsdaten auf Grundlage des Entwurfs einer Verordnung über den Europäischen Raum für Gesundheitsdaten (EHDS) in *Janisch/Krempelmeier/Mader/Staudegger/Thiele*, Am Glasfaserpuls – Festschrift für Dietmar Jahnel (2025).

Kogut-Czarkowska/Shabani, Federated networks and secondary uses of health data in *Slokenberga/Ó Cathaoir/Shabani*, The European Health Data Space (2025).

Kotschy, Die Zulässigkeitsvoraussetzungen für Forschungsdatenverarbeitungen nach dem FOG – eine kritische Analyse in *Jahnel*, Datenschutzrecht (2020).

Kuss/Moers, Die Europäische und nationale Datenstrategie im Gesundheitswesen am Beispiel des European Health Data Space und des Gesundheitsdatennutzungsgesetzes: Ein Durchbruch für die Forschung? in *Hoffberger-Pippan/Ladeck/Ivankovics*, Digitalisierung und Recht (2024).

Nägele/Apel, Immaterialgüterrecht in *Kaulartz/Braegelmann*, Rechtshandbuch Artificial Intelligence und Machine Learning (2020).

Pinggera/Stadler, Von verantwortungsvollen Verantwortlichen in *Brameshuber/Blasch*, Jahrbuch Sozialversicherungsrecht (2022).

Raji, 120.5 European Health Data Space in *Taegeer/Pohle*, Computerrechts-Handbuch (Werkstand: 39. EL April 2024).

Straub, Datenhoheit und Datenschutz aus Nutzer-, Verbraucher- und Patientenperspektive in *Rohde/Bürger/Peneva/Mock*, Datenwirtschaft und Datentechnologie (2022).

Thiele, Urheberrechtliche Fragen der Weitergabe und Veröffentlichung von personenbezogenen Daten in der Forschung in *Jahnel/Krempelmeier/Schmid*, Wissenschaft und Datenschutz (2024).

Wehde/Brandenberg, Teil 16.8 Sekundärnutzung von Gesundheitsdaten in *Hoeren/Sieber/Holznagel*, Handbuch Multimedia-Recht (Werkstand: 61. EL März 2024).

Online Dokumente:

Artikel-29-Datenschutzgruppe, WP 216 Stellungnahme 5/2014 zu Anonymisierungstechniken, angenommen am 10. 4. 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf (abgefragt am 14.4.2025).

Artikel-29-Datenschutzgruppe, Stellungnahme zum Begriff des berechtigten Interesses (WP217), https://dsb.gv.at/sites/site0344/media/downloads/wp251rev01_de.pdf (abgefragt am 14.4.2025).

Austrian Micro Data Center, Safe Center, <https://www.statistik.at/services/tools/services/amdc-mikrodaten-fuer-die-wissenschaft/safe-center> (abgefragt am 14.4.2025).

Austrian Micro Data Center, Vertragsmuster für die Nutzung des AMDC, https://www.statistik.at/fileadmin/pages/1805/Vertragsmuster_AMDC.pdf (abgefragt am 14.4.2025).

Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz,
Presseaussendung betreffend EHDS-Umsetzung in Österreich
https://www.ots.at/presseaussendung/OTS_20240313_OT0157/rauch-europaeischer-gesundheitsdatenraum-ermoeeglicht-verbesserungen-fuer-patientinnen-und-forschung
(abgefragt am 14.4.2025).

Bundesregierung, Regierungsprogramm Stocker I,
https://www.dievolkspartei.at/Download/Regierungsprogramm_2025.pdf (abgefragt
am 14.4.2025).

Bundesverband der Arzneimittel-Hersteller e.V. (BAH), Stellungnahme zum Vorschlag für
eine Verordnung des Europäischen Parlaments und des Rates über den europäischen
Raum für Gesundheitsdaten (COM 2022/0140 (COD)) 20220407-EHDS for Decide
(003) (europa.eu),
https://www.pharmadeutschland.de/index.php?id=1&type=565&file=redakteur_filesys-tem/public/Stellungnahmen_und_Positionspapiere/20220728_BAH_Stellungnahme_zum_Verordnungsvorschlag_EHDS.pdf (abgefragt am 14.4.2025).

EDSA, Guidelines 01/2025 on Pseudonymisation (Adopted on 16 January 2025),
https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf (abgefragt am 14.4.2025).

EDSA/EDSB, Gemeinsame Stellungnahme 3/2022 des EDSA und des EDSB zum
Vorschlag für eine Verordnung über den europäischen Raum für Gesundheitsdaten,
https://www.edpb.europa.eu/system/files/2023-04/edpb_edps_jointopinion_202203_europeanhealthdataspace_de.pdf (abgefragt am
14.4.2025).

EIT Health Austria, Der Weg zum European Health Data Space in Österreich,
https://eithealth.eu/wp-content/uploads/2024/10/Der-Weg-zum-EHDS-in-Osterreich-EIT-Health-Austria-Report-v1.2_300dpi.pdf (abgefragt am 14.4.2025).

Europäische Kommission, Europäische Datenstrategie. Link:
https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de.

Fåhraeus/Reichel/Slokenberga, The European Health Data Space: Challenges and Opportunities, <https://uu.diva-portal.org/smash/get/diva2:1845108/FULLTEXT01.pdf> (abgefragt am 14.4.2025).

HealthData@EU Pilot, D7.1, https://ehds2pilot.eu/wp-content/uploads/2024/04/HealthData@EU-Pilot-Deliverable-7.1_FIN.docx-1-1.pdf (abgefragt am 14.4.2025).

Menager et. al., Qualitative study to assess citizens' perception of sharing health data for secondary use and recommendations on how to engage citizens in the EHDS, <https://tehdas.eu/app/uploads/2023/03/tehdas-study-to-assess-citizens-perception-of-sharing-health-data-for-secondary-use.pdf> (abgefragt am 14.4.2025).

Plattform Registerforschung, <https://www.registerforschung.at> (abgefragt am 14.4.2025).

Towards European Health Data Space, Description of steps in accessing individual-level data for national and EU researchers in a selection of centralised systems and decentralised systems, <https://tehdas.eu/app/uploads/2022/04/tehdas-report-description-of-steps-in-accessing-individual-level-data-for-national-and-eu-researchers-in-a-selection-of-centralised-systems-and-decentralised-systems.pdf> (abgefragt am 14.4.2025).

von Kalle, Digitalisierung für Patient:innen denken: Vom Recht auf Gefundenwerden, https://e-health-com.de/fileadmin/user_upload/dateien/Downloads/Vision_Zero_2024_Recht_auf_Gefundenwerden.pdf (abgefragt am 14.4.2025).

7 Judikaturverzeichnis

EuGH 7.3.2024, C-604/22, *IAB Europe*, ECLI:EU:C:2024:214.

EuGH 9.11.2023, C-319/22, *Scania*, ECLI:EU:T:2022:48.

EuGH 11.12.2019, C-708/18, *Asociația de Proprietari bloc M5A-ScaraA*,
ECLI:EU:C:2019:1064.

EuGH 5.6.2018, C-210/16, *Wirtschaftsakademie Schleswig-Holstein*,
ECLI:EU:C:2018:388.

EuGH 19.10.2016, C-582/14, *Breyer*, ECLI:EU:C:2016:779.

EuGH 13.5.2014, C-131/12, *Google Spain*, ECLI:EU:C:2014:317.

EuGH 1.3.2012, C-604/10, *Football Dataco v Yahoo*, ECLI:EU:C:2012:115.

EuGH 24.11.2011, C-468/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)*, ECLI:EU:C:2011:777.

EuGH 9.11.2004, C-444/02, *Fixtures Marketing*, ECLI:EU:C:2004:697.

EuG 26.4.2023, T-557/20, *SRB/EDS*, ECLI:EU:T:2023:219.

OGH 4 Ob 188/20f ecolex 2021, 450 (*Hofmarcher*).

OGH 27.11.2019, 6 Ob 150/19f.

OGH 4 Ob 206/14v jusIT 2015, 184 (*Stauddegger*) = ecolex 2015, 798 (*Tonninger*).

OGH 4 Ob 25/04m ecolex 2004, 722 (*Beck*).

OGH 4 Ob 58/04i MR 2004, 331 (*Walter*).

OGH 9. 11. 1999, 4 Ob 282/99w.

DSB 26.6.2020, 2020-0.349.984.

DSB 7.6.2018, DSB-D202.207/0001-DSB./2018