Das Land Steiermark

IDE@S Innovative Data Environment @ Styria

# Datenschutzrechtliche Roadmap für die Entwicklung einer kollaborativen Dateninfrastruktur

*Gutachten*

*vorgelegt von*

*Mag. iur. Dr. iur. Nikolaus Forgó*

*Universitätsprofessor an der Universität Wien*

*und*

*Mag. iur. Žiga Škorjanc*

*Universitätsassistent an der Universität Wien*

*am*

*14.7.2021*

# Inhaltsverzeichnis

## 1. Sachverhalt und Auftrag[1]

Die Nachfrage an Dateninfrastrukturen, Datenzugängen, einem entsprechenden Regelwerk sowie neuen innovativen Dienstleistungen und Supportmöglichkeiten steigt sowohl in der **Forschung** als auch in der **Industrie**.

Im Projekt Innovative Data Environment @ Styria („**IDE@S**“) soll in einem Konsortium bestehend aus der Technischen Universität Graz, FH JOANNEUM, der Medizinischen Universität Graz und der Karl-Franzens-Universität Graz ein Konzept für eine umfassende und nachhaltige Dateninfrastruktur entwickelt werden.

Durch das Projekt soll der Grundstein für die langfristige Entwicklung einer anschlussfähigen Infrastruktur im Sinne eines **Referenzmodells für ein kollaboratives Daten-, Informations- und Wissensmanagement** im regionalen und europäischen Kontext („RegioData-Referenzmodell“) gelegt werden.

Damit die Forschung und die Industrie von einer solchen Infrastruktur profitieren können, muss eine vertrauenswürdige Umgebung („*trusted environment*“) geschaffen werden, welche Forschung und Entwicklung ermöglicht sowie Kollaboration zwischen verschiedenen Stakeholdern fördert. Den rechtlichen Rahmen für eine solche vertrauenswürdige Umgebung bietet (primär) die Datenschutz-Grundverordnung („**DSGVO**“), die seit 25. Mai 2018 anwendbar ist.

Vor diesem Hintergrund haben die Verfasser ein rechtswissenschaftliches Gutachten zu datenschutzrechtlichen Fragen des zu entwickelnden RegioData-Referenzmodells erstellt. Das Ziel dieses Gutachtens ist die Erstellung einer **datenschutzrechtlichen Roadmap** als Grundlage der Entwicklung der kollaborativen Dateninfrastruktur laut Projektplan.

Das gegenständliche Gutachten wurde im Rahmen des Projekts IDE@S von der Medizinischen Universität Graz, Auenbruggerplatz 2, 8036 Graz, unter Projektleitung von Herrn Univ.-Prof. Dr. Zatloukal, in Auftrag gegeben („Auftraggeberin“). Das Projekt IDE@S wird vom Land Steiermark unter der Geschäftszahl GZ: ABT08-24920 gefördert.[2]

## 2. Fragestellung

Im Rahmen des gegenständlichen Gutachtens werden auftragsgemäß unter anderem folgende Fragestellungen untersucht:

[1] Ausschließlich zum Zweck der besseren Lesbarkeit wird in der vorliegenden Stellungnahme auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen sind geschlechtsneutral zu verstehen.
[2] https://www.forschungsdaten.info/fdm-im-deutschsprachigen-raum/oesterreich/projekte/ides/ (zuletzt abgerufen am 28.10.2021).

a) Daten und ihre Binnenunterscheidung in Bezug auf kollaborative Daten-, Informations- und Wissensmanagementinfrastrukturen (personenbezogen/nicht personenbezogen; öffentlich/geheim; Daten vs. Information vs. Datenbank vs. Programm etc.);

b) Grundzüge der privat- und datenschutzrechtlichen Einordnung der im Projekt anfallenden bzw. zu entwickelnden Daten-, Informations- und Wissensmanagementinfrastrukturen, insb. in datenschutz-, datensicherheits- und immaterialgüterrechtlicher Hinsicht;

c) Daraus zu entwickelnde Rechtspositionen an Daten (insb. Datenschutz, Dateneigentum, Betriebs- und Geschäftsgeheimnis; Urheberrechtliche Positionen) im Projektverlauf;

d) Handlungsoptionen und Handlungsempfehlungen bei der weiteren Entwicklung des Referenzmodells.

Die Verfasser haben die Fragestellung im Rahmen von Telefonkonferenzen am 7.4.2021 und am 9.7.2021 mit der Auftraggeberin erörtert und gemeinsam konkretisiert.

## 3. Zusammenfassung der Ergebnisse

3.1 **Personenbezogene Daten** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Die betroffene Person muss daher für den Verantwortlichen mit einem vertretbaren Aufwand und rechtlich zulässigen Mitteln zumindest ermittelbar sein. Davon zu unterscheiden sind **nicht-personenbezogene Daten**. Das sind Daten, die sich ursprünglich nicht auf eine identifizierte oder identifizierbare natürliche Person bezogen haben, und Daten, die ursprünglich personenbezogene Daten waren, später jedoch anonymisiert wurden (siehe Punkt 4.1.2.1).

3.2 Sind personenbezogene und nicht-personenbezogene Daten in einem **gemischten Datensatz** untrennbar miteinander verbunden, gilt die DSGVO für den gesamten Datensatz, und zwar auch dann, wenn die personenbezogenen Daten nur einen kleinen Teil des Datensatzes ausmachen (siehe Punkt 4.1.2.1).

3.3 Die Verarbeitung **anonymer Daten** unterliegt nicht der DSGVO. Es muss allerdings bei der Entfernung des Personenbezugs sichergestellt werden, dass weder der Verantwortliche selbst noch ein Dritter ohne unverhältnismäßigen Aufwand einen Personenbezug wiederherstellen kann (siehe Punkt 4.1.2.4). Sobald der Forschungszweck ohne die Verarbeitung personenbezogener Daten erreicht werden kann, ist die Anonymisierung die bevorzugte Lösung (siehe Punkt 4.2.5). Anders als Anonymisierung stellen Verschlüsselung und Pseudonymisierung lediglich Datensicherheitsmaßnahmen dar, die die Anwendung der DSGVO nicht entfallen lassen.

3.4 Nicht-personenbezogene Daten werden nicht per se geschützt. **Lediglich die auf den Rohdaten aufbauenden weiterentwickelten Daten sind sondergesetzlich geschützt**. Hingegen besteht für (Roh-)Daten, die nicht oder nicht ausreichend derart bearbeitet wurden, dass sie den Schutz des geistigen Eigentums erreichen oder als Geschäftsgeheimnis geschützt werden, kein gesetzlicher Schutz (siehe Punkt 4.1.3 und Punkt 4.4.2). Dies hindert den, der die Daten generiert und/oder faktisch beherrscht, nicht daran, durch vertragliche Instrumente den Umgang mit Daten zu gestalten. Derartige Vereinbarungen wirken jedoch nur zwischen den Vertragsparteien und nicht gegenüber Dritten.

3.5 Die **Verarbeitung personenbezogener Daten** ist nur rechtmäßig, wenn „*mindestens*“ ein gesetzlicher Erlaubnistatbestand erfüllt ist oder die betroffene Person eingewilligt hat (*Verbot mit Erlaubnisvorbehalt*; siehe Punkt 4.2.1).

3.6 Da die **gesetzlichen Erlaubnistatbestände** wie Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke grundsätzlich auch im Falle einer Verweigerung oder eines Widerrufs der Einwilligung greifen, sind diese vorab zu prüfen (siehe Punkt 4.2.2). Stützung der Verarbeitung auf die gesetzlichen Erlaubnistatbestände des Forschungsorganisationsgesetzes („FOG“) ist allerdings de lege lata mit erheblichen Rechtsunsicherheiten behaftet (siehe Punkt 4.2.5), die de lege ferenda weiter zunehmen werden, weil diverse Initiativen auf europäischer wie auf nationaler Ebene eine Änderung des Rechtszustands anstreben (allerdings mit divergierenden Zielen).

3.7 Die Verarbeitung kann auch auf eine freiwillige, informierte **Einwilligung** der betroffenen Person gestützt werden. Bei besonderen Kategorien personenbezogener Daten muss die Einwilligung ausdrücklich erfolgen (siehe Punkt 4.2.3). Kann bei wissenschaftlicher Forschung der Zweck der Verarbeitung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden, darf die Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung eingeholt werden („Bereichseinwilligung"; siehe Punkt 4.2.5).

3.8 Die **Weiterverarbeitung** personenbezogener Daten im Rahmen der wissenschaftlichen Forschung gilt nicht als unvereinbar mit den ursprünglichen Zwecken der Verarbeitung, daher bedarf es keine weitere Rechtsgrundlage (siehe Punkt 4.2.6).

3.9 Werden bei **kollaborativer Arbeit mit personenbezogenen (Forschungs-)Daten** diese von Verantwortlichen an einen Dritten weitergegeben werden, so kann dieser Auftragsverarbeiter, ein selbständiger Verantwortlicher oder ein gemeinsam Verantwortlicher sein (siehe Punkt 4.3.2).

3.10 Bei gemeinsamer Datenverarbeitung und bei Outsourcing an Auftragsverarbeiter ist verpflichtend eine **Vereinbarung** zwischen den Beteiligten abzuschließen (siehe Punkt 4.3.3 und 4.3.4). Bei Data Sharing zwischen selbständigen Verantwortlichen ist Abschluss eines „*Data Sharing Agreements*" zwar nicht gesetzlich vorgeschrieben, stellt allerdings eine gute Praxis dar und wird bei regelmäßigem bzw systematischem Datenaustausch empfohlen (siehe Punkt 4.3.5).

3.11 Es besteht derzeit weder auf nationaler noch auf Unionsebene eine umfassende Regelung für die **Governance von nicht-personenbezogenen Daten** (siehe Punkt 4.4.1).

3.12 Des Weiteren besteht auch kein zivilrechtliches Schutzinstrument in Form eines „Dateneigentums" an **Rohdaten**, daher sollte Nutzung nicht-personenbezogener Daten vertraglich geregelt werden („***Datennutzungsvereinbarungen***"; siehe Punkt 4.4.4).

3.13 Bei der Veröffentlichung von (Forschungs-)Daten als **Open Data** sind datenschutzrechtliche Anforderungen sowie allfällige Rechte Dritter an geistigem Eigentum und Geheimhaltungsverpflichtungen zu beachten. Für die Erteilung der Nutzungsrechte sollten offene Standardlizenzen verwendet werden. (siehe Punkt 4.4.5).

# 4. Rechtliche Würdigung

## 4.1. Daten und ihre Binnenunterscheidung in Bezug auf kollaborative Daten-, Informations- und Wissensmanagementinfrastrukturen

### 4.1.1. Einleitung

Die Europäische Kommission widmet sich dem Phänomen „Daten" in der Europäische Datenstrategie. Diese stehen im Mittelpunkt des digitalen Wandels. Der Zugang zu ständig wachsenden Datenmengen und die Fähigkeit, diese zu nutzen, wurden – zurecht – als der Schlüssel zu Innovation und Wachstum identifiziert. Die Schaffung eines Binnenmarkts für Daten sollte gewährleisten, dass die Daten innerhalb der EU und branchenübergreifend zum Nutzen von Unternehmen, Forschern und öffentlichen Verwaltungen weitergegeben und verwendet werden können.[3]

Im Daten- und Wissensmanagement sind Daten das **Fundament der Wissenspyramide**. Diese ist ein Konzept zur Darstellung der Entstehung von Wissen. Einfache Zeichen stellen die Basis und Grundvoraussetzung der Wissensgewinnung und werden durch bestimmte Syntaxregeln zu einer Aussage angeordnet. Dieser Aussage wird eine gewisse Bedeutung (Semantik) mittels Interpretation zugeordnet, wodurch Daten zu Informationen werden. In einem letzten Schritt wird aus Information Wissen gewonnen, indem die Information mit Erfahrung verknüpft wird. Wissen entsteht also dann, wenn mehrere Informationen miteinander verknüpft werden.[4]

Des Weiteren sind Daten **der zentrale Anknüpfungspunkt aller rechtlichen Befassung mit der Digitalisierung**. Allerdings ist der Begriff des Datums selbst unbestimmt und nur punktuell in einigen Rechtsakten definiert sowie der rechtliche Schutz von Daten wenig systematisiert.[5]

Seit 2014 hat die Europäische Kommission eine Reihe von Maßnahmen ergriffen, um den Weg zu einer datenagilen Wirtschaft zu ebnen.[6] Neben der DSGVO wurden die Free-Flow-of-Data Verordnung[7], die Open Data und PSI Richtlinie[8] und der Rechtsakt zur Cybersicherheit erlassen[9]. Das Daten(schutz)- und

[3] *EK*, Eine europäische Datenstrategie, Mitteilung COM(2020) 66 final, 1ff, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0066&from=DE und https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de (beides zuletzt abgerufen am 27.4.2021).
[4] *Rungg/Buchroithner*, Data Ownership in Binder Grösswang, Digital Law (2. Aufl, 2020), 140ff mwN.
[5] *Forgó*, Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen in Forgó/Zöchling-Jud, Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter, 20. ÖJT Band II/1, 351ff.
[6] *EK*, Eine europäische Datenstrategie, Mitteilung COM(2020) 66 final, 4f.
[7] VO (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, ABl. L 303 vom 28.11.2018, S. 59–68.
[8] RL (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors, ABl. L 172 vom 26.6.2019, S. 56–83.
[9] VO (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), ABl. L 151 vom 7.6.2019, S. 15–69.

Informationssicherheitsrecht[10] bilden gemeinsam mit den Rechten des geistigen Eigentums und dem Schutz des vertraulichen Know-hows und Geschäftsinformationen *de lege lata* den **Rechtsrahmen** für ein kollaboratives Daten-, Informations- und Wissensmanagement. De lege ferenda sind weitere Rechtsakte geplant, die eine grundrechtskonform operierende Datenwirtschaft weiter befördern sollen. Zu nennen sind hier insbesondere der geplante Data Governance Act[11], die geplante Verordnung zur Regulierung Künstlicher Intelligenz[12] und, als Soft-Law-Instrument, die European Cloud Initiative.[13]

In der Folge wird einleitend untersucht, wie die im Projekt anfallenden bzw. zu entwickelnden Daten-, Informations- und Wissensmanagementinfrastrukturen rechtlich einzuordnen sind und welche Rechtspositionen daran im Laufe des Projekts entstehen können (siehe auch Punkt 4.4 unten).

### 4.1.2. Personenbezogene und nicht-personenbezogene Daten

Die digitale Transformation führt dazu, dass jeder Einzelne immer größere Mengen personenbezogener Daten erzeugt. Zudem werden immer mehr nicht-personenbezogene industrielle und öffentliche Daten generiert, die in Verbindung mit den technologischen Veränderungen bei der Speicherung und Verarbeitung der Daten eine potenzielle Quelle für Wachstum und Innovation darstellen.[14]

#### *4.1.2.1. Begriffe „personenbezogene Daten" und „nicht-personenbezogene Daten"*

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

[10] Siehe auch ePrivacy-RL (RL 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), idF Berichtigung, ABl. L 162 vom 23.6.2017, S. 56 [2009/136/EG]) und NIS-RL (RL (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, idF Berichtigung, ABl. L 033 vom 7.2.2018, S. 5 [2016/1148]).

[11] Proposal for a Regulation on European data governance (Data Governance Act), COM/2020/767 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767.

[12] Proposal for a Regulation laying down harmonised rules on artificial intelligence, COM(2021) 206 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELLAR%3Ae0649735-a372-11eb-9585-01aa75ed71a1#.

[13] https://ec.europa.eu/digital-single-market/en/european-cloud-initiative.

[14] *EK*, Eine europäische Datenstrategie, Mitteilung COM(2020) 66 final, 1.

personenbezogener Daten ist beabsichtigt und im Vergleich zur DSRL[15] im Wesentlichen unverändert geblieben.[16]

„Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern."[17] „Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind."[18]

Es ist daher darauf abzustellen, ob mit einem vertretbaren Aufwand und rechtlich zulässigen Mitteln eine Identifizierung möglich ist.[19] Ein Personenbezug ist daher dann zu vereinen, wenn der Aufwand den Informationswert so wesentlich übertrifft, dass man vernünftigerweise davon ausgehen muss, dass der Versuch der Bestimmung der Person unter Verwendung der vorhandenen Daten nicht unternommen wird.[20]

Maßgebend ist somit, dass die Person, auf die sich die Daten beziehen, dem Verantwortlichen bekannt oder zumindest von ihm ermittelbar ist.[21] Für die indirekte Bestimmbarkeit sind alle Daten ausreichend, die ein Wiedererkennen ermöglichen (zB Telefonnummer, Reisepass- oder Personalausweisnummer), selbst wenn die Information erst in Verbindung mit anderen Informationen eine Unterscheidung bzw Identifizierbarkeit ermöglicht.[22] Die Identifizierung einer Person setzt damit insbesondere nicht die Kenntnis eines Namens voraus.[23]

Die DSGVO enthält ferner eine taxative Aufzählung **besonderer Kategorien personenbezogener** Daten, die aus verschiedenen Gründen als besonders schutzwürdig eingestuft sind.[24] Dabei handelt es sich um personenbezogene Daten, „aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit

---

[15] 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 (gültig bis 24. Mai 2018, aufgehoben durch die DSGVO).

[16] *EK*, Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, Mitteilung COM(2019) 250 final, 5 (FN 10), https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52019DC0250 (zuletzt abgerufen am 29.4.2021).

[17] EG 26 Satz 3 DSGVO.

[18] EG 26 Satz 4 DSGVO; Siehe weitere Interpretationsansätze bei EuGH 19. 10. 2016, C-582/14, *Breyer*, Rn 49: „[…] eine dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum i.S.d. genannten Bestimmung darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen."

[19] DSB 31.10.2018, DSB-D123.076/0003.DSB/2018 (Informationspflichtenverletzung beim Cold Calling); *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG) § 1 (Stand 1.1.2020, rdb.at) Rz 14.

[20] *Schild* in Wolff/Brink, BeckOK Datenschutzrecht (35. Edition, Stand: 01.02.2021) Art 4 Rn 18.

[21] *Gola* in Gola, DS-GVO[2] Art 4 Rz 16.

[22] *Schild* in Wolff/Brink, BeckOK Datenschutzrecht (35. Edition, Stand: 01.02.2021) Art 4 Rn 18.

[23] *Artikel-29-Datenschutzgruppe,* Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP136, 16f, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_de.pdf (zuletzt abgerufen am 29.4.2021).

[24] *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 9 DSGVO (Stand 7.5.2020, rdb.at) Rz 16ff.

hervorgehen, sowie […] genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person".[25]

Der **Begriff „nicht-personenbezogene Daten"** wird in der Free-Flow-of-Data-VO in Abgrenzung zu personenbezogenen Daten im Sinne der DSGVO definiert.[26] Entsprechend der Negativdefinition bezieht sich diese Verordnung auf „Daten, die keine personenbezogenen Daten im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679 sind".[27] Der sachliche Anwendungsbereich ist zusätzlich auf die Verarbeitung elektronischer Daten beschränkt.[28]

Nicht-personenbezogene Daten lassen sich je nach Herkunft klassifizieren als i) Daten, die sich ursprünglich nicht auf eine identifizierte oder identifizierbare natürliche Person bezogen, und ii) Daten, die ursprünglich personenbezogene Daten waren, später jedoch anonymisiert wurden.[29] Bedeutende Quellen für nicht-personenbezogene Daten stellen das wachsende Internet der Dinge, künstliche Intelligenz und maschinelles Lernen, zB durch ihren Einsatz in automatisierten industriellen Produktionsprozessen, dar.[30] „Konkrete Beispiele für nicht-personenbezogene Daten umfassen aggregierte und anonymisierte Datensätze für Big-Data-Analysen, Daten im Zusammenhang mit der Präzisionslandwirtschaft, die dabei helfen können, den Einsatz von Pestiziden und Wasser zu überwachen und zu optimieren, oder Daten zum Wartungsbedarf von Industriemaschinen."[31]

Wird es allerdings „durch technologische Neuentwicklungen möglich, anonymisierten Daten wieder in personenbezogene Daten umzuwandeln, müssen diese Daten als personenbezogene Daten behandelt werden, und die [DSGVO] muss entsprechend gelten."[32]

Des Weiteren gilt die Free-Flow-of-Data-VO bei einem Datensatz, der aus personenbezogenen und nicht-personenbezogenen Daten besteht („**gemischte Datensätze**"), für die nicht-personenbezogenen Daten des Datensatzes. Sind personenbezogene und nicht-personenbezogene Daten in einem Datensatz untrennbar miteinander verbunden, berührt die Free-Flow-of-Data-VO nicht die Anwendung der DSGVO.[33] Die Datenschutzrechte und -pflichten aus der DSGVO gelten in vollem Umfang für den gesamten gemischten Datensatz, und zwar auch dann, wenn die personenbezogenen Daten nur einen kleinen Teil des Datensatzes ausmachen.[34]

Beispiele für gemischte Datensätze sind etwa i) Anonymisierte statistische Daten von Forschungseinrichtungen und die ursprünglich erhobenen Rohdaten, zB die Antworten der einzelnen Teilnehmer auf die Fragen im Rahmen statistischer Erhebungen, ii) Daten im Zusammenhang mit dem Internet der Dinge, wenn einige der Daten Annahmen über bestimmbare Personen ermöglichen (zB

[25] Art 9 Abs 1 DSGVO; zum Begriff „genetische Daten" siehe Art 4 Nr 13; zum Begriff „biometrische Daten" siehe Art 4 Nr 14; zum Begriff „Gesundheitsdaten" siehe Art 4 Nr 15.
[26] *EK*, Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, Mitteilung COM(2019) 250 final, 4.
[27] Art 3 Z 1 Free-Flow-of-Data-VO.
[28] Art 2 Abs 1 Free-Flow-of-Data-VO.
[29] *EK*, Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, Mitteilung COM(2019) 250 final, 5ff.
[30] EG 9 Satz 1 Free-Flow-of-Data-VO.
[31] EG 9 Satz 2 Free-Flow-of-Data-VO.
[32] EG 9 Satz 3 Free-Flow-of-Data-VO.
[33] Art 2 Abs 2 Free-Flow-of-Data-VO.
[34] *EK*, Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, Mitteilung COM(2019) 250 final, 9f.

Anwesenheit an einer bestimmten Adresse und Nutzungsmuster) und iii) Analysen der Betriebslog-Daten von Produktionsanlagen in der verarbeitenden Industrie.[35]

**Im Ergebnis** sind „[a]uch potentiell personenbezogene Daten […] konsequenterweise als Daten über bestimmbare Personen zu behandeln."[36] Bei einem kollaborativen Daten-, Informations- und Wissensmanagement können neben den verarbeiteten „Inhaltsdaten" auch Stammdaten[37] und sonstige Nutzungsdaten[38] der Nutzer der Infrastruktur und allfälligen sonstigen Akteure wie Administratoren (zB Registrierungs- und Zugriffsdaten) personenbezogen sein.

#### *4.1.2.2. Sachlicher Anwendungsbereich der DSGVO und des DSG*

Die DSGVO schützt die Grundrechte und Grundfreiheiten natürlicher Personen.[39] Sie „gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen."[40]

Unter **Verarbeitung** im Sinne der DSGVO ist jeder „mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung", zu verstehen.[41]

Nicht der DSGVO unterliegt „die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person."[42] Ausnahmsweise sind auch juristische Personen geschützt, wenn sich in der Firma der juristischen Person der Name einer natürlichen Person findet.[43]

Der Schutzbereich des **Grundrechts auf Datenschutz** wird durch das österreichische DSG allerdings weiterhin erweitert, nach dem „[j]edermann [einen] Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht [hat]".[44]

Laut DSB „schützt die DSGVO selbst [zwar] nur natürliche Personen, jedoch sei in verfassungskonformer Interpretation davon auszugehen, dass die in § 1 DSG normierten Rechte auch **juristischen Personen** zukommen und diese sich folglich darauf berufen können."[45] Danach stehen den

[35] *EK*, Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, Mitteilung COM(2019) 250 final, 8.
[36] Ernst in Paal/Pauly, DS-GVO BDSG (3. Auflage 2021) Art 4 Rn 12.
[37] Siehe dazu etwa § 92 Abs 3 Z 3 TKG 2003.
[38] Siehe dazu etwa § 15 dTMG.
[39] Art 1 DSGVO.
[40] Art 2 Abs 1 DSGVO.
[41] Art 4 Z 2 DSGVO.
[42] EG 14 Satz 2 DSGVO.
[43] EuGH 9. 11. 2010, C-92/09 und C-93/09 (*Volker und Markus Schecke and Eifert*), Rz 53, 87; zuletzt etwa EuG 2. 11. 2017, T-670/16 (*Digital Rights Ireland Ltd*), Rz 26.
[44] § 1 Abs 1 DSG.
[45] DSB 13. 9. 2018, DSB-D216.713/0006-DSB/2018.

juristischen Personen das Recht auf Auskunft sowie das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten zu, weil diese bereits in § 1 DSG angelegt sind, nicht aber weitere in der DSGVO vorgesehenen Rechte, wie zB das Recht auf Datenübertragbarkeit.[46, 47]

Nach der Rechtsprechung der DSB kann sich allerdings eine juristische Person lediglich in jenen Fällen, in denen Beschwerdeführer und Beschwerdegegner in Österreich ansässig sind und die Datenschutzbehörde alleine für das Verfahren zuständig ist, auf die in § 1 DSG statuierten verfassungsgesetzlichen Rechte berufen („**Binnenfälle**“).[48] Hingegen sind grenzüberschreitende Fälle ausschließlich nach der DSGVO zu beurteilen, daher können sich juristische Personen hier nicht auf § 1 DSG berufen.[49]

Bei der Planung und Gestaltung des Referenzmodells für ein kollaboratives Daten-, Informations- und Wissensmanagement ist **zu untersuchen**, ob personenbezogene Daten juristischer Personen, wie etwa Kontaktdaten und Wirtschaftsdaten,[50] verarbeitet werden und ob ein Binnenfall vorliegt. Bejahendenfalls ist die Erfüllung der Rechte nach dem DSG sicherzustellen.

#### *4.1.2.3. Offensichtlich öffentlich gemachte Daten*

Eine Person hat ihre personenbezogenen Daten öffentlich gemacht, wenn die Daten dem Zugriff einer unbestimmten Anzahl von Personen ohne wesentliche Zulassungsschranke offenstehen.[51] Die betroffene Person muss die Daten offensichtlich, dh durch eigenen (bewussten) Willensakt, öffentlich gemacht haben, was nach allen Umständen des Einzelfalls zu beurteilen ist (zu den geheimen Daten siehe Punkt 4.1.3.3 unten).[52]

Eine **generelle Ausnahme** vom Anspruch auf Geheimhaltung für zulässigerweise veröffentlichte Daten ist **nicht mit der DSGVO vereinbar**, daher dürfen nicht alle Daten, die veröffentlicht werden oder öffentlich zugänglich sind, von einem Verantwortlichen für beliebige eigene Zwecke verwendet werden.[53]

---

[46] *Schmidl*, Wesentliche Rechtsfragen des ersten Anwendungsjahres der DSGVO, Jahrbuch Datenschutzrecht 2019, 9 (13).
[47] Es ist allerdings befremdlich, dass eine analoge (!) Anwendung europarechtlicher Bestimmungen aufgrund einer nationalstaatlichen Besonderheit, die im nationalen Verfassungsrecht verwurzelt ist, geboten sein soll. Schon bei der (europarechtlichen) Lücke sind Zweifel einigermaßen berechtigt, weist doch schon der Titel der DSGVO darauf hin, nur für natürliche Personen einschlägig zu sein – erst Recht gälte das für die Planwidrigkeit und die Gebotenheit der Lückenschließung aus Gründen der Gleichbehandlung.
[48] DSB 13. 9. 2018, DSB-D216.713/0006-DSB/2018; *Schmidl*, Wesentliche Rechtsfragen des ersten Anwendungsjahres der DSGVO, Jahrbuch Datenschutzrecht 2019, 9 (13.
[49] DSB 19. 7. 2018, DSB-D123.089/0002-DSB/2018; *Schmidl*, Wesentliche Rechtsfragen des ersten Anwendungsjahres der DSGVO, Jahrbuch Datenschutzrecht 2019, 9 (13).
[50] *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG) § 1 (Stand 1.1.2020, rdb.at) Rz 15 ff.
[51] *dBMWi*, Orientierungshilfe zum Gesundheitsdatenschutz (Nov 2018), 24f, https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/orientierungshilfe-gesundheitsdatenschutz.html (zuletzt abgerufen am 3.5.2021).
[52] *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 9 DSGVO (Stand 7.5.2020, rdb.at) Rz 41.
[53] *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG) § 1 (Stand 1.1.2020, rdb.at) Rz 17 mit Verweis auf DSB 31.10.2018, DSB-D123.076/0003.DSB/2018 (Informationspflichtenverletzung beim Cold Calling) und DSB 15.1.2019, DSB-D123.527/0004-DSB/2018 (Ärztebewertungsplattform); siehe auch § 1 Abs 1

Als Rechtsgrundlage für die Verarbeitung von offensichtlich öffentlich gemachten personenbezogenen Daten kommt regelmäßig das berechtigte Interesse des Verantwortlichen oder eines Dritten gemäß Artikel 6 Abs 1 lit f DSGVO in Betracht (siehe Punkt 4.2.2 unten).[54] Sind Informationen im Internet durch die betroffene Person frei verfügbar gemacht worden, so ist ihre Nutzung datenschutzrechtlich grundsätzlich erlaubt. Die Interessensabwägung muss jedoch auch hier immer einzelfallbezogen erfolgen und die Rechte und Interessen der betroffenen Person sind hinreichend und dokumentiert zu berücksichtigen.[55]

Bezieht sich die Verarbeitung auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat, dürfen in der Regel auch besondere Kategorien personenbezogener Daten verarbeitet werden (siehe Punkt 4.2.2.5 unten).[56]

Der Verantwortliche sollte **dokumentieren**, woher die Daten stammen, um auf diese Weise nachweisen zu können, dass die Daten tatsächlich öffentlich gemacht wurden. Des Weiteren ist die Rechtsgrundlage für die Verarbeitung, inklusive der bei Stützung auf ein berechtigtes Interesse durchzuführenden Interessensabwägung, festzuhalten.[57]

#### *4.1.2.4. Anonymisierung von Daten*

Anonym sind „Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann."[58] Die Anonymisierung ist daher das Ergebnis der Verarbeitung personenbezogener Daten mit dem Ziel, eine **Identifizierung unwiderruflich unmöglich zu machen**.[59]

**Die Verarbeitung anonymer Daten unterliegt nicht der DSGVO und/oder dem DSG**, daher ist für die Verarbeitung von Daten nach der Entfernung des Personenbezugs **keine Rechtsgrundlage** iSv Art 6 oder Art 9 DSGVO erforderlich (siehe Punkt 4.2 unten).[60] Dies gilt auch, wenn die Verarbeitung zu statistischen oder für Forschungszwecken erfolgt (siehe Punkt 4.2.5 unten).[61]

---

Satz 2 DSG: „Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind."

[54] *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 54.

[55] *dBMWi*, Orientierungshilfe zum Gesundheitsdatenschutz (Nov 2018), 24f; *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 9 DSGVO (Stand 7.5.2020, rdb.at) Rz 41.

[56] Art 9 Abs 2 lit e DSGVO; *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 9 DSGVO (Stand 7.5.2020, rdb.at) Rz 41ff.

[57] *dBMWi*, Orientierungshilfe zum Gesundheitsdatenschutz (Nov 2018), 25; siehe auch *Dallmann/Busse*, Verarbeitung von öffentlich zugänglichen personenbezogenen Daten - Datenschutzrechtliche Voraussetzungen und Grenzen, ZD 2019, 394.

[58] EG 26 Satz 5 DSGVO.

[59] *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP216 (Angenommen am 10. April 2014), 3, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf (zuletzt abgerufen am 3.5.2021).

[60] EG 26 Satz 6 DSGVO.

[61] EG 26 Satz 6 DSGVO.

Wenn der Verantwortliche die Daten auf einer Ebene aggregiert, auf der keine Einzelereignisse mehr identifizierbar sind, kann der entstandene Datenbestand als anonym, d.h. ohne Personenbezug, bezeichnet werden.[62] Es muss allerdings bei der Entfernung des Personenbezugs („Anonymisierung von personenbezogenen Daten") sichergestellt werden, dass weder der Verantwortliche selbst, noch ein Dritter ohne unverhältnismäßigen Aufwand einen Personenbezug wiederherstellen kann.[63] Deswegen verlangt (gerade) auch der Umgang mit anonymisierten Daten die Einhegung durch vertragliche Vereinbarungen zwischen dem Halter und dem Nutzer der Daten, um sicherzustellen, dass diese nicht kontextlos und ungeschützt weiter verarbeitet und damit einem inakzeptabel erhöhten Reidentifizierungsrisiko ausgesetzt werden.

„Dass sich zu irgendeinem Zeitpunkt eine Rekonstruktion (etwa unter Verwendung neuer technischer Hilfsmittel) als möglich erweist", macht die Anonymisierung nicht unzureichend. Eine völlige Irreversibilität ist daher nicht notwendig.[64] Wird es allerdings „durch technologische Neuentwicklungen möglich, anonymisierten Daten wieder in personenbezogene Daten umzuwandeln, müssen diese Daten als personenbezogene Daten behandelt werden" und die Verarbeitung unterliegt (wieder) der DSGVO.[65]

Hingegen handelt es sich bei der **Verschlüsselung** und Pseudonymisierung personenbezogener Daten (lediglich) um Informationssicherheitsmaßnahmen zur Aufrechterhaltung der IT-Sicherheit, Vorbeugung einer rechtswidrigen Verarbeitung und Eindämmung der mit der Verarbeitung verbundenen Risiken.[66]

Die Verschlüsselung der Daten unterstützt wichtige in der DSGVO verankerten Ziele wie Sicherstellung der Vertraulichkeit und Integrität der Daten sowie Verbindlichkeit und Authentizität der Quelle. Die DSGVO enthält jedoch keine spezifischen Bestimmungen, bei welchen Verarbeitungen eine Verschlüsselung als angebracht erscheint und überlässt diese Entscheidung dem Verantwortlichen.[67]

Als **Pseudonymisierung** wird „die Verarbeitung personenbezogener Daten in einer Weise" definiert, „dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden".[68]

Sollten daher in einem Datensatz (gewisse) personenbezogene Daten durch Kennungen ersetzt werden, eine Re-Identifizierung aber bei Bedarf, etwa im Fall eines Rechtsstreits, möglich bleiben, handelt es sich dabei nicht um eine Maßnahme, die zum Entfall der Anwendbarkeit der DSGVO führt.[69]

---

[62] *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken (Angenommen am 10. April 2014), WP216, 10.
[63] DSB 5.12.2018, DSB-D123.270/0009-DSB/2018 (D.2) (Anonymisierung): zur Anonymisierung zulässiger als „Löschung durch Unkenntlichmachung".
[64] DSB 5. 12. 2018, DSB-D123.270/0009-DSB/2018 mwN (Anonymisierung).
[65] EG 9 Satz 3 Free-Flow-of-Data-VO.
[66] Art 32 DSGVO; EG 83 Satz 1 DSGVO.
[67] *Pollirer* in Knyrim, DatKomm Art 32 DSGVO (Stand 1.10.2018, rdb.at) Rz 45.
[68] Art 4 Z 5 DSGVO.
[69] Art 4 Z 5 DSGVO; EG 28f DSGVO; *Hödl* in Knyrim, DatKomm Art 4 DSGVO (Stand 1.12.2018, rdb.at) Rz 57ff.

Die Aufhebung des Personenbezugs der Daten kann allerdings etwa „durch Löschung der Zuordnungstabelle zuvor pseudonymisierter Daten oder durch Löschung des Schlüssels zuvor verschlüsselter Daten“ erfolgen.[70]

### 4.1.3. Sondergesetzlicher Schutz von Daten

#### *4.1.3.1. Einleitung*

Neben dem Datenschutzrecht stellt der sondergesetzliche Schutz des geistigen Eigentums und des vertraulichen Know-hows und Geschäftsinformationen einen weiteren Anknüpfungspunkt zur Kontrolle der Daten.

Diese Schutz- und Zuordnungsregimes stellen auf den **Verarbeitungsgrad** der Daten ab. Die **Rohdaten**, etwa die von Maschinen generierten (Maschinen-)daten, entstehen in einem ersten „Verarbeitungsschritt“. Werden diese weiterverarbeitet und ist ein bestimmter Grad an Verarbeitung erreicht, werden aus Rohdaten durch die Schaffung von verarbeiteten und veredelten Daten **Informationen**. In einer letzten Stufe werden mithilfe von Wissen konkrete **Inhalte** geschaffen.[71]

#### *4.1.3.2. Schutz der Daten als geistiges Eigentum*

Ein Patent wird auf Antrag erteilt, „[f]ür Erfindungen auf allen Gebieten der Technik […], sofern sie neu sind, sich für den Fachmann nicht in nahe liegender Weise aus dem Stand der Technik ergeben und gewerblich anwendbar sind“. Diese weite Definition ermöglicht es, diverse Erzeugnisse und Verfahren zu schützen. Patentierbare Innovationen können die gesamte Spanne von Alltagsgegenständen bis hin zu High-Tech-Produkten betreffen.[72] Bei Rohdaten fehlt es allerdings an einer Erfindung.[73]

Des Weiteren kann ab der Erkennbarkeit eigentümlicher geistiger Leistungen oder dem Einsatz entsprechender Investitionen Schutz nach dem Urheberrecht in Anspruch genommen werden.[74] Urheberrechtich geschützte Werke „sind eigentümliche geistige Schöpfungen auf den Gebieten der Literatur, der Tonkunst, der bildenden Künste und der Filmkunst.“[75] Umfasst sind auch etwa Computerprogramme.[76] Geschützt wird nicht nur Quellcode, sondern „alle Ausdrucksformen

[70] *Hötzendorfer/Tschohl/Kastelitz* in Knyrim, DatKomm Art 5 DSGVO (Stand 7.5.2020, rdb.at) Rz 51; EuGH 20. 12. 2017, C-434/16, *Nowak*, Rz 55 f: Vernichtung oder Anonymisierung.
[71] *Rungg/Buchroithner*, Data Ownership in Binder Grösswang, Digital Law (2. Aufl, 2020), 141.
[72] *Ciarnau/Heinzl/Klammer/Seling* in Anderl, IP in der Praxis, 1. Kapitel (Stand 1.4.2020, rdb.at) Rz 1.184.
[73] *Forgó*, Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen in Forgó/Zöchling-Jud, Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter, 20. ÖJT Band II/1, 360.
[74] *Rungg/Buchroithner*, Data Ownership in Binder Grösswang, Digital Law (2. Aufl, 2020), 155.
[75] § 1 Abs 1 UrhG.
[76] § 2 Z 1 UrhG.

einschließlich des Maschinencodes sowie das Material zur Entwicklung des Computerprogramms".[77] Bei einem rohen Datum liegt allerdings eine derartige eigentümliche geistige Schöpfung nicht vor.[78]

Werden Daten, Werke oder andere unabhängige Elemente systematisch oder methodisch angeordnet und einzeln mit elektronischen Mitteln oder auf andere Weise zugänglich, handelt es sich bei diesen Sammlungen um Datenbanken im Sinne des Urheberrechts.[79] Das sui-generis-Recht des Datenbankherstellers knüpft nicht an eine eigentümliche geistige Schöpfung, sondern an eine wesentliche Investition an, „die für die Beschaffung, Überprüfung oder Darstellung ihres Inhalts […] erforderlich war".[80]

Das Schutzobjekt ist die geleistete Investition in die Organisation von Daten, nicht das Datum selbst.[81] Es ist daher nicht die Investition in die Erzeugung von Daten, aus denen der Inhalt einer Datenbank besteht, geschützt.[82]

Es entsteht auch kein (eigentumsähnliches) Vollrecht an der Datenbank, sondern es werden nur bestimmte Verwertungshandlungen dem Hersteller vorbehalten.[83] Daher ist auch der Datenbankschutz kein geeigneter Anknüpfungspunkt für den Schutz von Rohdaten.[84]

#### *4.1.3.3. Schutz der Daten als Geschäftsgeheimnis*

Als Geschäftsgeheimnis ist eine „Information [geschützt], 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

[77] § 40a Abs 2 UrhG.
[78] *Forgó*, Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen in Forgó/Zöchling-Jud, Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter, 20. ÖJT Band II/1, 360.
[79] § 40f Abs 1 UrhG.
[80] § 76c Abs 1 UrhG.
[81] *Forgó*, Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen in Forgó/Zöchling-Jud, Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter, 20. ÖJT Band II/1, 360 mwN; Vgl. § 76c Abs 3 und Abs 4 UrhG: Der Schutz ist unabhängig davon, ob die Datenbank als solche oder ihr Inhalt für den urheberrechtlichen oder einen anderen sonderrechtlichen Schutz in Betracht kommt und berührt nicht die am Inhalt der Datenbank etwa bestehenden Rechte.
[82] EuGH 9.11.2004, C-203/02, *British Horseracing/William Hill* (Pferdewetten), Rz 42; OGH 12. 6. 2007, 4 Ob 11/07 g (*EDV-Firmenbuch III*); *Woller* in Kucsko/Handig, urheber.recht2 § 76c UrhG (Stand 1.4.2017, rdb.at) Rz 22f mwN.
[83] § 76d Abs 1 UrhG: der Hersteller „hat mit den vom Gesetz bestimmten Beschränkungen das ausschließliche Recht, die ganze Datenbank oder einen nach Art oder Umfang wesentlichen Teil derselben zu vervielfältigen, zu verbreiten, durch Rundfunk zu senden, öffentlich wiederzugeben und der Öffentlichkeit zur Verfügung zu stellen. Diesen Verwertungshandlungen stehen die wiederholte und systematische Vervielfältigung, Verbreitung, Rundfunksendung und öffentliche Wiedergabe von unwesentlichen Teilen der Datenbank gleich, wenn diese Handlungen der normalen Verwertung der Datenbank entgegenstehen oder die berechtigten Interessen des Herstellers der Datenbank unzumutbar beeinträchtigen".
[84] *Forgó*, Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen in Forgó/Zöchling-Jud, Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter, 20. ÖJT Band II/1, 360.

die Person ist, welche die rechtmäßige Verfügungsgewalt über diese Informationen ausübt".[85] Der Inhaber eines Geschäftsgeheimnisses ist „jede natürliche oder juristische Person, welche die rechtmäßige Verfügungsgewalt über ein Geschäftsgeheimnis besitzt".[86]

Die aus aggregierten, verarbeiteten und veredelten Daten entwickelten Informationen können in den Schutzbereich von Geschäftsgeheimnissen fallen. Bei Rohdaten ist allerdings die erforderliche Geheimhaltung von Informationen oft weder technisch noch faktisch erreichbar.[87]

**Im Ergebnis** sind lediglich die auf den Rohdaten aufbauenden weiterentwickelten Daten sondergesetzlich geschützt. Hingegen besteht für (Roh-)Daten, die nicht oder nicht ausreichend derart bearbeitet wurden, dass sie den Schutz des geistigen Eigentums erreichen oder als Geschäftsgeheimnis geschützt werden, kein gesetzlicher Schutz (siehe Punkt 4.4 unten).

## 4.2. Rechtsgrundlagen für die Verarbeitung personenbezogener Daten

### 4.2.1. Einleitung

Bei den im Projekt anfallenden bzw. zu entwickelnden Daten-, Informations- und Wissensmanagementinfrastrukturen werden auch personenbezogene Daten verarbeitet (siehe Punkt 4.1.2.1 oben).

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime **Zwecke** erhoben und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (**Primärerhebung** bzw **Erstverarbeitung**; zur Weiterverarbeitung siehe Punkt 4.2.6 unten).[88] Diese Zwecke sollten zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen (Grundsatz der Zweckbindung und der Zweckvereinbarkeit).[89]

Die Verarbeitung personenbezogener Daten ist nur erlaubt, wenn für sie eine Legitimationsgrundlage vorliegt (*Verbot mit Erlaubnisvorbehalt*). Die Verarbeitung Daten ist nur **rechtmäßig**, wenn *„mindestens"* ein gesetzlicher **Erlaubnistatbestand** erfüllt ist oder die betroffene Person eingewilligt hat.[90] Zwischen den Erlaubnistatbeständen besteht kein Rangverhältnis, diese stehen alternativ nebeneinander. Deren Aufzählung ist abschließend.[91]

Da die gesetzlichen Erlaubnistatbestände grundsätzlich auch im Falle einer Verweigerung (oder eines Widerrufs) der Einwilligung greifen, sind diese vorab zu prüfen.[92] Es ist auch zu beachten, dass eine

[85] § 26b Abs 1 UWG; *Görg* in Görg (Hrsg), UWG Kommentar (2020) § 26b UWG Rz .
[86] § 26b Abs 2 UWG; *Görg* in Görg (Hrsg), UWG Kommentar (2020) § 26b UWG Rz 83ff.
[87] *Rungg/Buchroithner*, Data Ownership in Binder Grösswang, Digital Law (2. Aufl, 2020), 152ff; *Forgó*, Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen in Forgó/Zöchling-Jud, Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter, 20. ÖJT Band II/1, 360.
[88] Art 5 Abs 1 lit b DSGVO.
[89] ErwGr 39 Satz 6 DSGVO, vgl. zur Zweckbindung *Artikel-29-Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, WP203 (Adopted on 2 April 2013).
[90] Art 6 Abs 1 DSGVO; EG 40 Satz 1 DSGVO.
[91] Art 6 Abs 1 DSGVO; *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 14.
[92] *Schulz* in Gola, DS-GVO[2] Art 6 Rz 11.

Datenverarbeitung nicht *„sicherheitshalber“* auf eine Einwilligung gestützt werden soll, wenn eine andere Rechtsgrundlage vorhanden ist, besteht doch in einem solchen Fall die Gefahr einerseits einer nicht zutreffenden und damit nicht normkonformen Information des Betroffenen (siehe Punkt 4.3.3 unten) und andererseits einer *„Verdrängung“* des Erlaubnistatbestands durch die eingeholte Einwilligung (siehe Punkt 4.2.4 unten). Außerdem hat die Einwilligung aus Sicht des Verantwortlichen den Nachteil, jederzeit und unbegründet widerrufbar zu sein, was die Rechtsgrundlage mit Wirkung für die Zukunft jederzeit entfallen lassen kann.

### 4.2.2. Gesetzliche Rechtsgrundlagen

Die Verarbeitung personenbezogener Daten kann auf mehrere gesetzliche Erlaubnistatbestände gestützt werden.[93] Bei kollaborativem Daten-, Informations- und Wissensmanagement sind Folgende besonders hervorzuheben:

#### *4.2.2.1. Vertragserfüllung oder -abschluss*

Die Verarbeitung personenbezogener Daten ist rechtmäßig, wenn sie „für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich [ist], die auf Anfrage der betroffenen Person erfolgen“[94]

Erlaubt die Verarbeitung personenbezogener Daten im Rahmen einer Vertragserfüllung im weiteren Sinne, somit auch die Erfüllung von Nebenpflichten, sofern diese für die Vertragszwecke erforderlich sind.[95] Auf diesen Rechtfertigungsgrund kann etwa die Verarbeitung von Kreditkartendetails zum Zwecke der Zahlungsdurchführung gestützt werden.[96]

Die Bestimmung ist eng auszulegen und gilt nicht für Situationen, in denen die Verarbeitung für die Erfüllung eines Vertrags nicht wirklich notwendig ist, sondern der betroffenen Person von dem Verantwortlichen einseitig auferlegt wird. „Beispielsweise [ist sie] keine geeignete Rechtsgrundlage für die Erstellung eines Profils der Geschmacksvorlieben und des Lebensstils eines Nutzers auf der Grundlage seiner Clickstream-Daten von einer Website und der von ihm gekauften Waren.“[97]

---

[93] EG 40 DSGVO.
[94] Art 6 Abs 1 lit b DSGVO; EG 44 DSGVO; siehe auch *EDSA*, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen (Version 2.0, 8.10.2019), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_de (zuletzt abgerufen am 3.5.2021).
[95] *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 33.
[96] *Artikel-29-Datenschutzgruppe,* Stellungnahme zum Begriff des berechtigten Interesses, WP217, 21, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_de.pdf (zuletzt abgerufen am 3.5.2021).
[97] *Artikel-29-Datenschutzgruppe,* Stellungnahme zum Begriff des berechtigten Interesses, WP217, 21f; *EDSA*, Leitlinien 2/2019 Artikel 6 Absatz 1 Buchstabe b DSGVO iZm Online-Diensten (Version 2.0, 8.10.2019), 12.

#### *4.2.2.2. Rechtliche Verpflichtung*

Rechtmäßig ist eine Datenverarbeitung, die „zur Erfüllung einer rechtlichen Verpflichtung erforderlich [ist], der der Verantwortliche unterliegt“[98] Diese rechtliche Verpflichtung muss eine Grundlage im Unionsrecht oder im Recht eines Mitgliedstaats haben.[99]

Damit dieser Erlaubnistatbestand zur Anwendung kommt, muss die betreffende Verarbeitungspflicht kraft objektiven Rechts – darunter sind Gesetz, Verordnung, Kollektivverträge und Betriebsvereinbarungen zu subsumieren[100] – vorgeschrieben worden sein. Eine Verpflichtung durch vertragliche Vereinbarung ist nicht ausreichend. Der Verantwortliche darf auch nicht die Wahl haben, ob er die Verpflichtung erfüllt oder nicht. Freiwillige einseitige Verabredungen und öffentlich-private Partnerschaften, die Daten über den gesetzlich geforderten Rahmen hinaus verarbeiten, sind daher nicht umfasst.[101]

#### *4.2.2.3. Öffentliche Aufgabe*

Die Verarbeitung ist rechtmäßig, wenn sie „für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.“[102] „Dies kann beispielsweise im Zusammenhang mit Verarbeitungsmaßnahmen im Verkehrs- oder Gesundheitssektor der Fall sein (etwa bei epidemiologischen Studien oder Forschungsarbeiten).[103]

Ist die Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich, muss hierfür eine Grundlage im Unionsrecht oder im Recht eines Mitgliedstaats bestehen.[104] Die Aufgabe kann nicht nur einer Behörde oder einer anderen unter das öffentliche Recht fallenden natürlichen oder juristischen Person, sondern auch einer natürlichen oder juristischen Personen des Privatrechts zugewiesen werden.[105]

#### *4.2.2.4. Berechtigtes Interesse*

Eine Datenverarbeitung, die „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich [ist], ist rechtmäßig, „sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern,

[98] Art 6 Abs 1 lit c DSGVO.
[99] EG 45 Satz 1 DSGVO; siehe auch EG 41 DSGVO „Rechtsgrundlagen und Gesetzgebungsmaßnahmen“.
[100] EG 41 DSGVO; *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 39.
[101] *Artikel-29-Datenschutzgruppe,* Stellungnahme zum Begriff des berechtigten Interesses, WP217, 24f.
[102] Art 6 Abs 1 lit e DSGVO.
[103] *Artikel-29-Datenschutzgruppe,* Stellungnahme zum Begriff des berechtigten Interesses, WP217, 28.
[104] EG 45 Satz 1 DSGVO; siehe auch EG 41 DSGVO „Rechtsgrundlagen und Gesetzgebungsmaßnahmen“.
[105] EG 45 Satz 6 DSGVO; *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 46.

überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt".[106] Die Rechtmäßigkeit kann auch durch die berechtigten eines Verantwortlichen, dem die personenbezogenen Daten offengelegt werden dürfen, begründet sein.[107]

Bei der Interessenabwägung „sind die vernünftigen Erwartungen der betroffenen Personen, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen."[108] Es ist auch zu prüfen, „ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird."[109] Insbesondere in Situationen, „in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen."[110]

„Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht."[111] Ferner sind Netz- und Informationssicherheit als überwiegendes berechtigtes Interesse für die Verarbeitung von personenbezogenen Daten zu qualifizieren.[112]

Behörden, die eine Verarbeitung in Erfüllung ihrer Aufgaben vornehmen, können sich nicht auf diese Rechtsgrundlage berufen, weil es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen.[113] Ebenso ist zu beachten (dazu sogleich), dass diese Rechtsgrundlage bei Verarbeitung besonderer Kategorien personenbezogener Daten nicht zur Verfügung steht und daher insb. die Verarbeitung von Gesundheitsdaten darauf nicht gestützt werden kann.

#### *4.2.2.5. Verarbeitung besonderer Kategorien personenbezogener Daten*

Hingegen kann die Verarbeitung besonderer Kategorien personenbezogener Daten (siehe Punkt 4.1.2.1 oben) nur auf restriktivere gesetzliche Erlaubnistatbestände gemäß Art 9 Abs 2 DSGVO oder eine **ausdrückliche Einwilligung** der betroffenen Person gestützt werden (siehe Punkt 4.2.3.4 unten).

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist etwa zulässig, wenn die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses[114] oder aus Gründen des

[106] Art 6 Abs 1 lit f DSGVO.
[107] EG 47 Satz 1 DSGVO; *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 49 (51).
[108] EG 47 Satz 1 DSGVO.
[109] EG 47 Satz 3 DSGVO.
[110] EG 47 Satz 4 DSGVO.
[111] EG 47 Satz 2 DSGVO.
[112] EG 47 Satz 2 DSGVO.
[113] EG 49 DSGVO.
[114] Art 9 Abs 2 lit g DSGVO.

öffentlichen Interesses im Bereich der öffentlichen Gesundheit[115] erforderlich ist. Die Verarbeitung kann auch für die Zwecke der individuellen Versorgung im Gesundheits- und Sozialbereich[116] erfolgen.

Des Weiteren ist die Verarbeitung zulässig, wenn sie „für im öffentlichen Interesse liegende Archivzwecke, für **wissenschaftliche** oder historische **Forschungszwecke** oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich" ist und sie „auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht" (siehe zur Verarbeitung zu Forschungszwecken Punkt 4.2.5 unten).[117]

Es handelt sich hier um keinen eigenständigen Zulässigkeitstatbestand, sondern um eine „Öffnungsklausel" zugunsten unionsrechtlicher und mitgliedstaatlicher Regelungen der Datenverarbeitung zu den Archiv-, Forschungs- und statistischen Zwecken.[118]

Der normative Mehrwert der Einstufung von Daten als besondere Kategorie personenbezogener Daten liegt insb. in der Nichteinschlägigkeit einer möglichen Interessenabwägung mit berechtigten Interessen des Verantwortlichen oder eines Dritten[119].[120] Des Weiteren ist eine Verarbeitung besonderer Kategorien personenbezogener Daten auf vertraglicher Basis[121] mangels Nennung in Art 9 Abs 2 DSGVO nur bei Subsumtion eines Vertragssachverhalts unter einen in dieser Bestimmung genannten spezifischen Erlaubnistatbestand möglich (zB aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs nach Art 9 Abs 2 lit h DSGVO, wobei sich die Zulässigkeit hier eben nicht aus dem Vertrag allein ergibt).[122]

### 4.2.3. Einwilligung

#### *4.2.3.1. Definition der Einwilligung*

Die Einwilligung wird in der DSGVO als *„jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist"*, definiert.[123] Diese Elemente müssen kumulativ vorliegen.

Die Rechtsnatur der Einwilligung ist ausschließlich unionsrechtsautonom zu bestimmen, sodass sie nicht einer nationalen zivilrechtlichen Kategorie zuzuordnen ist, sondern vielmehr **eine**

[115] Art 9 Abs 2 lit i DSGVO.
[116] Art 9 Abs 2 lit h DSGVO.
[117] Art 9 Abs 2 lit j DSGVO.
[118] *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 9 DSGVO (Stand 1.10.2018, rdb.at) Rz 59.
[119] Art 6 Abs 1 lit f DSGVO.
[120] *Schiff* in Ehmann/Selmayr, DS-GVO[2] Art 9 Rz 27.
[121] Art 6 Abs 1 lit b DSGVO.
[122] *Schulz* in Gola, DS-GVO[2] Art 9 Rz 6.
[123] Art 4 Z 11 DSGVO.

**rechtserhebliche Handlung sui generis** darstellt, welche auch hinsichtlich der Wirksamkeitsvoraussetzungen autonom zu behandeln ist.[124]

Die Einwilligung muss auf jeden Fall eingeholt werden, bevor der Verantwortliche mit der Verarbeitung der personenbezogenen Daten beginnt, für die die Einwilligung benötigt wird (**Erfordernis der „vorherigen" Einwilligung**). Eine nachträgliche Einwilligung ist von der DSGVO weder definiert noch gemeint.[125]

Beruht die Datenverarbeitung auf einer Einwilligung, trifft den Verantwortlichen weiters die Verpflichtung zu deren Nachweis. Dieser trägt daher die Beweislast für das Vorliegen sämtlicher Elemente der Einwilligung.[126]

#### *4.2.3.2. Freiwillige Einwilligung*

Die Einwilligung muss nach der DSGVO „freiwillig" erfolgen.[127] Davon ist nur dann auszugehen, wenn die betroffene Person „eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden".[128] Dies ist nicht der Fall, wenn die Einwilligung ein nicht verhandelbarer Teil von Geschäftsbedingungen ist.[129]

Eine Einwilligung wird „durch jede Form des unangemessenen Drucks oder der Einflussnahme (die sich auf viele verschiedene Weisen manifestieren können) auf die betroffene Person, die diese von der Ausübung ihres freien Willens abhalten, unwirksam.".[130]

Wenn es sich „bei dem Verantwortlichen um eine Behörde handelt", besteht „häufig ein klares Ungleichgewicht zwischen dem Verantwortlichen und der betroffenen Person". Allerdings ist „die Verwendung der Einwilligung als Rechtsgrundlage für die Datenverarbeitung durch Behörden im Rechtsrahmen der DS-GVO nicht vollständig ausgeschlossen".[131]

Des Weiteren gilt die Einwilligung „nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist" (**Granularität**) oder „wenn die Erfüllung eines

[124] *Buchner/Kühling* in Kühling/Buchner, DS-GVO/BDSG[2] Art 7 Rz 1a; *Ingold* in Sydow, EU-DSGVO (2017) Art 7 Rz 13.
[125] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020) Rz 90, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (zuletzt abgerufen am 3.5.2021).
[126] Art 7 Abs 1 DSGVO.
[127] Art 4 Z 11 DSGVO.
[128] EG 42 Satz 5 DSGVO.
[129] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020) Rz 13; zum Transparenzgebot und Trennungsgrundsatz bei Einwilligungserklärungen in Schriftform siehe Art 7 Abs 2 DSGVO und EG 42 Satz 3 DSGVO.
[130] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020) Rz 14.
[131] EG 43 Satz 1 DSGVO; *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020) Rz 16f.

Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist" (Konditionalität bzw **Kopplungsverbot**)."[132]

#### *4.2.3.3. Informierte Einwilligung (in Kenntnis der Sachlage)*

Eine Einwilligung muss ferner in „informierter Weise" erfolgen.[133] „Es ist von grundlegender Bedeutung, den betroffenen Personen Informationen bereitzustellen, bevor ihre Einwilligung eingeholt wird."[134]

„Damit eine Einwilligung in Kenntnis der Sachlage erfolgt, muss die betroffene Person über bestimmte Elemente informiert werden, die für die Entscheidungsfindung wesentlich sind." Es sind **mindestens** Informationen (i) über die Identität des Verantwortlichen, (ii) den Zweck jedes Verarbeitungsvorgangs, für den die Einwilligung eingeholt wird, (iii) die (Art der) Daten, die erhoben und verwendet werden, (iv) das Bestehen eines Rechts, die Einwilligung zu widerrufen, erforderlich. Ferner sind (v) gegebenenfalls Informationen über die Verwendung der Daten für eine automatisierte Entscheidungsfindung nach Art 22 DSGVO, und (vi) Angaben zu möglichen Risiken von Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien nach Art 46 DSGVO zu erteilen.[135]

Falls erforderlich, um die Datenverarbeitung vollinhaltlich nachzuvollziehen, kann im konkreten Fall die Erteilung von weiteren Informationen notwendig sein.[136]

Die DSGVO schreibt nicht vor, in welcher **Form** die Informationen bereitzustellen sind, um das Erfordernis der Einwilligung in informierter Weise zu erfüllen. Die Informationen können daher auf verschiedene Weise zur Verfügung gestellt werden, beispielsweise als schriftliche oder mündliche Erklärungen oder als Audio- oder Videonachrichten.[137]

#### *4.2.3.4. Ausdrückliche Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten*

Die DSGVO normiert eine ausdrückliche Einwilligung als Erlaubnistatbestand für die Verarbeitung besonderer Kategorien personenbezogener Daten (siehe Punkt 4.1.2.1 oben).

Der Begriff „ausdrücklich" bezieht sich darauf, „**wie** die betroffene Person ihre Einwilligung zum Ausdruck bringt. Die betroffene Person muss eine ausdrückliche Einwilligungserklärung abgeben."[138]

---

[132] EG 43 Satz 2 DSGVO; Art 7 Abs 4 DSGVO; *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020) Rz 25ff und 42ff.
[133] Art 4 Nr 11 DSGVO.
[134] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020) Rz 62.
[135] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020) Rz 64.
[136] ErwGr 42 Satz 4 DSGVO; *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP259 rev.01, 16, https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Guidelines/WP259_LeitlinienFuerDieEinwilligung.html (zuletzt abgerufen am 4.5.2021).
[137] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020), Rz 66ff.
[138] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020), Rz 93.

Neben einer schriftlichen (und unterschriebenen) Erklärung, kann eine betroffene Person vor allem im digitalen oder Online-Kontext eine ausdrückliche Einwilligung(serklärung) etwa „durch Ausfüllen eines elektronischen Formulars, Senden einer E-Mail, Hochladen eines eingescannten von der betroffenen Person unterzeichneten Dokuments oder durch das Unterzeichnen mit einer elektronischen Signatur erteilen.“ [139]

Ferner ist zu beachten, dass auch bei einer ausdrücklichen Einwilligung sonstige Voraussetzungen einer gültigen Einwilligung erfüllt werden müssen sowie die Informationspflichten gemäß Art 13 und Art 14 DSGVO einzuhalten sind.[140] Die erteilten Informationen müssen unmittelbar auf die Verarbeitung besonderer Kategorien personenbezogener Daten Bezug nehmen (siehe Punkt 4.2.3.3 oben).[141]

#### *4.2.3.5. Widerrufbarkeit der Einwilligung*

Ferner ist zu beachten, dass jede betroffene Person das Recht hat, ihre Einwilligung **jederzeit** zu **widerrufen**.[142] Ein Widerrufsgrund ist nicht erforderlich, auf ihr Widerrufsrecht kann die betroffene Person datenschutzrechtlich auch nicht (wirksam) verzichten.[143] Die betroffene Person wird vor Abgabe der Einwilligung über ihr Widerrufsrecht in Kenntnis gesetzt (siehe Punkt 4.2.3.3 oben).[144]

Durch den Widerruf der Einwilligung wird zwar die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt („Wirkung ex nunc“).[145] Der bisherige Datenbestand bleibt dem Verantwortlichen jedoch nicht erhalten. Vielmehr greift insoweit regelmäßig die Löschpflicht gemäß Art 17 DSGVO.[146]

Die DSGVO legt zwar nicht fest, dass „das Erteilen und Widerrufen der Einwilligung immer durch dieselbe Handlung erfolgen muss“, allerdings muss „[d]er Widerruf der Einwilligung […] so einfach wie die Erteilung der Einwilligung sein.“[147]

### 4.2.4. Wechselwirkungen zwischen der Einwilligung und gesetzlichen Rechtsgrundlagen

Die Verantwortliche müssen **vor** der Erhebung der personenbezogenen Daten entschieden haben, welche Rechtsgrundlage zur Anwendung kommt, und sind verpflichtet diese Rechtsgrundlage zum Zeitpunkt der Erhebung anzugeben.[148] Nach der Ansicht des Europäischen Datenschutzausschusses („EDSA“) kann der **Verantwortliche nicht von der Einwilligung zu einer anderen Rechtsgrundlage**

[139] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020), Rz 94.
[140] *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 9 DSGVO (Stand 1.10.2018, rdb.at) Rz 32.
[141] *Kampert* in Sydow, EU-DSGVO² Art 9 Rz 14.
[142] Art 7 Abs 3 Satz 1 DSGVO.
[143] *Ingold* in Sydow, EU-DSGVO² Art 7 Rz 46; *Heckmann/Paschke* in Ehmann/Selmayr, DS-GVO² Art 7 Rz 93.
[144] Art 7 Abs 3 Satz 3 DSGVO.
[145] Art 7 Abs 3 Satz 2 DSGVO.
[146] *Ingold* in Sydow, EU-DSGVO² Art 7 Rz 48.
[147] Art 7 Abs 3 Satz 4 DSGVO; *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020), Rz 113f.
[148] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020), Rz 123.

**wechseln**.[149] „Es ist beispielsweise nicht gestattet, rückwirkend das berechtigte Interesse als Grundlage für die Rechtfertigung der Verarbeitung zu wählen, wenn Probleme mit der Gültigkeit der Einwilligung aufgetreten sind“ („**Rückgriffsverbot**“).[150]

Ein Verantwortlicher, der sich für die Verarbeitung (oder einen Teil davon) auf eine Einwilligung stützt, muss daher die Verarbeitung (oder deren Teil) beenden, wenn eine betroffene Person ihre Einwilligung widerruft.[151] Laut EDSA wäre es nämlich „gegenüber der betroffenen Person ein in höchstem Maß missbräuchliches Verhalten, ihr zu sagen, dass die Daten auf der Grundlage der Einwilligung verarbeitet werden, wenn tatsächlich eine andere Rechtsgrundlage zugrunde gelegt wird.“ Diese Verhaltensweise wäre mit dem Grundsatz von Treu und Glauben sowie dem Transparenzgrundsatz nicht vereinbar.[152]

### 4.2.5. Wissenschaftliche Forschung

Die DSGVO sieht **Öffnungsklauseln** vor, die dem Unionsgesetzgeber bzw den nationalen Gesetzgebern gestatten, für „[d]ie Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken“ Ausnahmen von bestimmten Betroffenenrechten zu schaffen, wenn diese Verarbeitung „geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person [unterliegen]“ (siehe Punkt 4.2.2.5 oben).[153]

Hingegen wird der Begriff „wissenschaftliche Forschung“ in der DSGVO nicht definiert. Dieser Begriff sollte allerdings „weit ausgelegt werden und […] beispielsweise die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen.“[154] „Die wissenschaftlichen Forschungszwecke sollten auch Studien umfassen, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden.“[155] Damit ist es insbesondere nicht schädlich, wenn die Forschung an einer Einrichtung des privaten Rechts betrieben wird.[156]

Allerdings sollte der Begriff „wissenschaftliche Forschung“ nach der Ansicht des EDSA „nicht über seine allgemeine Bedeutung hinaus ausgeweitet werden“. Die wissenschaftliche Forschung ist „in diesem Kontext als ein Forschungsprojekt [zu verstehen], das in Übereinstimmung mit den maßgeblichen, für

[149] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020), Rz 123 (EN): „In other words, the controller cannot swap from consent to other lawful bases.“
[150] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020), Rz 123.
[151] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020), Rz 122.
[152] In der Literatur wird auch vertreten, dass die Einwilligung „sicherheitshalber“ eingeholt und die Verarbeitung auf mehrere Rechtsgrundlagen parallel gestützt werden kann, wenn dem Grundsatz von Treu und Glauben genüge getan wird. Insbesondere ist die betroffene Person in diesen Fällen über das Bestehen dieser weiteren Rechtsgrundlage sowie über die Tatsache, dass ein jederzeit möglicher Widerruf der Einwilligung nicht unbedingt zur Einstellung der Verarbeitung führen muss, zu informieren; siehe unter anderem *Schulz* in Gola, DS-GVO[2] Art 6 Rz 11ff, *Heckmann/Paschke* in Ehmann/Selmayr, DS-GVO[2] Art 7 Rz 20; *Buchner/Kühling* in Kühling/Buchner, DS-GVO/BDSG[2] Art 7 Rz 17ff; *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 1.10.2018, rdb.at) Rz 15ff mwN.
[153] Art 89 Abs 1 Satz 1, Abs 2 und Abs 3 DSGVO; *Löffler* in Knyrim, DatKomm Art 89 DSGVO (Stand 1.10.2018, rdb.at) Rz 3.
[154] EG 159 Satz 2 DSGVO.
[155] EG 159 Satz 4 DSGVO.
[156] *Feiler/Forgó*, EU-DSGVO (2018) Art 89 Rz 3.

den Sektor relevanten methodischen und ethischen Standards und in Übereinstimmung mit bewährten Verfahren entwickelt wird."[157]

Nationale Regelungen im Bereich der wissenschaftlichen Forschung sind insbesondere in § 7 DSG und im 2. Abschnitt des Forschungsorganisationsgesetzes („FOG")[158] enthalten. FOG regelt in diesem Abschnitt die Rahmenbedingungen für Verarbeitungen zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken sowie zu statistischen Zwecken.[159] Die Regelungen des FOG sind nach herrschender Meinung gegenüber dem DSG als leges speciales anzusehen und gehen diesem vor. Nachdem sich die Regelungsbereiche der beiden Bestimmungen in vielen Bereichen decken, ist § 7 DSG kaum ein sachlicher Anwendungsbereich geblieben.[160, 161]

Ergänzend sei darauf hingewiesen, dass im Zusammenhang mit nationalen Regelungen der Verarbeitung personenbezogenen Daten im Bereich der wissenschaftlichen Forschung zahlreiche Rechtsfragen offen und strittig sind, und in der Literatur Zweifel an der Verfassungs- und Europarechtskonformität mehrerer Bestimmungen des FOG geäußert wurden.[162] Auch (deshalb) ist zu erwarten, dass, gerade auch wegen des durch die Covid-19 Pandemie im allgemeinen Bewusstsein deutlich gewordenen weiter bestehenden Problems des Zugangs zu Forschungsdaten in Österreich de lege ferenda Initiativen gibt (zB durch die Plattform Registerforschung[163]) und/oder geben wird.

#### *4.2.5.1. Gesetzliche Rechtsgrundlagen*

Die Verarbeitung von Daten für Forschungszwecke kann nicht nur auf die Einwilligung, sondern auch auf andere **gesetzliche Erlaubnistatbestände** gestützt werden. Es kommen vor allem öffentliche Aufgabe[164] (siehe Punkt 4.2.2.3 oben), berechtigte Interessen des Verantwortlichen oder eines Dritten[165] (siehe Punkt 4.2.2.4 oben), und bei besonderen Kategorien personenbezogener Daten die

[157] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020), Rz 152.
[158] „Durchführung der Datenschutz-Grundverordnung und ergänzende Regelungen".
[159] § 1 Abs 3 Z 1 FOG; mit Verweis auf Art 4 Z 2 und Art 89 Abs 1 DSGVO.
[160] ErlRV 68 BlgNR XXVI. GP 31, https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00068 /index.shtml (zuletzt abgerufen am 5.5.2021); *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, DSG (2018) § 7 Rz 10; *Knotzer*, Wissenschaftliche Forschung und Datenschutz. Eine kritische Analyse ausgewählter Aspekte der österreichischen Rechtslage, ZTR 2018, 202 (206f); *Roth*, Recht für F&E; Open Innovation, 11/26; *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG) § 7 (Stand 1.1.2020, rdb.at) Rz 12; **aA** *Lachmayer/Souhrada-Kirchmayer*, Datenschutzrecht in der wissenschaftlichen Forschung, zfhr 2018, 153 (V.2), die von einer Wahlmöglichkeit zwischen einer eingeschränkten Datenverarbeitung gemäß § 7 DSG und einer beinahe unbeschränkten Datenverarbeitung gemäß § 2d Abs 2 lit a FOG, bei der sodann die höheren administrativen Anforderungen gemäß § 2d Abs 1 FOG bestehen, ausgehen.
[161] Siehe auch § 2d Abs 7 FOG und § 2a Z 9 FOG.
[162] Siehe etwa *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, DSG (2018) § 7 Rz 9; *Lachmayer/Souhrada-Kirchmayer*, Datenschutzrecht in der wissenschaftlichen Forschung, zfhr 2018, 153 (V.1); *Roth*, Recht für F&E; Open Innovation, 11/38.
[163] https://www.registerforschung.at/.
[164] Art 6 Abs 1 lit e DSGVO.
[165] Art 6 Abs 1 lit f DSGVO; *Artikel-29-Datenschutzgruppe,* Stellungnahme zum Begriff des berechtigten Interesses, WP217, 30.

Verarbeitung zu Archiv-, Forschungs- und statistischen Zwecken[166] (siehe Punkt 4.2.2.5 oben) in Betracht.[167]

Die bei mehreren Erlaubnistatbeständen in der DSGVO verlangte „Grundlage im Recht eines Mitgliedstaats" wird im **FOG** vorgesehen, das umfassende gesetzliche Verarbeitungsgrundlagen enthält. Der Anknüpfungspunkt der Regelung ist die wissenschaftliche Einrichtung. Diese muss im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verfolgen. Es ist allerdings irrelevant, ob die verfolgten Zwecken gemeinnützig oder gewinnorientiert sind und, ob die Tätigkeiten im universitären, betrieblichen oder außeruniversitären Rahmen stattfinden. Damit sind auch Forschung und experimentellen Entwicklung in privatwirtschaftlichen Industriebetrieben umfasst.[168]

Das FOG enthält eine „Generalklausel für sämtliche Verarbeitungen".[169] Nach dieser Ermächtigung zur Datenverarbeitung dürfen wissenschaftliche Einrichtungen für Zwecke des FOG, „insbesondere auf Grundlage des Art. 9 Abs. 2 Buchstabe g, i und j DSGVO",[170] unter Einhaltung des Pflichtenkatalogs der angemessenen Maßnahmen für die Rechte und Freiheiten der betroffenen Person[171] „sämtliche personenbezogene Daten jedenfalls verarbeiten, insbesondere im Rahmen von Big Data, personalisierter Medizin, biomedizinischer Forschung, Biobanken und der Übermittlung an andere wissenschaftliche Einrichtungen und Auftragsverarbeiter", wenn gewisse Maßnahmen zur Datenminimierung und insb. auch zur Datensicherheit gesetzt werden. Als Maßnahmen zur Datenminimierung kommen alternativ, i) Verwendung bereichsspezifische Personenkennzeichen für den Tätigkeitsbereich „Forschung" (bPK-BF-FO) oder andere eindeutige Identifikatoren zur Zuordnung herangezogen werden, ii) Verarbeitung in pseudonymisierter Form, iii) Veröffentlichungen nicht oder nur in anonymisierter oder pseudonymisierter Form oder ohne Namen, Adressen oder Foto erfolgen oder iv) Verarbeitung ausschließlich zum Zweck der Anonymisierung oder Pseudonymisierung und keine Offenlegung direkt personenbezogener Daten an Dritte (siehe Punkt 4.1.2.4 oben).[172] Es ist auch die Verarbeitung besonderer Kategorien personenbezogener Daten umfasst.

Diese Bestimmung ist unionskonform auszulegen, daher sind die in dem jeweils einschlägigen Erlaubnistatbestand der DSGVO allenfalls vorgesehenen materiellen Voraussetzungen einzuhalten. Die Verarbeitung muss daher insbesondere für den jeweiligen Zweck erforderlich sein und allenfalls eine hinreichend spezifische Rechtnorm existieren, die die materiellen Voraussetzungen im nationalen

[166] Art 9 Abs 2 lit j DSGVO.
[167] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020), Rz 153.
[168] § 2b Z 12 FOG, mit Verweis auf Art 89 Abs 1 DSGVO; *Roth*, Recht für F&E; Open Innovation, 11/28ff.
[169] BGBl I 2018/31, Anhang 4 zum FOG.
[170] Gemeint daher (wohl) neben für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Art 89 Abs 1 DSGVO und Art 9 Abs 2 lit j DSGVO, auch aus Gründen eines erheblichen öffentlichen Interesses gemäß Art 9 Abs 2 lit g DSGVO und aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Art 9 Abs 2 lit i DSGVO.
[171] § 2d Abs 1 FOG; *Knotzer*, Wissenschaftliche Forschung und Datenschutz. Eine kritische Analyse ausgewählter Aspekte der österreichischen Rechtslage, ZTR 2018, 202 (207, FN 47): „Bei allen Datenverarbeitungen auf Grundlage des FOG sind die in § 2d Abs 1 Z 1 bis 4 FOG zu beachten. Wird eine Verarbeitung auf Basis des § 2d Abs 2 FOG durchgeführt, sind zusätzlich die Pflichten gemäß § 2d Abs 1 Z 5 FOG zu beachten".
[172] § 2d Abs 2 Satz 3 Z 1 FOG; *Roth*, Recht für F&E; Open Innovation, 11/36ff; *Knotzer*, Wissenschaftliche Forschung und Datenschutz. Eine kritische Analyse ausgewählter Aspekte der österreichischen Rechtslage, ZTR 2018, 202 (207); *Lachmayer/Souhrada-Kirchmayer*, Datenschutzrecht in der wissenschaftlichen Forschung, zfhr 2018, 153 (V.1).

Recht konkretisiert. Vor Stützung der Verarbeitung auf diese Ermächtigung ist daher eine eingehende Prüfung für den jeweiligen Einzelfall erforderlich.[173]

Ferner enthält FOG eigene spezielle Rechtsgrundlagen für die Registerforschung,[174]Abgleich von Bilddaten[175], Repositories[176] und Wissens- und Technologietransfer[177].[178] Diese Rechtsgrundlagen sind jeweils mit eigenen Rechtsunsicherheiten behaftet.

#### *4.2.5.2. Einwilligung*

In der **DSGVO** wird anerkannt, dass „der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten [oftmals] nicht vollständig angegeben werden [kann].“[179] Die **Einwilligung** darf daher „für bestimmte Bereiche wissenschaftlicher Forschung“ eingeholt werden, „wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht“ („**Bereichseinwilligung**“).[180]

Laut EDSA ermöglicht dieser **flexible Ansatz** lediglich, dass in den Fällen, „in denen die Zwecke für die Datenverarbeitung im Rahmen eines wissenschaftlichen Forschungsprojektes am Anfang nicht angegeben werden können, […] **ausnahmsweise** […] der Zweck allgemeiner beschrieben werden kann.“[181]

In diesen Fällen „muss der Verantwortliche anderweitig sicherstellen, dass dem Wesensgehalt der Anforderungen an die Einwilligung am besten gedient wird, beispielsweise indem betroffenen Personen in allgemein beschriebene Forschungszwecke und spezielle Phasen des Forschungsprojekts einwilligen können, von denen bereits am Anfang bekannt ist, dass sie stattfinden werden. Mit dem Fortschreiten der Forschung können Einwilligungen in die nachfolgenden Schritte des Projekts eingeholt werden, bevor die nächste Phase beginnt.“[182]

Der Verantwortliche hat in solchen Fällen zusätzliche geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person vorzusehen. „Sobald der Forschungszweck ohne die Verarbeitung personenbezogener Daten erreicht werden kann, ist die Anonymisierung die bevorzugte Lösung“ (siehe Punkt 4.1.2.4 oben).[183]

---

[173] Art 9 Abs 2 lit g, i und j DSGVO; *Roth*, Recht für F&E; Open Innovation, 11/38.
[174] § 2d Abs 2 Z 3 FOG.
[175] § 2d Abs 8 FOG.
[176] § 2 f Abs 1 FOG.
[177] § 2i Abs 1 FOG.
[178] *Knotzer*, Wissenschaftliche Forschung und Datenschutz. Eine kritische Analyse ausgewählter Aspekte der österreichischen Rechtslage, ZTR 2018, 202 (207ff).
[179] EG 33 Satz 1 DSGVO.
[180] EG 33 Satz 2 DSGVO.
[181] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020), Rz 154ff; siehe auch EG 33 Satz 3 DSGVO.
[182] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020), Rz 158, 160ff; siehe auch *Schaar*, Anpassung von Einwilligungserklärungen für wissenschaftlichen Forschungsprojekte, ZD 2017, 213.
[183] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020), Rz 159; Art 89 Abs 1 Satz 2 ff DSGVO: „Mit diesen Garantien wird sichergestellt, dass technische und organisatorische

Ergänzend ist darauf hinzuweisen, dass die „Einwilligung in die Verwendung personenbezogener Daten von anderen Einwilligungsanforderungen [zu unterscheiden ist], die als ethischer Standard oder als verfahrensrechtliche Verpflichtung dienen. Ein Beispiel für eine solche verfahrensrechtliche Verpflichtung, bei der die Verarbeitung nicht auf einer Einwilligung beruht, sondern auf einer anderen Rechtsgrundlage, kann in der Verordnung über Klinische Prüfungen gefunden werden.[184]

Des Weiteren enthält FOG das Konzept des "broad consent" als gesetzliche Einwilligung.[185] Laut mehreren Literaturmeinungen ist diese Regelung (wohl) mit der DSGVO unvereinbar, daher sollte die Verarbeitung personenbezogener Daten, wenn möglich, aus Vorsichtsgründen bis auf Weiteres weiterhin nicht auf „broad consent“ gemäß FOG gestützt werden.[186]

### 4.2.6. Weiterverarbeitung personenbezogener Daten für andere Zwecke („Sekundärnutzung“)

Die DSGVO enthält eine normative Durchbrechung des Grundsatzes der (strengen) Zweckbindung und regelt die **Rechtmäßigkeit der Weiterverwendung von für ursprüngliche andere Zwecke erhobene Daten** (siehe Punkt 4.2.1 oben).[187] Es sind dabei zwei Konstellationen zu unterscheiden.

Eine Datenverarbeitung für andere, nicht mit dem ursprünglichen Zweck vereinbare Zwecke („Zweckändernde Weiterverarbeitung **für inkompatible Zwecke**“) ist dann zulässig, wenn eine (den neuen bzw geänderten Zweck abdeckende) Einwilligung der betroffenen Person vorliegt oder die Datenverarbeitung auf Unionsrecht oder nationalem Recht der MS beruht.[188]

Hingegen ist eine Datenverarbeitung für andere, aber mit dem ursprünglichen Zweck vereinbare Zwecke („Zweckändernde Weiterverarbeitung **für kompatible Zwecke**“) dann zulässig, wenn der „Kompatibilitätstest“ eine Vereinbarkeit ergibt.[189] Die Kriterien für den Kompatibilitätstest sind in der DSGVO demonstrativ aufgezählt (zB Verbindung zwischen den Zwecken, Zusammenhang, in dem die personenbezogenen Daten erhoben wurden).[190] In diesem Fall bedarf es nach hier vertretener Ansicht für die Weiterverarbeitung keiner zusätzlichen oder neuen Rechtsgrundlage.[191]

---

Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Zu diesen Maßnahmen kann die Pseudonymisierung gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen. In allen Fällen, in denen diese Zwecke durch die Weiterverarbeitung, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, erfüllt werden können, werden diese Zwecke auf diese Weise erfüllt.“

[184] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, 4.5.2020), Rz 153; EG 161 DSGVO.

[185] § 2d Abs 3 FOG; ErlRV 68 BlgNR XXVI. GP 35; *Knotzer*, Wissenschaftliche Forschung und Datenschutz. Eine kritische Analyse ausgewählter Aspekte der österreichischen Rechtslage, ZTR 2018, 202 (208).

[186] *Lachmayer/Souhrada-Kirchmayer*, Datenschutzrecht in der wissenschaftlichen Forschung, zfhr 2018, 153 (V.4); *Roth*, Recht für F&E; Open Innovation, 11/44.

[187] *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 58f.

[188] *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 60, 65; EG 50 Satz 7 DSGVO.

[189] *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 66.

[190] Art 6 Abs 4 DSGVO; EG 50 Satz 6 DSGVO; *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 61ff.

[191] EG 50 Satz 2 DSGVO; *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 62, 67.

Des Weiteren enthält die DSGVO eine **gesetzliche Fiktion**, wonach die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für **wissenschaftliche** oder historische **Forschungszwecke** oder für statistische Zwecke **nicht unvereinbar mit den ursprünglichen Zwecken** ist.[192] Diese Einschränkung des Zweckbindungsgrundsatzes ermöglicht Zweckänderungen bei Verarbeitung in der wissenschaftlichen Forschung (siehe Punkt 4.2.5 oben).[193]

Ergänzend wird im **FOG** klargestellt, dass die Weiterverarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke auch keine unzulässigen Zwecke im Sinne des verwaltungsrechtlichen Tatbestands „Verletzung des Datengeheimnisses" gemäß § 62 Abs. 1 Z 2 DSG darstellen.[194]

Dabei ist allerdings zu beachten, dass die Weiterverarbeitung personenbezogener Daten zu den privilegierten Zwecken erst dann erfolgen darf, „wenn der Verantwortliche geprüft hat, ob es möglich ist, diese Zwecke durch die Verarbeitung von personenbezogenen Daten, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, zu erfüllen" (siehe Punkt 4.1.2.4 oben).[195] Können wissenschaftlichen Forschungszwecke unter Nutzung anonymer Daten erreicht werden, dürfen daher bloß solche Daten verarbeitet werden.[196] Dies entspricht dem Grundsatz der Speicherbegrenzung. Dieser ist vor der Weiterverarbeitung aktiv zu prüfen.[197]

## 4.3. Kollaboratives Arbeiten mit personenbezogenen Daten

### 4.3.1. Einleitung

Die Europäische Kommission hält fest, dass der eigentliche Wert von Daten in ihrer Nutzung und Weiterverwendung liegt.[198] Damit die Forschung und die Industrie von einem kollaborativen Daten-, Informations- und Wissensmanagement profitieren können, muss dieses Kollaboration zwischen verschiedenen Stakeholdern fördern.[199]

Für die kollaborative Arbeit mit personenbezogenen (Forschungs-)Daten ist aufgrund der Vielzahl von Beteiligten eine zentral koordinierte Planung des Forschungsdatenmanagements und aller Workflows unersetzlich. Die Grundregeln für den Umgang mit den im Forschungsprojekt anfallenden bzw. zu entwickelnden Daten (zB grundlegende Verantwortlichkeiten) sollten von Beginn an in einer Projekt-Richtlinie oder einem Datenmanagementplan festgelegt werden, die unter anderem die Vorgaben zur

[192] Art 5 Abs 1 lit b DSGVO, mit Verweis auf Art 89 Abs 1 DSGVO; *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 64, 66 (mwN)
[193] *Feiler/Forgó*, EU-DSGVO (2018) Art 89 Rz 1.
[194] § 2 Abs 4 FOG mit Verweisen auf Art 5 Abs 1 lit b DSGVO und Art 89 Abs 1 DSGVO.
[195] EG 156 Satz 3 DSGVO.
[196] *Löffler* in Knyrim, DatKomm Art 89 DSGVO (Stand 1.10.2018, rdb.at) Rz 41.
[197] *Feiler/Forgó*, EU-DSGVO (2018) Art 89 Rz 8.
[198] *EK*, Eine europäische Datenstrategie, Mitteilung COM(2020) 66 final, 2f.
[199] Siehe zum kollaborativen Arbeiten https://www.forschungsdaten.info/themen/organisieren-und-aufbereiten/kollaboratives-arbeiten/ (zuletzt abgerufen am 7.5.2021).

Einhaltung der datenschutzrechtlichen Anforderungen enthält.[200, 201] Nachstehend werden die rechtlichen Rahmenbedingungen beschrieben.

### 4.3.2. Datenschutzrechtliche Rollen

Die DSGVO sieht für die datenschutzrechtliche Rollenverteilung[202] in Konstellationen mit mehreren Akteuren drei verschiedene Möglichkeiten vor, die ganz unterschiedliche Rechtsfolgen nach sich ziehen. Wenn die Daten von Verantwortlichen an einen Dritten weitergegeben werden, so kann dieser Auftragsverarbeiter, ein selbständiger Verantwortlicher oder ein gemeinsam Verantwortlicher sein.[203]

Ein **Auftragsverarbeiter** ist „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet".[204] Hingegen ist ein **Verantwortlicher** „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und (wesentliche) Mittel der Verarbeitung von personenbezogenen Daten entscheidet".[205] „Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie **gemeinsam Verantwortliche**."[206]

„Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftragsverarbeiter bedarf es einer klaren Zuteilung der Verantwortlichkeiten."[207]

### 4.3.3. Gemeinsame Datenverarbeitung

Die **Verarbeitung** personenbezogener Daten im Sinne der DSGVO umfasst etwa „das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine

[200] https://www.forschungsdaten.info/themen/organisieren-und-aufbereiten/kollaboratives-arbeiten/planung-der-gemeinsamen-arbeit-mit-daten/ (zuletzt abgerufen am 7.5.2021).
[201] Art 24 Abs 2 DSGVO verpflichtet zur „Anwendung geeigneter Datenschutzvorkehrungen" (in der engl Sprachfassung: „implementation of appropriate data protection policies"); *Hötzendorfer/Kastelitz/Tschohl* in Knyrim, DatKomm Art 24 DSGVO (Stand 1.10.2018, rdb.at) Rz 31ff; *Feiler/Forgó*, EU-DSGVO (2018) Art 24 Rz 7.
[202] Siehe auch Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Stand: 02 September 2020), https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_de (zuletzt abgerufen am 7.5.2021); *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", WP 169 (16. Februar 2010).
[203] BVwG W214 2196366/20182 = jusIT 2019/56, 162 (163) (*Jahnel*); *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 3.
[204] Art 4 Z 8 DSGVO.
[205] Art 4 Z 7 DSGVO: „sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden".
[206] Art 26 Abs 1 Satz 1 DSGVO.
[207] EG 79 DSGVO.

andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“ der Daten (siehe Punkt 4.1.2.2 oben).[208]

„Offenlegung durch Übermittlung, Verbreitung, oder andere Formen der Bereitstellung“, ist ein Begriff, der alle Vorgänge beschreibt, durch die der Verantwortliche personenbezogene Daten anderen Stellen in einer Weise zugänglich macht, die es diesen erlauben, vom Informationsgehalt Kenntnis zu haben.[209] Eine Unterform der Offenlegung ist die **Übermittlung**, die Mitteilung an individuell bestimmte Adressaten, etwa einen anderen (gemeinsam) Verantwortlichen.[210]

Die gemeinsam Verantwortlichen legen gemeinsam die Zwecke der und die Mittel der gemeinsamen Datenverarbeitung fest (zB eines Data Poolings).[211] Zu bedenken ist allerdings, dass **eine gemeinsame Verantwortlichkeit weder eine wechselseitige Datenübermittlung noch einen Zugang zu den Daten für alle Verantwortlichen voraussetzt**.[212] Schon alleine der Umstand, dass eine kollaborative Entscheidung über das „Warum“ (Zwecke) und das „Wie“ (Mittel) einer Verarbeitung stattfindet, führt zu einer gemeinsamen Verantwortlichkeit.[213] Eine faktische Entscheidungsmacht ist dafür ausreichend.[214]

Die DSGVO knüpft an gemeinsame Verantwortlichkeit konkrete Rechtsfolgen. Die gemeinsam Verantwortlichen müssen eine transparente **Vereinbarung** abschließen, in der festgelegt wird, wer von ihnen welche Verpflichtungen aus der DSGVO erfüllt, insbesondere wer Rechte der betroffenen Person wahrnimmt und wer welchen Informationspflichten nachkommt („*Joint Controller Agreement*“).[215] Diese muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln.[216] Zu Beweiszwecken sollte die Vereinbarung in schriftlicher Form abgeschlossen werden.[217] Das (datenschutzrechtlich) Wesentliche dieser Vereinbarung muss den betroffenen Personen offengelegt werden.[218]

Die Vereinbarung über die gemeinsame Verantwortlichkeit kann auch eine Anlaufstelle für die betroffenen Personen vorgesehen werden.[219] Ungeachtet dieser Vereinbarung können die betroffenen Personen ihre Rechte gegenüber jedem der gemeinsam Verantwortlichen geltend machen.[220]

---

[208] Art 4 Z 2 DSGVO.
[209] *Hödl* in Knyrim, DatKomm Art 4 DSGVO (Stand 1.12.2018, rdb.at) Rz 35.
[210] *Hödl* in Knyrim, DatKomm Art 4 DSGVO (Stand 1.12.2018, rdb.at) Rz 36.
[211] Art 26 Abs 1 Satz 1 DSGVO; Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Stand: 02 September 2020), 21: Example: Research project by institutes und Example: Clinical Trials; siehe etwa auch https://www.forschungsdaten.info/themen/organisieren-und-aufbereiten/kollaboratives-arbeiten/gemeinsamer-datenzugriff-und-data-sharing/ (zuletzt abgerufen am 7.5.2021).
[212] EuGH 10.7.2018, C-25/17 (*Zeugen Jehovas*) Rz 69; EuGH 5.6.2018, C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) Rz 38; *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 3.
[213] *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 3.
[214] *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 13ff.
[215] Art 26 Abs 1 DSGVO; *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 25ff.
[216] Art 26 Abs 2 Satz 1 DSGVO; *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 32ff.
[217] *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 35f.
[218] Art 26 Abs 2 Satz 2 DSGVO; *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 37ff.
[219] Art 26 Abs 2 Satz 3 DSGVO; *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 45ff.
[220] Art 26 Abs 3 DSGVO; *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 48ff.

Darüber hinaus müssen die anderen gemeinsam Verantwortlichen im Verarbeitungsverzeichnis dokumentiert und gegenüber den betroffenen Personen offengelegt werden.[221]

### 4.3.4. Outsourcing

Mit dem Begriff Outsourcing wird eine Vielzahl von Tätigkeiten und Vertragsgegenständen beschrieben. Datenschutzrechtlich relevant ist die Übermittlung personenbezogener Daten an einen (oder mehrere) Dienstleister.

In diesem Fall verarbeitet eine vom Verantwortlichen verschiedene Stellen personenbezogene Daten lediglich in dessen Auftrag, und ist daher als **Auftragsverarbeiter** zu qualifizieren.[222] Der Auftragsverarbeiter darf diese Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen verarbeiten.[223]

Der Auftragsverarbeiter ist (datenschutzrechtlich) der Sphäre des Verantwortlichen zuzuordnen („innerer Kreis"), daher bedarf die Datenübermittlung von einem Verantwortlichen an einen Auftragsverarbeiter keine eigene Rechtsgrundlage (siehe Punkt 4.2 oben).[224] Die Voraussetzung für die Legitimität einer Datenübermittlung ist vielmehr der Abschluss einer **Auftragsverarbeitungsvereinbarung**.[225]

Die Auftragsverarbeitungsvereinbarung muss schriftlich abgefasst sein, was auch in einem elektronischen Format erfolgen kann, eine Bindungswirkung zwischen den Parteien hergestellt und gesetzlich determinierten Mindestinhalt aufweisen (zB Gegenstand und Dauer, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, die Kategorien betroffener Personen, geeignete technische und organisatorische Maßnahmen, und Bedingungen für die Inanspruchnahme von Sub-Auftragsverarbeiter).[226]

Sind Auftragsverarbeiter einem Drittland[227] ansässig, sind zudem die Sonderbestimmungen für den internationalen Datenverkehr zu beachten.[228] Damit soll sichergestellt werden, dass das durch die DSGVO gewährleistete Schutzniveau durch Datenübermittlungen in Drittstaaten nicht untergraben wird.[229] Besteht für das Zielland kein Angemessenheitsbeschluss, können geeignete Garantien etwa durch Vereinbarung von Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern vorgesehen werden.[230]

---

[221] *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 2.
[222] *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 3.
[223] Art 29 DSGVO; Art 28 Abs 3 Satz 2 lit a DSGVO.
[224] *Bogendorfer* in Knyrim, DatKomm Art 28 DSGVO (Stand 1.10.2018, rdb.at) Rz 23ff (28).
[225] *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 3.
[226] Art 28 Abs 3 Satz 1 und Satz 2, Abs 9 DSGVO; *Bogendorfer* in Knyrim, DatKomm Art 28 DSGVO (Stand 1.10.2018, rdb.at) Rz 54ff.
[227] Darunter sind alle Staaten, außer jenen der EU und des EWR zu verstehen, *Feiler/Forgó*, EU-DSGVO (2018) Art 44 Rz 2.
[228] Art 44 ff DSGVO; *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 3.
[229] *Bogendorfer* in Knyrim, DatKomm Art 28 DSGVO (Stand 1.10.2018, rdb.at) Rz 29f mwN.
[230] Art 46 Abs 2 lit c und lit d DSGVO; siehe *DSB*, Internationaler Datenverkehr, https://www.dsb.gv.at/aufgaben-taetigkeiten/internationaler-datenverkehr.html (zuletzt abgerufen am 7.5.2021); *EK*, Standard contractual clauses for data transfers between EU and non-EU countries,

Typische Auftragsverarbeitungen sind etwa Outsourcing personenbezogener Datenverarbeitungen im Rahmen von Cloud-Computing, die Auslagerung der Backup-Sicherungsspeicherung oder Dienstleistungen von Rechenzentren.[231]

### 4.3.5. Data Sharing

Liegt weder gemeinsame Verantwortlichkeit noch Auftragsverarbeitung vor und werden personenbezogene Daten einer betroffenen Person einem Dritten[232] zu einer Verarbeitung übermittelt, bei der der Dritte über den Zweck und die (wesentlichen) Mittel der Verarbeitung entscheiden, ist dieser ein **weiterer selbständiger Verantwortlicher**.[233]

Da es sich dabei um datenschutzrechtlich eigenständige Akteure, die die übermittelten Daten unabhängig voneinander jeweils für ihre eigenen Zwecke verarbeiten („Verarbeitungskette"), bedarf sowohl die i) Übermittlung personenbezogener Daten von einem Verantwortlichen an den weiteren als auch die ii) Verarbeitung durch den weiteren Verantwortlichen bedürfen eine (eigene) Rechtsgrundlage (siehe Punkt 4.2 oben)."[234]

Eine Vereinbarung zwischen dem übermittelnden und dem empfangenden Verantwortlichen („*Data Sharing Agreement*") ist zwar nicht gesetzlich vorgeschrieben, deren Abschluss empfiehlt sich allerdings und stellt eine gute Praxis – insbesondere bei regelmäßigem bzw systematischem Datenaustausch – dar. Diese Vereinbarungen legt den Zweck der Datenübermittlung fest, regelt, was mit den Daten in jeder Phase der Übermittlung geschieht, setzen Standards für die Datenverarbeitung und hilft allen der beteiligten Verantwortlichen, sich über ihre Rollen und Verantwortlichkeiten klar zu werden.[235]

Nach **FOG** sind zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken Übermittlungen personenbezogener Daten an wissenschaftliche Einrichtungen (zB im Ausland ansässige Tochtergesellschaften oder sonstige Unternehmen) und Wissens- und Technologietransfer in Mitgliedstaaten der Europäischen Union zulässig, soweit die Vorgaben des 2. Abschnitts des FOG auch von diesen Empfängern als weiteren selbständigen Verantwortlichen beachtet werden.[236]

---

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_de (zuletzt abgerufen am 7.5.2021).

[231] *Bogendorfer* in Knyrim, DatKomm Art 28 DSGVO (Stand 1.10.2018, rdb.at) Rz 10.

[232] Art 4 Z 10 DSGVO: „Dritter" ist „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten".

[233] *Bogendorfer* in Knyrim, DatKomm Art 28 DSGVO (Stand 1.10.2018, rdb.at) Rz 19.

[234] *Bogendorfer* in Knyrim, DatKomm Art 28 DSGVO (Stand 1.10.2018, rdb.at) Rz 19; *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 3.

[235] *ICO*, Data Sharing Code of Practice (17.12.2020 - 1.0.123), 21, 26ff; https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/data-sharing-covered-by-the-code/ (zuletzt abgerufen am 7.5.2021).

[236] § 2j FOG; *Knotzer*, Wissenschaftliche Forschung und Datenschutz. Eine kritische Analyse ausgewählter Aspekte der österreichischen Rechtslage, ZTR 2018, 202 (208).

Bei Übermittlung an einen Verantwortlichen in ein Drittland sind (wiederum) die Sonderbestimmungen für den internationalen Datenverkehr zu beachten.[237] Besteht für das Zielland kein Angemessenheitsbeschluss, können geeignete Garantien etwa durch Vereinbarung von Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer an Verantwortliche in Drittländern vorgesehen werden.[238]

## 4.4. Governance von nicht-personenbezogenen Daten

### 4.4.1. Einleitung

Rohdaten, insbesondere maschinengenerierte Daten (zB in vernetzten Geräten oder Steuerungssystemen), die im Zusammenhang mit der Nutzung generiert werden, sind als wirtschaftliches Gut von wesentlicher Bedeutung.[239] Entscheidend ist die Frage der **Datenhoheit**, d.h. der Berechtigung, von dritter Seite generierte bzw übermittelte Daten nutzen zu dürfen.[240] Es besteht jedoch derzeit weder auf nationaler noch auf Unionsebene eine umfassende Regelung für die Nutzung von Rohdaten, bei denen es sich nicht um personenbezogene Daten handelt.[241]

Ein Referenzmodell für ein kollaboratives Daten-, Informations- und Wissensmanagement sollte sich aus den geschilderten Gründen nicht auf personenbezogene Daten beschränken, sondern auch die Grundregeln für die kollaborative Arbeit mit nicht-personenbezogenen (Forschungs-)Daten aufstellen. In einer Projekt-Richtlinie oder einem Datenmanagementplan können unter anderem das geistige Eigentum an den anfallenden bzw zu entwickelnden Daten, Datenbanken oder Computerprogrammen, diesbezügliche Lizenzen, Vertraulichkeitsvereinbarungen sowie der Umgang mit den Daten am Projektende, wie Datenveröffentlichung oder -vernichtung, geregelt werden.[242] Nachstehend werden die rechtlichen Rahmenbedingungen beschrieben.

### 4.4.2. Dateneigentum

Bei der Zuordnung von nicht-personenbezogenen Daten herrscht in der Praxis zum Teil die „normative Kraft des Faktischen“, wenn die Hersteller oder Diensteanbieter die Kontrolle über Daten ausüben und

[237] Art 44 ff DSGVO; *Horn* in Knyrim, DatKomm Art 26 DSGVO (Stand 1.10.2018, rdb.at) Rz 3; *Bogendorfer* in Knyrim, DatKomm Art 28 DSGVO (Stand 1.10.2018, rdb.at) Rz 29f mwN.
[238] Art 46 Abs 2 lit c und lit d DSGVO; siehe *DSB*, Internationaler Datenverkehr, https://www.dsb.gv.at/aufgaben-taetigkeiten/internationaler-datenverkehr.html (zuletzt abgerufen am 7.5.2021); *EK*, Standard contractual clauses for data transfers between EU and non-EU countries, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_de (zuletzt abgerufen am 7.5.2021).
[239] *Rungg/Buchroithner*, Data Ownership in Binder Grösswang, Digital Law (2. Aufl, 2020), 138.
[240] *Ensthaler/Haase*, Datenhoheit und Datenschutz im Zusammenhang mit Smart Services (2017), 3, https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smart%20service%20welt_positionspapier_recht.pdf?__blob=publicationFile&v=11 (zuletzt abgerufen am 8.5..2021).
[241] *Rungg/Buchroithner*, Data Ownership in Binder Grösswang, Digital Law (2. Aufl, 2020), 146.
[242] https://www.forschungsdaten.info/themen/organisieren-und-aufbereiten/kollaboratives-arbeiten/planung-der-gemeinsamen-arbeit-mit-daten/ (zuletzt abgerufen am 7.5.2021).

zu „Eigentümern“ der von ihren Maschinen oder Prozessen erzeugten Daten werden.[243] Es stellt sich daher die Frage, ob jenseits des bestehenden sondergesetzlichen Schutzes des geistigen Eigentums und der Geschäftsgeheimnisse ein eigenes **zivilrechtliches Schutzinstrument** in Form eines „Dateneigentums“ besteht.[244, 245] Das ist im Ergebnis zu verneinen.

Der Begriff „Sache“ wird in österreichischen Zivilrecht als „[a]lles, was von der Person unterschieden ist, und zum Gebrauche der Menschen dient“, definiert.[246] Entsprechend dieser Definition, die keine Körperlichkeit voraussetzt, erkennt die herrschende Meinung **Daten** zwar als (unkörperliche) Rechtssache an, diese werden sachenrechtlich jedoch per se nicht geschützt. Vielmehr müsse ein Schutz spezialgesetzlich, beispielsweise im Urheber- oder im Datenschutzrecht, angeordnet werden (siehe Punkt 4.1.2.2 oben und Punkt 4.1.3 oben).[247]

Die Rohdaten sind zivilrechtlich somit nicht geschützt und ihr Handel wird durch Verträge organisiert (siehe Punkt 4.4.4 unten).[248] „Die Marktteilnehmer, die die Kontrolle über die Daten haben“, können daher, „Lücken in der Rechtslage oder die […] rechtlichen Unklarheiten ausnutzen, und den Nutzern unfaire Standardvertragsbedingungen aufzwingen oder zu technischen Mitteln wie proprietären Formaten oder Verschlüsselung greifen.“[249]

### 4.4.3. Free-Flow-of-Data Verordnung

Anders als die DSGVO regelt die Free-Flow-of-Data-VO den freien Verkehr von Daten nicht-personenbezogener Daten in der EU, der insbesondere maschinengenerierte Daten betrifft (siehe Punkt 4.1.2.1 oben).[250] Der sachliche Anwendungsbereich ist zusätzlich auf die Verarbeitung elektronischer Daten beschränkt.[251]

Die Kernanliegen der Verordnung sind i) **Beseitigung von Datenlokalisierungsauflagen** innerhalb der Europäischen Union („Prinzip des freien Datenflusses nicht-personenbezogener Daten“), ii) Sicherstellung der Datenverfügbarkeit für zuständige Behörden, und iii)

[243] *Rungg/Buchroithner*, Data Ownership in Binder Grösswang, Digital Law (2. Aufl, 2020), 146.
[244] *Forgó*, Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen in Forgó/Zöchling-Jud, Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter, 20. ÖJT Band II/1, 353.
[245] Siehe etwa *Härting*, Acht Thesen zum “Dateneigentum” (17.2.2016), https://www.cr-online.de/blog/2016/02/17/acht-thesen-zum-dateneigentum/ (zuletzt abgerufen am 7.5.2021).
[246] § 285 ABGB.
[247] *Forgó*, Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen in Forgó/Zöchling-Jud, Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter, 20. ÖJT Band II/1, 354ff; *Rungg/Buchroithner*, Data Ownership in Binder Grösswang, Digital Law (2. Aufl, 2020), 155.
[248] *Forgó*, Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen in Forgó/Zöchling-Jud, Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter, 20. ÖJT Band II/1, 362.
[249] *EK*, Aufbau einer europäischen Datenwirtschaft, Mitteilung COM(2017) 9 final, 2f, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=COM%3A2017%3A9%3AFIN (zuletzt abgerufen am 8.5.2021); *Forgó*, Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen in Forgó/Zöchling-Jud, Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter, 20. ÖJT Band II/1, 362.
[250] *Rungg/Mazzia*, Rechtsgrundlagen des neuen europäischen Datenverkehrs, ZIIR 2019, 267.
[251] Art 2 Abs 1 Free-Flow-of-Data-VO.

Selbstregulierungsmaßnahmen (Codes of Conducts) zum leichteren Wechsel zwischen Cloud Service Provider und/oder Datenübertragung.[252]

Die Free-Flow-of-Data-VO ist seit 28.5.2019 anwendbar. Bestehende Datenlokalisierungsauflagen sind bis 30.5.2021 aufzuheben, es sei denn, sie sind aus Gründen der öffentlichen Sicherheit unter Achtung des Grundsatzes der Verhältnismäßigkeit gerechtfertigt.[253] In der österreichischen Rechtsordnung finden sich nach Ansicht der Europäischen Kommission Datenlokalisierungsauflagen etwa in den Anforderungen an die Verarbeitung von Gesundheitsdaten und genetischen Daten im Gesundheitstelematikgesetz.[254]

### 4.4.4. Vertragliche Zuordnung von Daten

Eine rechtliche Grundlage für die Zuordnung von nicht-personenbezogenen Daten können vor allem vertragliche Regelungen schaffen („***Datennutzungsvereinbarungen***“).[255]

Einschlägige Verträge enthalten zum Teil umfangreiche Regelungen zur Zuordnung und der Verwendung der Daten für bestimmte, regelmäßig detailliert beschriebene Zwecke. Als besonders problematisch gelten bei derartigen vertraglichen Zuordnungen die Fragen, die sich in Bezug auf die Beherrschbarkeit des Vertragsgegenstands (zB durch proprietäre Formate oder Verschlüsselung) und die allfälligen gewährleistungsrechtlichen Ansprüche ergeben.[256]

Bei den Vertragsregeln handelt es sich regelmäßig um allgemeine Geschäftsbedingungen, die der Einbeziehungs-, Geltungs- und Inhaltskontrolle unterliegen.[257] Um der Inhaltskontrolle standzuhalten, sollte für das Nutzungsrecht des Herstellers oder des Diensteanbieters an den Daten eine Gegenleistung an den Nutzer, der die Daten generiert, vereinbart werden, soweit die Datennutzung nicht in spürbarem Ausmaß zu dessen Vorteil erfolgt (zB Wartung einer Maschine, Sicherheitsupdate

[252] https://www.bmdw.gv.at/Themen/Digitalisierung/Digitales-Oesterreich/E-Government-International/EK-Legisativvorschlaege.html (zuletzt abgerufen am 29.4.2021); *EK*, Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, Mitteilung COM(2019) 250 final, 2f; *Staudegger*, Die VO (EU) 2018/1807: Ein Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, jusIT 2019/2, Punkt 4.

[253] Art 4 Abs 1 und Abs 3 Free-Flow-of-Data-VO.

[254] §§ 6, 14 und 20 Gesundheitstelematikgesetz. Weitere Datenlokalisierungsauflagen wurden im UGB, BAO, WAG 2007, Bundesgesetz über die Bundesrechenzentrum GmbH und Bundesgesetz, mit dem IKT - Lösungen und IT -Verfahren bundesweit konsolidiert werden, identifiziert; siehe dazu Commission Staff Working Document Impact Assessment SWD(2017) 304 final, Part 2/2, 70f https://eur-lex.europa.eu/resource.html?uri=cellar:51c9c47e-985c-11e7-b92d-01aa75ed71a1.0001.02/DOC_2&format=PDF (zuletzt abgerufen am 9.5.2021).

[255] *EK*, Leitfaden für die gemeinsame Nutzung von Daten des Privatsektors in der europäischen Datenwirtschaft, SWD(2018) 125 final, 5, https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:52018SC0125 (zuletzt abgeruden am 9.5.2021); *Rungg/Buchroithner*, Data Ownership in Binder Grösswang, Digital Law (2. Aufl, 2020), 154.

[256] *Rungg/Buchroithner*, Data Ownership in Binder Grösswang, Digital Law (2. Aufl, 2020), 154; zu weiteren Möglichen Inhalten von Datennutzungsvereinbarungen siehe *EK*, Leitfaden für die gemeinsame Nutzung von Daten des Privatsektors in der europäischen Datenwirtschaft, SWD(2018) 125 final, 6f.

[257] *Ensthaler/Haase*, Datenhoheit und Datenschutz im Zusammenhang mit Smart Services (2017), 3f; *Bollenberger/P. Bydlinski* in KBB[6] § 864a Rz 1f und § 879 Rz 1, 22ff.

einer App). Die Gegenleistung muss allerdings nicht in Geld, sondern kann etwa in der Partizipation an bestimmten Verwertungsergebnissen bestehen.[258]

Nutzen mehrere Unternehmen gemeinsam Daten, sollte festgelegt werden, wie jede Partei ohne weitere Zustimmung einer anderen Partei(en) Daten verwerten darf. So kann sich die Eigennutzung etwa auch auf die mit den jeweils eigenen Daten vermengten Daten der anderen Unternehmen beziehen.[259]

### 4.4.5. Rechtsrahmen von Open Data

Die Verfügbarkeit von Daten wird zu einem immer bedeutenderen Wirtschaftsfaktor und ist Teil einer modernen Infrastruktur.[260] Die freie Verfügbar- und Nutzbarkeit von Daten im Web wird oft mit dem Begriff „Open Data" bezeichnet.[261]

Der Rechtsrahmen in der Europäischen Union bezüglich offener Daten und der Weiterverwendung von Informationen des **öffentlichen Sektors**, d.h. öffentlichen und öffentlich finanzierten Informationen, beruht auf der **Open Data und PSI Richtlinie**, welche die bisherige Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors ersetzt.[262]

Um die Verwendung offener Daten[263] zu fördern und Anreize für die Innovation bei Produkten und Dienstleistungen zu vermitteln, enthält sie **Mindestvorschriften** für die Weiterverwendung und die praktischen Modalitäten zur Erleichterung der Weiterverwendung von vorhandenen Dokumenten im Besitz öffentlicher Stellen der Mitgliedstaaten, vorhandenen Dokumenten im Besitz gewisser öffentlicher Unternehmen und Forschungsdaten.[264]

Der Begriff „Dokument" umfasst jeden Inhalt oder einen beliebigen Teil davon unabhängig von der Form des Datenträgers (auf Papier oder in elektronischer Form oder als Ton-, Bild- oder audiovisuelles Aufnahme.[265] „**Forschungsdaten**" bilden eine Unterkategorie davon und werden definier als

[258] *Ensthaler/Haase*, Datenhoheit und Datenschutz im Zusammenhang mit Smart Services (2017), 3f, 6.
[259] *Ensthaler/Haase*, Datenhoheit und Datenschutz im Zusammenhang mit Smart Services (2017), 6f.
[260] Sie zu Deutschland https://www.bmi.bund.de/DE/themen/moderne-verwaltung/open-government/open-data/open-data-node.html (14.5.2021).
[261] Siehe dazu Open Data Österreich, https://www.data.gv.at/; Anders als bei Open Access liegt das Gewicht bei Open Data auf Informationen, die nicht in einer gebundenen Textform vorliegen, https://www.forschungsdaten.info/themen/finden-und-nachnutzen/open-data-open-access-und-nachnutzung/ (beide zuletzt abgerufen am 14.5.2021).
[262] RL 2003/98/EG in der Fassung der Novelle aus dem Jahre 2013 (Richtlinie 2013/37/EU); https://www.bmdw.gv.at/Themen/Europa/OesterreichinderEU/Open-Data-und-PSI.html; und https://digital-strategy.ec.europa.eu/en/policies/legislation-open-data (beide zuletzt abgerufen am 14.5.2021);
[263] EG 16 Satz 1 Open Data und PSI RL: „Das Konzept „offene Daten" (Open Data) bezeichnet nach dem allgemeinen Verständnis Daten in einem offenen Format, die von allen zu jedem Zweck frei verwendet, weiterverwendet und weitergegeben werden können".
[264] Art 1 Abs 1 Open Data und PSI RL.
[265] Art 2 Z 6 Open Data und PSI RL; EG 30 Open Data und PSI RL: „Diese Richtlinie gibt eine Definition des Begriffs „Dokument" vor, und diese Begriffsbestimmung sollte alle Teile eines Dokuments umfassen. Der **Begriff „Dokument"** sollte jede Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen unabhängig von der Form des Datenträgers (auf Papier oder in elektronischer Form, Ton-, Bild- oder audiovisuelles Material) umfassen. Der

„Dokumente in digitaler Form, bei denen es sich nicht um wissenschaftliche Veröffentlichungen handelt und die im Laufe von wissenschaftlichen Forschungstätigkeiten erfasst oder erzeugt und als Nachweise im Rahmen des Forschungsprozesses verwendet werden oder die in der Forschungsgemeinschaft allgemein für die Validierung von Forschungsfeststellungen und -ergebnissen als notwendig erachtet werden".[266] „Zu den Forschungsdaten gehören Statistiken, Versuchsergebnisse, Messungen, Beobachtungen aus der Feldarbeit, Umfrageergebnisse, Befragungsaufzeichnungen und Bilder. Auch Metadaten, Spezifikationen und andere digitale Objekte sind Teil davon."[267]

Nach der Richtlinie haben die Mitgliedstaaten die Verfügbarkeit von Forschungsdaten durch die Politik des offenen Zugangs zu unterstützen, die sich an Forschungseinrichtungen und Forschungsförderungseinrichtungen richtet, und die Annahme nationaler Strategien und einschlägiger Maßnahmen umfasst, um die öffentlich finanzierte Forschungsdaten nach dem Grundsatz der „standardmäßig offenen Daten" und im Einklang mit den FAIR[268]-Grundsätzen offen zugänglich zu machen.[269]

Die Forschungsdaten können **für kommerzielle und nichtkommerzielle Zwecke weiterverwendet werden**, soweit i) sie **öffentlich finanziert wurden** und wenn ii) sie von Forschern, Forschungseinrichtungen oder Forschungsförderungseinrichtungen **bereits über ein institutionelles oder thematisches Archiv öffentlich zugänglich gemacht wurden**.[270] Durch diese Verpflichtungen sollten keine zusätzlichen Kosten für den Abruf der Datensätze verursacht oder eine zusätzliche Pflege der Daten erforderlich gemacht werden.[271] Durch diese Einschränkung sollte Verwaltungsaufwand vermieden werden, allerdings dürfen die Mitgliedstaaten auch weitergehende Regelungen vorsehen.[272]

Des Weiteren sind bei öffentlicher Zugänglichmachung von Forschungsdaten berechtigte Geschäftsinteressen, Wissenstransfertätigkeiten, bestehende Rechte Dritter an geistigem Eigentum und Schutzes personenbezogener Daten nach dem Grundsatz „so offen wie möglich, so geschlossen wie nötig" (as open as possible, as closed as necessary) zu berücksichtigen.[273]

Die in den Anwendungsbereich der Regelung fallende Forschungseinrichtungen und Forschungsförderungseinrichtungen können „auch als öffentliche Stellen oder öffentliche Unternehmen eingerichtet sein." Allerdings „gilt [sie] für solche Hybridorganisationen nur in ihrer Funktion als Forschungseinrichtungen und bezüglich ihrer Forschungsdaten."[274]

---

Begriff „Dokument" erstreckte sich nicht auf Computerprogramme. Die Mitgliedstaaten können den Anwendungsbereich dieser Richtlinie auf Computerprogramme ausweiten."

[266] Art 2 Z 9 Open Data und PSI RL.

[267] EG 27 Satz 3f Open Data und PSI RL.

[268] Findable, Accessible, Interoperable, Reusable.

[269] Art 10 Abs 2 Open Data und PSI RL; EG 27 Open Data und PSI RL, siehe Satz 6: „„Offener Zugang" ist als die Praxis zu verstehen, Forschungsergebnisse dem Endnutzer kostenlos und ohne Beschränkung der Verwendung und Weiterverwendung, abgesehen von der Möglichkeit, die Nennung des Urhebers zu verlangen, online verfügbar zu machen".

[270] Art 10 Abs 2 Open Data und PSI RL.

[271] EG 28 Open Data und PSI RL.

[272] EG 28 Open Data und PSI RL; *Horn*, Neufassung der Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors (PSI-II-Richtlinie), jusIT 2020/1, 1 (3).

[273] Art 10 Abs 1 und Abs 2 sowie Art 1 Abs 2 lit c und lit h Open Data und PSI RL.

[274] EG 28 Satz 2f Open Data und PSI RL.

Für die Weiterverwendung von Forschungsdaten darf **kein Kostenersatz** verlangt werden.[275] Die Bedingungen für die Weiterverwendung von Forschungsdaten (und sonstigen Dokumenten) dürfen nichtdiskriminierend sein.[276] Des Weiteren dürfen „Verträge oder sonstige Vereinbarungen zwischen den öffentlichen Stellen oder öffentlichen Unternehmen, die im Besitz der Dokumente sind, und Dritten […] keine ausschließlichen Rechte gewähren", weil die Weiterverwendung von Dokumenten allen potenziellen Marktteilnehmern offen steht.[277]

Die Weiterverwendung sollte keinen Bedingungen unterliegen, es sei denn, diese Bedingungen sind objektiv, verhältnismäßig, nichtdiskriminierend und durch ein im Allgemeininteresse liegendes Ziel gerechtfertigt.[278] Die Bedingungen müssen auf das notwendige Mindestmaß beschränkt sein und sollen möglichst in Form von **Standardlizenzen** auferlegt werden, die an besondere Lizenzanträge angepasst und elektronisch verarbeitet werden können.[279] Diese Lizenzen können „Bedingungen für die Weiterverwendung durch den Lizenznehmer, wie die Haftung, der Schutz personenbezogener Daten, die ordnungsgemäße Verwendung der Dokumente, die Garantie der unveränderten Wiedergabe und der Quellennachweis", festlegen.[280]

Ergänzend ist darauf hinzuweisen, dass nach der Open Data und PSI RL ferner **hochwertige Datensätze** in Datenkategorien Georaum, Erdbeobachtung und Umwelt, Meteorologie, Statistik, Unternehmen und Eigentümerschaft von Unternehmen, und Mobilität, zu ermitteln und festzulegen sind. Diese müssen europaweit kostenlos (gegebenenfalls als Massen-Download) verfügbar, maschinenlesbar und über Schnittstellen (API) abrufbar sein.[281]

Die Open Data und PSI-RL ist am 16. Juli 2019 in Kraft getreten. Die Umsetzungsfrist von zwei Jahren endet am 17. Juli 2021. Die Umsetzung wird voraussichtlich durch eine Novelle (oder vollständige Neufassung) des Bundesgesetzes über die Weiterverwendung von Informationen öffentlicher Stellen (**Informationsweiterverwendungsgesetz** - IWG) und der neun Landes-Informationsweiterverwendungsgesetze erfolgen.[282] Ein Ministerialentwurf des neu gefassten IWG wurde allerdings noch nicht veröffentlicht.[283]

[275] Art 6 Abs 6 lit b Open Data und PSI RL; *Horn*, Neufassung der Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors (PSI-II-Richtlinie), jusIT 2020/1, 1 (3).
[276] Art 11 Abs 1 Open Data und PSI RL.
[277] Art 12 Abs 1 Open Data und PSI RL; EG 48 Open Data und PSI RL.
[278] Art 8 Abs 1 Open Data und PSI RL.
[279] Art 8 Abs 2 Open Data und PSI RL; *Horn*, Neufassung der Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors (PSI-II-Richtlinie), jusIT 2020/1, 1 (2).
[280] EG 44 Open Data und PSI RL.
[281] Art 14 Open Data und PSI RL; Beispiele für Datensätze siehe bei Bekanntmachung der Kommission, Leitlinien für empfohlene Standardlizenzen, Datensätze und Gebühren für die Weiterverwendung von Dokumenten, 2014/C 240/01, 3.1, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52014XC0724(01)#ntc4-C_2014240DE.01000101-E0004 (zuletzt abgerufen am 14.5.2021).
[282] *Horn*, Neufassung der Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors (PSI-II-Richtlinie), jusIT 2020/1, 1.
[283] Stand: 14.5.2021, https://www.parlament.gv.at/PAKT/MESN/index.shtml?jsMode=&xdocumentUri=&filterJq=&view=&GP=XXVII&anwenden=Anwenden&MESN=ME&R_MESN=ME&MIN=ALLE&SUCH=dat&listeId=102&FBEZ=FP_002 (zuletzt abgerufen am 14.5.2021).

Obwohl sich der Rechtsrahmen für Open Data im Wandel befindet, ergeben sich daraus für ein kollaboratives Daten-, Informations- und Wissensmanagement **im Ergebnis** folgende Grundsätze für die Veröffentlichung von (Forschungs-)Daten als Open Data.[284]

Vorab muss sichergestellt werden, dass die Veröffentlichung rechtlich zulässig ist. Es ist daher zu prüfen, ob durch die Veröffentlichung die datenschutzrechtlichen Anforderungen oder die Rechte Dritter an geistigem Eigentum verletzt werden (siehe Punkt 4.1.2 oben und 4.1.3 oben). Des Weiteren können vor allem bei wirtschaftlich wertvollen bzw sensiblen Daten weitere Geheimhaltungsinteressen bestehen, die einer Veröffentlichung entgegenstehen (siehe Punkt 4.1.3.3 oben). Die Geheimhaltungsverpflichtung kann auch in einem Kooperations-, Werk- oder Arbeitsvertrag enthalten oder Gegenstand einer (separaten) Vertraulichkeits- und/oder Geheimhaltungsvereinbarung („*Non-Disclosure Agreements*“) sein.

Ist beabsichtigt, für die Ergebnisse eines Projekts ein Patent oder ein Gebrauchsmuster anzumelden, muss die Neuheit der Erfindung gewährt werden, weil diese eine der Schutzvoraussetzungen ist.[285] Der Charakter als neu kann allerdings verloren gehen, wenn die Daten, die eine Erfindung beschreiben, bereits veröffentlicht sind. Daher sollten Forschungsdaten erst veröffentlicht werden, wenn das Anmeldeverfahren abgeschlossen ist.[286]

Für die Erteilung der Nutzungsrechte sollten offene Standardlizenzen verwendet werden wie beispielsweise den neuesten Creative Commons Lizenzen (Version 4.0).[287] Neben Creative-Commons-Lizenzen kommen für Datensammlungen etwa Open Data Commons Lizenzen in Frage.[288] Es ist zu beachten, dass der Urheber/herr der Daten über die Lizenzform disponieren kann und durch Disparitäten ind en Lizenzen Inkongruenzen in der Nutzbarkeit der Daten auftreten können. Aus diesen Gründen ist auf beiden datenwirtschaftlichen Seiten auf eine möglichst kongruente und kompatible Lizenzierung zu achten.

### 4.4.6. Vorschlag für ein europäisches Daten-Governance-Gesetz („Data Governance Act“)

Wie in der 2020 veröffentlichten europäischen Datenstrategie angekündigt, hat die Europäische Kommission am 25.11.2020 einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Data-Governance-Act) veröffentlicht.[289]

[284] Siehe dazu auch Empfehlung (EU) 2018/790 der Kommission vom 25. April 2018 über den Zugang zu wissenschaftlichen Informationen und deren Bewahrung, C/2018/2375, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32018H0790 (zuletzt abgerufen am 14.5.2021).
[285] § 1 Abs 1 Patentgesetz 1970 („PatG“); § 1 Abs 1 Gebrauchsmustergesetz („GMG“).
[286] *forschungsdaten.info*, Forschungsdaten veröffentlichen, https://www.forschungsdaten.info/themen/rechte-und-pflichten/forschungsdaten-veroeffentlichen/ (zuletzt abgerufen am 14.5.2021).
[287] Bekanntmachung der Kommission, Leitlinien für empfohlene Standardlizenzen, Datensätze und Gebühren für die Weiterverwendung von Dokumenten, 2014/C 240/01, 2.2.
[288] Siehe dazu *forschungsdaten.info*, Forschungsdaten veröffentlichen; zu den empfohlenen Lizenzbestimmungen siehe auch Bekanntmachung der Kommission, Leitlinien für empfohlene Standardlizenzen, Datensätze und Gebühren für die Weiterverwendung von Dokumenten, 2014/C 240/01, 2.3.
[289] COM(2020) 767 final, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020PC0767 (zuletzt abgerufen am 14.5.2021).

Dieser Vorschlag zielt darauf ab, die Verfügbarkeit von Daten zur Nutzung zu fördern, indem das Vertrauen in die Datenmittler erhöht wird und die Mechanismen für die gemeinsame Datennutzung in der gesamten EU gestärkt werden.[290]

Die wesentlichen Inhalte des Vorschlags sind Bereitstellung von Daten des öffentlichen Sektors zur Weiterverwendung in Fällen, in denen diese Daten den Rechten anderer unterliegen, gemeinsame Datennutzung durch Unternehmen gegen Entgelt in jedweder Form, Ermöglichung der Nutzung personenbezogener Daten mithilfe eines „Mittlers für die gemeinsame Nutzung personenbezogener Daten", der Einzelpersonen bei der Ausübung ihrer Rechte gemäß der Datenschutz-Grundverordnung (DSGVO) unterstützen soll, sowie Ermöglichung der Nutzung von Daten aus altruistischen Gründen.[291]

Das vorgeschlagene Daten-Governance-Gesetz geht in seinem Anwendungsbereich über den Regelungsgegenstand der Open Data und PSI Richtlinie hinaus und wird daher bedeutende Änderungen bei der Governance von nicht-personenbezogenen Daten mit sich bringen.[292]

Im nächsten Schritt wird der Vorschlag im Rahmen eines Trilogs zwischen Vertretern des Parlaments, des Rates und der Kommission verhandelt und sein Inhalt angepasst, um ein Einvernehmen herzustellen. Es ist unwahrscheinlich, dass diese Verhandlungen weniger als 2 Jahre in Anspruch nehmen werden.[293]

[290] COM(2020) 767 final, Begründung, Punkt 1.
[291] COM(2020) 767 final, Begründung, Punkt 1; siehe auch *EK*, Verordnung über Daten-Governance – Fragen und Antworten, 25.11.2020, https://ec.europa.eu/commission/presscorner/detail/de/qanda_20_2103 (zuletzt abgerufen am 14.5.2021).
[292] Siehe dazu auch etwa *EDPB-EDPS*, Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), Rz 65 ff, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_en (zuletzt abgerufen am 14.5.2021); *Spindler*, Schritte zur europaweiten Datenwirtschaft – der Vorschlag einer Verordnung zur europäischen Data Governance; CR 2/2021, 98ff.
[293] Siehe zum Fortschritt https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-governance-act (zuletzt abgerufen am 14.5.2021). Siehe für eine Grundeinschätzung durch einen der Verf. auch https://www.derstandard.at/story/2000122074854/datenaltruismus-mit-formular-und-behoerde.