Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

International Green Data Spaces

Orientierungsbericht zu rechtlichen Herausforderungen inklusive Lösungsansätzen

FFG-Projektnummer: FO999897492

Wien, 18.09.2023

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität,
Innovation und Technologie, Radetzkystraße 2, 1030 Wien

Für den Inhalt verantwortlich:
Data Intelligence Offensive in Zusammenarbeit mit Ernst & Young

Wien, 19. April 2024

Vorwort

Der Green Data Hub ist ein Projekt der DIO, das sich zum Ziel gesetzt hat, ein nachhaltiges Daten-Service-Ökosystem aufzubauen, das Unternehmen, Organisationen und öffentliche Verwaltung miteinander ver-netzt, um gemeinsam Innovation in Richtung einer nachhaltigen, europäischen Datenwirtschaft zu ermöglichen und somit zur Erreichung der Klimaziele beizutragen.

Dieser Orientierungsbericht wurde vom non-profit Verein Data Intelligence Offensive (im Folgenden „DIO“, ZVR-Nummer 1683545785, UID-Nr. ATU76576867) mit Unterstützung durch EY verfasst und dient ausschließlich zu allgemeinen Informationszwecken.

Erstellt mit Unterstützung von:

Link zu freigegebenen DIO-Dok: DIO_Green_Data_Hub_Orientierungsbericht_RECHT_final_freigegeben.pdf

Gefördert durch:

Inhalt

1 Projekt

Das vorliegende Dokument ist ein Orientierungsbericht zu Herausforderungen und Lösungsansätzen im Kontext des folgenden Förderprojekts.

- **International Green Data Spaces (InGDS)**
- **FFG-Projektnummer:** FO999897492
- **eCall Nummer:** 45648918

Dieser Orientierungsbericht wurde vom non-profit Verein Data Intelligence Offensive (im Folgenden „DIO“, ZVR-Nummer 1683545785, UID-Nr. ATU76576867) mit Unterstützung durch EY verfasst und dient ausschließlich zu allgemeinen Informationszwecken. Er stellt keine rechtliche Beratung dar und kann nicht als Ersatz für eine fundierte Fachberatung angesehen werden. Der Bericht bietet eine begrenzte Betrachtung ausgewählter von DIO gesetzter Schwerpunkte. Weitere Details entnehmen Sie bitte auf der letzten Seite des Orientierungsberichtes.

1.1 Hintergrund

Der Green Data Hub ist ein Projekt der DIO, das sich zum Ziel gesetzt hat, ein nachhaltiges Daten-Service-Ökosystem aufzubauen, das Unternehmen, Organisationen und öffentliche Verwaltung miteinander vernetzt, um gemeinsam Innovation in Richtung einer nachhaltigen, europäischen Datenwirtschaft zu ermöglichen und somit zur Erreichung der Klimaziele beizutragen.

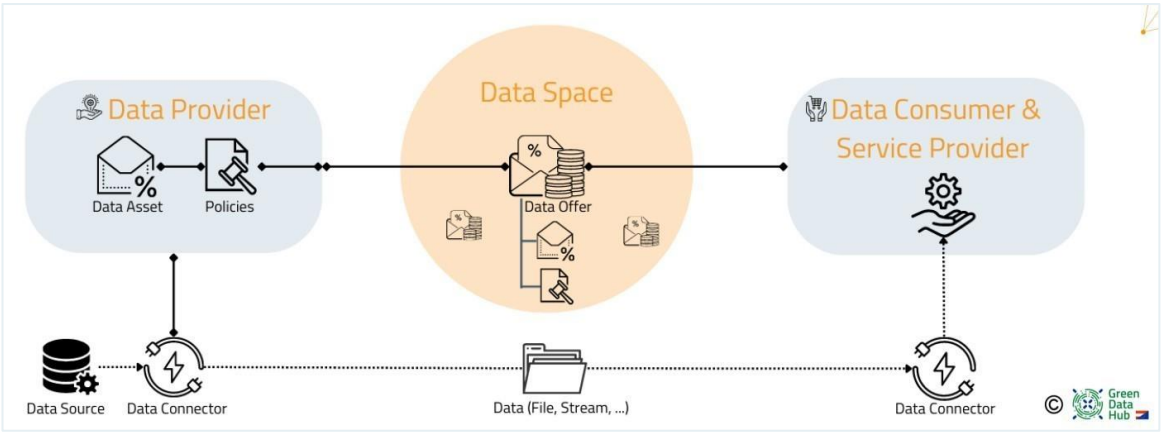


Abbildung 1: Aufbau eines Data Spaces und deren Akteure, Quelle: dataintelligence.at

Der Data Provider (Dateninhaber) stellt Daten über Data Spaces an die Data Consumer zur Verfügung. Data Spaces bezeichnet eine Plattform, auf der Data Provider und Data Consumer zusammentreffen können; Data Spaces sind jedoch ausdrücklich nicht die technische Umsetzung zum Datenaustausch. Die technische Umsetzung der Data Spaces übernimmt ein externer, technischer Dienstleister.

Die technischen Datenaustausch-Mechanismen sind entweder derart ausgestaltet, dass die Daten jeweils immer nur vom Data Provider an den jeweiligen Data Consumer übertragen werden, oder derart, dass der Data Consumer Zugang zu einem Datenbereich erlangt, in dem mehrere Daten von einem oder mehreren Data Providern vorhanden sind.

Die DIO wird hingegen zu keinem Zeitpunkt den effektiven (technischen) Datenaustausch (etwa durch Zurverfügungstellung von Speicherplatz odgl) ermöglichen

Im Mittelpunkt steht dabei die Datenvernetzung, die Datenbereitstellung sowie die Zusammenarbeit unter den relevanten Stakeholdern im Daten-Service-Ökosystem. Innerhalb dieses Ökosystems werden bestimmte Data Spaces als Themenbereiche definiert, wie z.B. Energiewende, Mobilitätswende, Kreislaufwirtschaft und Digitaler Klimazwilling, die wiederum als Rahmen für konkrete Use Cases (z.B. „Health“) dienen, bei denen Daten ausgetauscht und genutzt werden, um datengetriebene Lösungen mit sozio-ökologischem sowie nachhaltigem Fokus zu entwickeln.

1.2 Ziel des Projektes

Auch wenn die DIO selbst nicht die technische Infrastruktur für einen Datenaustausch zur Verfügung stellt, ist es das Ziel der DIO einen solchen Datenaustausch zwischen Data Provider und Data Consumer zu er-leichtern. Ziel dieses Forschungsprojektes ist es, die rechtlichen Rahmenbedingungen für einen solchen Datenaustausch abzustecken.

Dabei sind unter anderem Aspekte der Datensouveränität, -sicherheit, und -verfügbarkeit auf hohem Standard zu gewährleisten, ohne dabei starke Einbußen iS Benutzerfreundlichkeit hinnehmen zu müssen. Auf Grund dessen, dass im Data Space mehrere Datenakteure zusammenkommen, entstehen besondere rechtliche Herausforderungen bei der Vernetzung der Akteure und deren Umgang mit Daten. Daher sind die Herausforderungen immer im Zusammenspiel der Akteure zu sehen.

Während auf der einen Seite die Data Provider ihren Fokus auf das rechtlich konforme Zur-Verfügung-Stellen von Daten legen, wird auf der anderen Seite, beim Data Consumer, das Hauptaugenmerk auf die rechtlich konforme zweckmäßige Verwendung der Daten gelegt. Der Data Space muss hierfür als Schnitt-stelle für die Akteure eine vertrauensvolle Umgebung aufbauen, in der davon ausgegangen werden kann, dass alle Akteure ihre rechtlichen Pflichten erfüllen. Dabei stehen vor allem der Umgang und die

Verarbeitung von personenbezogenen Daten im Vordergrund, da diese als besonders schützenswert gelten.

2 Grundsätze der DSGVO

2.1 Sachlicher Anwendungsbereich

Die DSGVO gilt für personenbezogene Daten natürlicher Personen, wenn diese

- Ganz oder teilweise automatisiert verarbeitet werden oder
- Manuell verarbeitet werden und in einem Datensystem gespeichert sind oder gespeichert werden sollen.

Sofern die natürliche Person ihren Aufenthalt in der EU hat, ist sie ungeachtet ihrer Staatsangehörigkeit (d.h. auch Drittstaatsangehörige) geschützt (ErwGr 2 DSGVO).

"Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden auch "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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

"Verarbeitung" bedeutet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Die DSGVO gilt jedoch nicht für die Verarbeitung

- personenbezogener Daten von juristischen Personen (z.B. Name, Rechtsform, Kontaktdaten, ErwGr 14 S 2 DSGVO) oder
- personenbezogener Daten Verstorbener (ErwGr 27 DSGVO) bzw
- von anonymen Daten (ErwGr 26 DSGVO).

Die DSGVO findet außerdem keine Anwendung auf Datenverarbeitungen:

- die nicht in den Anwendungsbereich des Unionsrechts fallen (z.B. nationale Sicherheit, ErwGr 16 DSGVO);

- die Mitgliedstaaten im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der Union durchführen;
- durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;
- durch die Organe, Einrichtungen, Ämter und Agenturen der Union und
- durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (Art 2 Abs 2 und 3 DSGVO).

2.2 Räumlicher Anwendungsbereich

Die DSGVO findet in den folgenden drei Fällen Anwendung:

2.2.1 Niederlassung in der Union

Die DSGVO ist dann räumlich anwendbar, wenn

- ein:e Verantwortliche:r oder Auftragsverarbeiter:in eine Niederlassung in der Union hat und
- im Rahmen der Tätigkeit dieser Niederlassung personenbezogene Daten verarbeitet.

Dabei ist es irrelevant, ob die Verarbeitung als solche in oder außerhalb der EU stattfindet. "Im Rahmen der Tätigkeit der Niederlassung" bedeutet nicht, dass die Niederlassung selbst die Datenverarbeitung vornehmen muss. Es genügt, wenn ihre Tätigkeit im Zusammenhang mit einer Datenverarbeitung steht.

2.2.2 Niederlassung außerhalb der Union

Ferner ist die DSGVO auch dann räumlich anwendbar, wenn

- ein:e Verantwortliche:r oder ein:e Auftragsverarbeiter:in keine Niederlassung in der EU hat und
- diese:r personenbezogene Daten von in der EU befindlichen betroffenen Personen verarbeitet und
- die Verarbeitung dazu dient, diesen Personen
  a) Waren oder Dienstleistungen anzubieten (unabhängig davon ob entgeltlich oder unentgeltlich) oder

  b) deren Verhalten zu beobachten, soweit ihr Verhalten in der Union erfolgt.

2.2.3 2.2.3 Niederlassung außerhalb der Union + völkerrechtliche Regelung der Anwendbarkeit des Rechts eines EU-Mitgliedsstaates

Schließlich gelangt die DSGVO auch zur Anwendung, wenn nicht in der EU niedergelassene Verantwortliche oder Auftragsverarbeiter:innen personenbezogene Daten an einem Ort verarbeiten, der nach Völkerrecht dem Recht eines EU-Mitgliedstaates unterliegt. Ein Beispiel hierfür sind diplomatische oder konsularische Vertretungen eines Mitgliedstaates in einem Drittstaat.

Im Folgenden setzen wir die Anwendbarkeit der DSGVO voraus.

2.3 Rechtmäßigkeit der Datenverarbeitung

Art 6 DSGVO regelt, wann die Verarbeitung personenbezogener Daten rechtmäßig ist. Dessen Abs 1 enthält eine erschöpfende Liste mit sechs Erlaubnistatbeständen für die rechtmäßige Verarbeitung von personen-bezogenen Daten. Es muss mindestens einer dieser Tatbestände erfüllt sein, andernfalls eine unrechtmäßige Verarbeitung vorliegt. Unrechtmäßige Datenverarbeitungen sind verboten und können (hohe) Strafen mit sich bringen.

2.4 Sanktionen und Rechtsfolgen bei einem Verstoß gegen die DSGVO

Ein Verstoß gegen die Pflichten der DSGVO kann verwaltungsstrafrechtlich mit Geldbußen von bis zu EUR 20 Mio. oder – im Fall eines Unternehmens – von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet werden.

Jede betroffene Person hat das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt. Alternativ kann sie ihren Anspruch in unmittelbarer Anwendbarkeit des Art 79 DSGVO auch im gerichtlichen Verfahren geltend machen.1

Ist der betroffenen Person durch den Verstoß ein materieller oder immaterieller Schaden entstanden, hat sie einen Schadenersatzanspruch gegen die verantwortliche Person.2 Im Sinne einer rezenten Entscheidung des EuGH3 wird ein Schadenersatzanspruch nicht schon dann begründet, wenn ein Verstoß gegen die DSGVO vorliegt. Für einen Schadenersatzanspruch nach Art 82 DSGVO sind drei

[1] *Haidinger* in *Knyrim*, DatKomm Art 15 DSGVO, Rz 6 ff.
[2] *Haidinger* in *Knyrim*, DatKomm Art 17 DSGVO, Rz 7 f.
[3] EUGH 4.5.2023, C-300/21 – *Österreichische Post*.

zentrale Punkte erforderlich, die kumulativ vorliegen müssen: (i) ein Verstoß gegen die DSGVO, (ii) ein (im-) materieller Schaden, der aus dem Verstoß resultiert sowie (iii) der Kausalzusammenhang zwischen dem Verstoß und dem Schaden. Die DSGVO selbst enthält keine Regelung zur Bemessung des Schadenersatzanspruches, daher ist es insbesondere dem nationalen Recht vorbehalten, die Höhe des Anspruches festzulegen (unter Wahrung des Effektivitäts- und Äquivalenzgrundsatzes). Laut Rechtsprechung ist der Schadenersatzanspruch aber nicht auf immaterielle Schäden, die eine gewisse Erheblichkeitsschwelle überschreiten, beschränkt. Demnach haben Verantwortliche auch dann mit Ansprüchen betroffener Personen zu rechnen, wenn diese keine Erheblichkeitsschwelle überschreiten.

Neben den verwaltungsstrafrechtlichen und gerichtlichen Konsequenzen eines Verstoßes sind auch eine allfällige negative Öffentlichkeitswirkung und damit einhergehende Reputationsschäden nicht zu unterschätzen.

3 Österreichisches Datenschutzgesetz

3.1 Verhältnis zur DSGVO

In Österreich gilt neben der DSGVO auch das Datenschutzgesetz ("**DSG**"). Es nutzt einige der Öffnungsklauseln der DSGVO, die den Mitgliedsstaaten legistischen Spielraum einräumen, und ist somit zusätzlich zur DSGVO zu beachten. Darüber hinaus wurde in einer Reihe von Sondergesetzen (insbesondere im Zusammenhang mit Gesundheitsdaten und Datenverarbeitungen zu Forschungszwecken) von den Öffnungsklauseln der DSGVO Gebrauch gemacht, weshalb für jeden konkreten Use Case die einschlägigen nationalen Regelungen eigens zu bestimmen sind. Eine Darstellung dieser Sonderbestimmungen würde den Rahmen des vorliegenden Orientierungsberichts sprengen.

3.2 Juristische Personen und Recht auf Datenschutz

Wie dargelegt fallen personenbezogene Daten von juristischen Personen nicht in den Anwendungsbereich der DSGVO. Abweichend davon sieht § 1 DSG hingegen vor, dass in Österreich auch juristische Personen das Grundrecht auf Datenschutz genießen.

Dieses Grundrecht auf Datenschutz bedeutet, dass auch juristische Personen ua das Recht haben,

- Auskunft darüber zu erhalten, wer welche Daten über sie verarbeitet, woher die Daten stammen und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
- die Richtigstellung unrichtiger Daten zu verlangen; und
- die Löschung unzulässig verarbeiteter Daten zu verlangen.

4 Rechtliche Herausforderungen

4.1 Rollenverteilung nach der DSGVO

4.1.1 Beschreibung und Herausforderung

Beschreibung

Bei einer Datenverarbeitung wirken oftmals mehrere unterschiedliche Akteure zusammen. Die DSGVO sieht hierfür differenzierte Rollenkonzepte vor, an welche unterschiedliche Rechte und Pflichten geknüpft sind. Dementsprechend kommt der Rollenverteilung im Datenschutzrecht eine wesentliche Bedeutung zu, wobei diese für jede Datenverarbeitungstätigkeit separat bewertet werden muss. Hierzu sind die Begriffe und Rollen des “Verantwortlichen“, des “Auftragsverarbeiters“, der “betroffenen Person“ und des “Dritten“ näher zu beleuchten.

Verantwortliche:r

Verantwortliche Person ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die eigenständig oder in Zusammenarbeit mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Dies bedeutet jedoch nicht, dass der Verantwortliche selbst die Daten verarbeiten muss. Er kann sich hierzu auch eines Auftragverarbeiters bedienen (siehe sogleich).[4] Wie die Bezeichnung schon deutlich macht, ist der Verantwortliche jedoch Herr der Datenverarbeitung, weshalb er auch primärer Adressat der Pflichten und Anforderungen nach der DSGVO ist. Die Definition des Art 4 Z 7 stellt dabei stets auf die jeweiligen Rechtsträger und nicht auf die Leitungsorgane ab. So ist z.B. verantwortliche Person iSd Art 4 Z 7 DSGVO die GmbH und nicht ihr:e Geschäftsführer:in.5

Zudem besteht auch die Möglichkeit, dass mehrere Personen gemeinsam als Verantwortliche der konkreten Datenverarbeitung agieren. In einem solchen Fall sind diese als "Gemeinsam für die Verarbeitung Verantwortliche" iSd Art 26 DSGVO zu betrachten. Dabei wird die Erhebung, die Verarbeitung und/oder die Nutzung der personenbezogenen Daten gemeinsam ausgeführt. Zentral

[4] Art 29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, WP 169, 15 ff.

[5] *Bergauer* in *Bergauer/Jahnel/Mader/Staudegger*, jusIT Spezial: DS-GVO (2018) Die Rollenverteilung nach der DS-GVO – zugleich Überlegungen zu einem Übermittlungsprivileg im Konzern innerhalb enger Grenzen, 32.

hierbei ist, dass die Zwecke der Verarbeitung von den Verantwortlichen gemeinsam festgelegt werden.[6] Je nach konkretem Ausgangssachverhalt können die Pflichten gemäß DSGVO daher mehrere Personen gemeinsam treffen. Von der Datenverarbeitung Betroffene können die ihnen zustehenden Rechte gegenüber jedem einzelnen der Verantwortlichen geltend machen.7 Die Abgrenzung, wann eine sog "gemeinsame Verantwortung" vorliegt, kann im Einzelfall schwierig sein.[8] Verarbeiten Personen die personenbezogenen Daten hingegen unabhängig voneinander, d.h. gehen sie unterschiedlichen Zwecken nach und wird die Verarbeitung oder die Nutzung nicht gemeinsam ausgeführt, ist die Verantwortlichkeit gesondert zu untersuchen.

Auftragsverarbeiter:in

Nach der Legaldefinition des Art 4 Nr 8 DSGVO ist Auftragsverarbeiter:in eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des/der Verantwortlichen verarbeitet. Auftragsverarbeiter:innen üben zwar die physische Herrschaft über den Verarbeitungsprozess aus, entscheiden aber nicht selbst über die Zwecke und Mittel der Verarbeitung. Sie agieren daher nach Weisung des/der Verantwortlichen auf Basis einer vertraglichen Vereinbarung und ohne eigenen Wertungs- und Entscheidungsspielraum. Der rechtliche und tatsächliche Einfluss auf die Entscheidung, wozu personenbezogene Daten verarbeitet werden, steht ausschließlich dem/der Verantwortlichen zu.[9] Aufgrund dieser Tätigkeit als verlängerter Arm des/der Verantwortlichen trifft Auftragsverarbeiter grds nur ein beschränkter Pflichtenkatalog.

Betroffene Person

Wie bereits ausgeführt sind Betroffene jene natürlichen Personen, auf die sich die Daten beziehen, dh welche durch die Daten identifiziert werden oder zumindest indentifizierbar sind.

Dritte

Die DSGVO normiert in Art 4 Z 10 DSGVO, dass "Dritte" jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle ist, die nicht selbst betroffene Person, der/die Verantwortliche oder der/die Auftragsverarbeiter:in ist oder den verantwortlichen oder auftragsverarbeitenden Personen unmittelbar unterstellt ist. Dritte sind demnach all jene Personen, die weder an der konkreten

---

[6] Art 26 Abs 1 DSGVO.
[7] *Buder* in *Jahnel*, Datenschutzrecht (2020) Der Verantwortlichenbegriff der Datenschutz-Grundverordnung, 123.
[8] *Raschauer* in *Sydow*, Europäische Datenschutz-Grundverordnung (2017) Art 4, Rz 129; *Bergauer* in *Bergauer/Jahnel/Mader/Staudegger*, jusIT Spezial: DS-GVO (2018) Die Rollenverteilung nach der DS-GVO – zugleich Überlegungen zu einem Übermittlungsprivileg im Konzern innerhalb enger Grenzen, 31.
[9] *Sedef/Steiner*, Datenschutz - Auftragsverarbeiter (Stand 15.3.2023, Lexis Briefings in lexis360.at) mWn, zB *Feiler/Forgó*, EU-DSGVO (2016) Rz 12; *Martini* in *Paal/Pauly,* Datenschutz-Grundverordnung Art 28, Rz 2.

Datenverarbeitung mitwirken, noch deren personenbezogene Daten von der Verarbeitung betroffen sind.[10]

Herausforderung

Abhängig von der jeweiligen Rolle iSd DSGVO treffen die Beteiligten unterschiedliche Rechte und Pflichten. In der Datenökonomie zu unterscheiden sind etwa die Rollen der Data Provider, Infrastructure Provider, Data Consumer, Broker, Service Provider und End User. Bei Umsetzung der Data Spaces liegt die Herausforderung demnach darin, die an jeder einzelnen Verarbeitungstätigkeit beteiligten Akteure den entsprechenden Rollen zuzuordnen und demzufolge die anwendbaren Regelungen und Verpflichtungen zu ermitteln. Zu beachten ist ferner, dass je nach Konstellation (Auftragsverarbeiterverhältnis; gemeinsame Verantwortlichkeit) die Beteiligten ggf vertragliche Vereinbarungen untereinander abschließen müssen. Aufgrund der extensiven Rechtsprechungslinie zur gemeinsamen Verantwortlichkeit ist bei der Umsetzung der Data Spaces Art 26 DSGVO im Besonderen zu berücksichtigen. Insbesondere könnte sich hieraus auch eine datenschutzrechtliche Verantwortlichkeit der DIO ergeben.

4.1.2 Rechtliche Grundlagen

Art 4 Z 7 DSGVO: Definition der verantwortlichen Person.

Art 4 Z 8 DSGVO: Definition des Auftragsverarbeiters.

Art 4 Z 10: Definition des Dritten.

Art 24 DSGVO: Pflichten der verantwortlichen Personen.

Art 26 DSGVO: Definition und Pflichten der Gemeinsam für die Verarbeitung Verantwortlichen.

Art 28 DSGVO: Anforderungen an eine Auftragsverarbeitung.

4.1.3 Lösungsansatz

Um die Herausforderung der korrekten Zuordnung von DSGVO-Rollen zu Datenökonomie-Rollen und der korrekten Vergabe deren Verantwortlichkeiten zu überwinden, sollte eine klare Identifikation der Rollen

[10] *Bergauer* in *Bergauer/Jahnel/Mader/Staudegger*, jusIT Spezial: DS-GVO (2018) Die Rollenverteilung nach der DS-GVO - zugleich Überlegungen zu einem Übermittlungsprivileg im Konzern innerhalb enger Grenzen, 63.

nach dem DSGVO vorgenommen werden, sowie eine schriftliche und kommunikative Form der Verantwortlichkeitszuordnung. Für eine möglichst reibungsfreie Durchführung dieser Pflichten sollten die dafür notwendigen Prozesse möglichst in die anderen Prozesse der Unternehmen eingegliedert werden. Zu Beginn bedarf es die Verschriftlichung der Rollen und Pflichten, welche als Anhaltspunkt für die Datenverarbeitung dient. Wie in den Herausforderungen geschildert sollte die einzelnen Akteure ihren Rollen nach dem DSGVO zugeordnet werden. Nachfolgend ist ein Vorschlag zur Zuordnung der Rollen geschildert, um die Rollen je nach Situation zu bestimmen.

Ein **Data Provider** kann als Verantwortlicher im Sinne der DSGVO angesehen werden, da er die Kontrolle über die Art und Weise hat, wie die Daten verarbeitet werden, und die Zwecke und Mittel der Verarbeitung festlegt.

Der **Infrastructure Provider** kann als Auftragsverarbeiter im Sinne der DSGVO betrachtet werden, da er die Daten im Auftrag des Data Providers verarbeitet und technische Infrastruktur und sonstige Datenverarbeitungsdienste bereitstellt.

Der **Data Consumer** kann je nach Rolle entweder als Verantwortlicher oder Auftragsverarbeiter gelten. Wenn der Data Consumer die Daten für seine eigenen Zwecke verarbeitet und kontrolliert, wird er als Verantwortlicher betrachtet. Wenn der Data Consumer die Daten im Auftrag eines anderen verarbeitet, kann er als Auftragsverarbeiter agieren.

Der **Broker** kann eine Mischung aus verschiedenen DSGVO-Rollen sein, abhängig von seiner gewählten Funktion. Wenn der Broker lediglich als Vermittler agiert, um Daten zwischen einem Data Provider und Data Consumer zu vermitteln, könnte er als Datenverarbeiter im Auftrag betrachtet werden. Wenn der Broker jedoch zusätzliche Verarbeitungstätigkeiten ausführt, könnte er als Verantwortlicher gelten.

Der **Service Provider** kann je nach den erbrachten Dienstleistungen entweder als Verantwortlicher oder Auftragsverarbeiter eingestuft werden, ähnlich wie der Data Consumer.

Der **Endnutzer** wird normalerweise nicht als eigenständige DSGVO-Rolle betrachtet, es sei denn, er agiert in einer Rolle, die ihn zur Verarbeitung personenbezogener Daten befähigt, wie beispielsweise ein Unternehmen oder eine Organisation.

Wenn die Rollen der Verantwortlichen festgehalten wurden, sind diese dazu verpflichtet, die Verarbeitung der Daten rechtlich korrekt zu gestalten. Ein Vertragswerk dient hier als erstes Mittel, um die weitere Verarbeitung auf den rechtlichen und gewünschten Rahmen einzugrenzen. Als weiteres Mittel kann eine gemeinsame ROPA (Record of Processing Activities, „Verarbeitungsverzeichnis“) eingerichtet werden welches der folgenden Struktur folgen könnte:

- Verarbeitungsaktivität
  - Verwendete Daten
  - Zweck der Verarbeitung
  - Kategorien personenbezogener Daten
  - Verarbeitungsart (zb. Aggregierung, Übertragung, Applikationsrelevant, ML)

- Verantwortliche
  - Aufzählung der Verantwortlichen und deren Verantwortlichkeitsabgrenzung
- Auftragsverarbeitende
  - Aufzählung der verarbeitenden Einheiten und Verarbeitungsaufteilung
- Rechtsgrundlage
- Empfänger
  - Wem werden die Daten offengelegt (auch Drittländer)
- Dauer der Speicherung
- Änderungsverzeichnis

Um das Einhalten der Datenverarbeitung zu gewährleisten können, Data-Sharing-Lizenz-Vereinbarungen geschlossen werden, die darauf abzielen, Klarheit und Transparenz in Bezug auf die Nutzung von Daten zu schaffen, während gleichzeitig die Rechte der Dateninhaber, die Datenschutzvorschriften und andere rechtliche Anforderungen respektiert werden. Folgende Form könnte eine solche Vereinbarung annehmen:

- Lizenzgeber (Datenanbieter):
  - Der Lizenzgeber ist der Inhaber der Daten, der die Lizenzbedingungen festlegt.
  - Er legt die Art der Daten, die Dauer der Lizenz, den Zweck der Nutzung und andere relevante Bedingungen fest.
- Lizenznehmer (Datenempfänger):
  - Der Lizenznehmer ist die Partei, die die Lizenz erwirbt und die Daten gemäß den festgelegten Bedingungen nutzt.
  - Der Lizenznehmer kann eine Einzelperson, ein Unternehmen, eine Organisation oder eine andere Einheit sein.
- Lizenzbedingungen:
  - Zweck der Nutzung: Legt den spezifischen Zweck fest, für den die Daten verwendet werden dürfen (z. B. Forschung, Analyse, Marketing usw.).
  - Dauer der Lizenz: Bestimmt, wie lange die Daten genutzt werden dürfen.
  - Nutzungsbeschränkungen: Definiert, wie die Daten genutzt werden dürfen und welche Art von Verarbeitung erlaubt ist.
  - Datenkategorien: Gibt an, welche Art von Daten in der Lizenz enthalten ist.
  - Geografische Einschränkungen: Kann festlegen, wo die Daten genutzt werden dürfen.
  - Vertraulichkeit: Enthält Bestimmungen zur Vertraulichkeit und zum Schutz der Daten.
- Gebühren und Vergütung:
  - Legt fest, ob Gebühren für die Lizenzierung der Daten erhoben werden und wie diese Zahlungen erfolgen.
- Rechte und Pflichten:
  - Lizenzgeberrechte: Bestimmt die Rechte des Lizenzgebers, wie das Recht zur Überwachung der Datenverwendung und zur Beendigung der Lizenz.

- Lizenznehmerpflichten: Legt die Pflichten des Lizenznehmers fest, wie die Einhaltung der Lizenzbedingungen und die Sicherung der Daten.

- Datenschutz und Sicherheit:
  - Datenschutzbestimmungen: Enthält Maßnahmen zur Sicherstellung des Datenschutzes und zur Einhaltung der geltenden Datenschutzgesetze.
  - Sicherheitsanforderungen: Legt Sicherheitsstandards fest, um den Schutz der Daten während der Nutzung sicherzustellen.
- Vertragsdurchsetzung und Beendigung:
  - Vertragsdurchsetzung: Beschreibt, wie Verstöße gegen die Lizenzbedingungen behandelt werden.
  - Beendigung: Legt fest, unter welchen Umständen die Lizenz beendet werden kann, z. B. bei Verstoß gegen Bedingungen oder Ablauf der Lizenzdauer.
- Änderungen und Aktualisierungen:
  - Verfahren zur Aktualisierung oder Änderung der Lizenzbedingungen bei Bedarf.
- Rechtsprechung und Streitbeilegung:
  - Legt das anwendbare Recht und die zuständige Gerichtsbarkeit fest sowie Mechanismen zur Streitbeilegung.

Um diese Pflichten und Prozesse möglichst effizient in unternehmerische Prozesse einzugliedern, sollten Datenprozesse im Hinblick auf die DSGVO-Rollen bedacht werden. Die ROPA könnte zum Beispiel neben der DSGVO-Rolle auch eine Datenprozesskatalog-Rolle im Unternehmen übernehmen, um die Datenprozesse transparenter für alle Mitarbeitende Beschreibung und Herausforderung

4.2 Einholung der Einwilligung

Aus den Gesprächen mit der DIO haben wir verstanden, dass eine mögliche Datenverarbeitung im Rahmen der Data Spaces in den überwiegenden Fällen auf Basis einer zuvor eingeholten Einwilligung erbracht werden wird. Aufgrund dessen wird dem Thema Einwilligung besondere Aufmerksamkeit geschenkt.[11]

4.2.1 Beschreibung und Herausforderung

Beschreibung

Jede rechtmäßige Datenverarbeitung bedarf einer Rechtsgrundlage iSd Art 6 DSGVO. Als eine mögliche Rechtsgrundlage kann die Einwilligung der betroffenen Person dienen, die von der verantwortlichen

[11] Zu analysieren ist jedoch für jeden Einzelfall, ob eine etwaige Datenverarbeitung nicht auf andere Erlaubnistatbestände gestützt werden kann, zumal die Einwilligung von betroffenen Personen jederzeit widerrufbar ist.

Person iSd DSGVO wirksam einzuholen ist. Damit eine solche Einwilligung auch rechtsgültig ist, sieht die DSGVO eine Reihe von Anforderungen vor.

Eine gültige Einwilligung hat folgende Kriterien zu erfüllen:[12]

- **Freiwilligkeit:** Die betroffene Person muss eine echte Wahl zwischen Zustimmung und Ablehnung haben. Es soll eine faktisch erzwungene Einwilligungserteilung (die ua beim Vorliegen eines klaren Ungleichgewichts zwischen Betroffenem und Verantwortlichem vorliegen kann) verhindert werden.
- **Kopplungsverbot:** Es ist zu gewährleisten, dass die Erfüllung eines Vertrages oder die Erbringung einer Dienstleistung nicht von der Einwilligung in eine Datenverarbeitung abhängig gemacht wurde, wenn die Einwilligung nicht zwingend zur Vertragserfüllung benötigt wird.
- **Zweckbindung** für den bestimmten Fall: Für unterschiedliche Zwecke müssen separate Einwilligungen eingeholt werden, weshalb Generaleinwilligungen unwirksam sind.
- **Informiertheit:** Die Einwilligung muss "in informierter Weise" erfolgen, um die Folgen und Risiken einer Datenverarbeitung abschätzen zu können. Die betroffenen Personen sind demnach umfassend über den Hintergrund, Zusammenhang und die Tragweite ihrer Erklärung in Kenntnis zu setzen. Insbesondere ist darüber zu informieren, (i) wer der:die Verantwortliche ist, (ii) für welche Zwecke die Daten verarbeitet werden sollen, (iii) welche Personen Zugriff auf die Daten haben und (iv) wo die Daten gespeichert werden. Weiters müssen die Informationen gemäß Artt 13, 14 DSGVO bereitgestellt werden.
- **Eindeutigkeit:** Dies erfordert eine unmissverständlich abgegebene Willensbekundung der betroffenen Person (z.B. schriftliche Erklärung oder Ankreuzen einer Check-Box), weshalb ein bereits vorab angekreuztes Kästchen oder gesetztes Häkchen (dh eine “Opt-out“-Option) unzulässig ist. Für die Verarbeitung sensibler Daten bedarf es darüber hinaus einer ausdrücklichen Einwilligung.
- **Konkretisierung:** Die Einwilligungserklärung muss klar und einfach verständlich formuliert sein. Wenn Diese Teil eines Textes ist, muss sich die Einwilligung deutlich vom Rest des Textes abheben.
- **Information zum Widerrufsrecht:** Es muss auf die jederzeitige Widerrufsmöglichkeit der Einwilligung sowie auf die Folgen eines Widerrufs hingewiesen werden.[13]

Fehlerhaft eingeholte Einwilligungen sind ungültig. Hierbei ist strittig, ob die Einwilligung zumindest teilwirksam sein kann.[14] Ist die betroffene Person minderjährig, ist deren Einwilligung nach österreichischem Recht erst dann wirksam, wenn diese das 14. Lebensjahr bereits vollendet hat. Sofern dieses Mindestalter nicht erreicht ist, kann die Einwilligung zur Verarbeitung der personenbezogenen

[12] *Thiele/Wagner*, Umsetzung der DSGVO in der Personalpraxis (2019); *Pachinger*, DSGVO: Aus Zustimmung wird Einwilligung, ecolex 2017, 898.

[13] Art 29-Datenschhutzgruppe, Guidelines on consent under Regulation 2016/679, WP 259.

[14] *Schulz* in *Gola*, DS-GVO2 Art 7 Rz 52; *Frenzel* in *Paal/Pauly*, DS-GVO/BDSG2 Art 7, Rz 15.

Daten des Kindes nur durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt werden.

Aus Beweisgründen und im Hinblick auf die Rechenschaftspflicht15 ist anzuraten, dass Verantwortliche auch bei der Zustimmungserklärung zur Verarbeitung von nicht-sensiblen Daten schriftliche Einwilligungserklärungen oder sonstige nachweisbare Zustimmungserklärungen einholen. Hierbei ist auch zu dokumentieren, dass die Einwilligung den Anforderungen der DSGVO entspricht. Es ist weiters ratsam sicherzustellen, dass die Einwilligung jederzeit abrufbar ist und dass ausreichend technische und organisatorische Maßnahmen zum Schutz der Protokolle getroffen wurden.

Herausforderung

Die Metadaten, die im Data Space gespeichert werden, können Aufschluss darüber geben, ob die Einwilligung korrekt eingeholt wurde und zu welchem Verarbeitungszweck. Diese Informationen sind für den Data Consumer bzw. Service Provider, der Zugriff auf die Daten erhält, von großer Bedeutung. Der Service Provider ist verpflichtet, die Daten ausschließlich für den Zweck zu verwenden, für den die Einwilligung erteilt wurde bzw. andernfalls bei den Betroffenen, um eine Einwilligung für seine Zwecke zu ersuchen.

Kommt es zu einer Änderung des Verarbeitungszwecks, ist eine neuerliche Einwilligung einzuholen. Im Kontext der Data Spaces trifft diese Pflicht grds den Data Consumer bzw. Service Provider. Als problematisch könnte sich hierbei darstellen, dass der Service Provider im Regelfall über keine Kontaktdaten der betroffenen Personen verfügen wird. Dementsprechend ist dieser auf die Unterstützung des Data Provider angewiesen, um den datenschutzrechtlichen Anforderungen nachkommen zu können. Entsprechend müsste eine solche Kooperation zwischen Data Provider und Data Consumer vertraglich abgebildet werden.

Für die Umsetzung der Data Spaces besteht daher die grundlegende Anforderung, allen beteiligten Akteuren die aktuell gültige Einwilligung, zu welchem Zweck die Daten verarbeitet werden dürfen, wahrheitsgetreu und rechtskonform abzubilden. Daraus ergibt sich auf der Seite des Data Providers die Pflicht zur ständigen Pflege der Metadaten sowie auf der Seite des Data Consumers die Pflicht auf jegliche Verarbeitung der Daten außerhalb der gültigen Einwilligung zu verzichten bzw. zuerst eine entsprechende Erweiterung der Einwilligung einzuholen.

[15] *Wagner* in *Bergauer/Jahnel/Mader/Staudegger* (Hrsg), jusIT Spezial: DS-GVO (2018) Die Pflichten des Verantwortlichen nach der DS-GVO, 56.

Durch diese klare Aufteilung der Verantwortlichkeiten und die Berücksichtigung der datenschutzrechtlichen Rahmenbedingungen kann ein vertrauensvolles und sicheres Daten-Ökosystem geschaffen werden, das den Nutzen für alle Beteiligten maximiert.

4.2.2 Rechtliche Grundlagen

Die DSGVO kennt keine einheitliche Bestimmung, die die Wirksamkeit der Einwilligung abschließend regelt; vielmehr sind deren Voraussetzungen über die DSGVO verteilt. IdZ sind insbesondere Artt 4 Z 11, 6 Abs 1 lit a, 7, 8, 9 Abs 2 lit a, Art 13 Abs 2 lit c, 14 Abs 2 lit d, 17 Abs 1 lit b, 18 Abs 2, 20 Abs 1 lit a, 22 Abs 2 lit c, 83 Abs 5 lit a DSGVO sowie die dazugehörigen ErwGr 32, 33, 38, 40, 42, 43, 50, 51, 54, 65, 68, 71, 111, 112, 155, 161 und 171 der DSGVO relevant.

Die datenschutzrechtliche Einwilligung ist insbesondere auch für weitere Rechtsakte der EU maßgeblich. ErwGr 7 des Data Governance Act sieht etwa vor, dass die Verarbeitung personenbezogener Daten stets auf einer Rechtsgrundlage beruhen soll, die in den Art 6 und 9 DSGVO bestimmt sind. Wann immer der Austausch von personenbezogenen Daten vorgesehen ist, gilt daher die DSGVO und die Einwilligung stellt eine mögliche Rechtsgrundlage für die Verarbeitung dieser Daten dar.

4.3 Widerruf der Einwilligung

4.3.1 Beschreibung und Herausforderung

Beschreibung

Sofern sich eine Datenverarbeitung auf die Einwilligung der betroffenen Person stützt, kann diese jederzeit widerrufen werden. Der Widerruf der Einwilligung wirkt jedoch nur ex-nunc, dh ab dem Zeitpunkt des Widerrufs. Bereits erfolgte Datenverarbeitungen bleiben damit rechtmäßig. Das bedeutet, dass sichergestellt werden muss, dass die personenbezogenen Daten ab Widerruf nicht mehr verarbeitet werden. Sofern keine andere Rechtsgrundlage vorliegt, welche eine weitere Verarbeitung rechtfertigt (z.B. das Vorliegen einer Aufbewahrungspflicht iSd Art 6 Abs 1 lit c), sind die betroffenen personenbezogenen Daten zu löschen.[16]

Der Widerruf der Einwilligung muss genauso einfach erfolgen wie die Erteilung derselben. Die betroffene Person muss ihre Einwilligung daher in derselben Form bzw. in derselben Weise widerrufen können.

[16] *Kastelitz* in *Knyrim*, DatKomm Art 7 DSGVO, Rz 32.

Erfolgte die Einwilligungserklärung z.B. per Mausklick in einem Online-Formular, darf der Betroffene zur Ausübung des Widerrufs nicht auf einen anderen "Kanal", z.B. auf das Erfordernis einer schriftlichen Erklärung, verwiesen werden (sog "Korrespondenz der Erklärungsmittel").[17]

Die betroffene Person ist sowohl über das Bestehen des Widerrufsrechts zu informieren als auch auf deren ex-nunc-Wirkung ausdrücklich hinzuweisen.[18] Dabei ist auf die verständliche Gestaltung des Widerrufshinweises zu achten. Es darf nicht der Eindruck vermittelt werden, einer Datenverarbeitung jedenfalls zustimmen zu müssen und erst durch die Möglichkeit eines Widerrufs eine Datenverarbeitung zu solchen Zwecken unterbinden zu können (unzulässige "Opt-Out"-Lösung). [19] Bei einer fehlenden Belehrung über das Widerrufsrecht ist davon auszugehen, dass keine rechtsgültige Einwilligung vorliegt.[20]

Herausforderung

Erfolgt ein Widerruf der Einwilligung, so dürfen die von dem Widerruf umfassten personenbezogenen Daten ab dem Zeitpunkt des Widerrufes nicht mehr verarbeitet werden. Die Herausforderung ergibt sich hierbei, dass der Data Space von verschiedenen Akteuren iSd Rollenverteilung genutzt wird, die auf die betroffenen Daten zugegriffen haben. Sobald ein Widerruf vorliegt, müssen daher alle Beteiligten, wie der Data Provider oder die Data Consumer/Service Provider, die Verarbeitung der personenbezogenen Daten stoppen und gegebenenfalls die Löschung vornehmen, sofern keine abweichenden rechtlichen Verpflichtungen (wie insbesondere Aufbewahrungspflichten) greifen. Der Widerruf der Einwilligung muss daher von allen beteiligten Akteuren beachtet werden, um die betroffenen Datensätze korrekt zu behandeln.

Da sich die betroffene Person im Falle eines Widerrufs oftmals (nur) an den Data Provider wenden wird, muss der Data Provider eine aktive Rolle spielen und die Service Provider über den Widerruf informieren. Da sich eine solche Pflicht nicht direkt aus dem Gesetz ergibt, muss diese vertraglich abgebildet werden. Erreicht die Service Provider der Widerruf, muss dieser für die Service Provider klar und eindeutig formuliert sein, um sicherzustellen, dass die betroffenen Datensätze korrekt erfasst und in weiterer Folge gegebenenfalls gelöscht werden. Eine reibungslose Kommunikation zwischen Data Provider und Service Provider ist daher von großer Bedeutung, um den Schutz personenbezogener Daten zu gewährleisten und den rechtlichen Anforderungen zu entsprechen.

Insgesamt ist der Widerruf der Einwilligung in einem Data Space eine komplexe Angelegenheit, die sorgfältig und transparent behandelt werden muss. Im Data Space muss das Vertrauen herrschen, dass

---

[17] *Kastelitz* in *Knyrim*, DatKomm Art 7 DSGVO, Rz 29.
[18] Art 13 und 14 DSGVO iVm ErwGr 39 und ErwGr 65 DSGVO.
[19] *Kastelitz* in *Knyrim*, DatKomm Art 7 DSGVO, Rz 28.
[20] *Kastelitz* in *Knyrim*, DatKomm Art 7 DSGVO, Rz 30.

alle beteiligten Parteien korrekt handeln und zusammenarbeiten, um sicherzustellen, dass der Widerruf der Einwilligung rechtmäßig und effektiv umgesetzt wird.

4.3.2 Rechtliche Grundlagen

Art 7 Abs 3 DSGVO: Recht auf Widerruf, Rechtsfolgen des Widerrufs, Form des Widerrufs und Informationspflicht zum Widerruf.

Art 13 Abs 2 lit c DSGVO: Pflicht der oder des Verantwortlichen zur Information über das Bestehen eines Widerrufsrechts bei Erhebung von personenbezogenen Daten bei der betroffenen Person.

Art 14 Abs 2 lit d DSGVO: Pflicht der oder des Verantwortlichen zur Information über das Bestehen eines Widerrufsrechts, wenn personenbezogene Daten nicht bei der betroffenen Person erhoben werden (wenn sie also bspw. bei anderen Verantwortlichen, öffentlichen Quellen, Adressverlagen etc. erhoben werden).

4.4 Recht des Betroffenen auf Berichtigung und Löschung der Daten sowie Einschränkung der Verarbeitung

4.4.1 Beschreibung und Herausforderung

Beschreibung

Trotz Einspeisung der Daten in die Data Spaces müssen die betroffenen Personen die Kontrolle über deren weitere Verarbeitung behalten können (Datenhoheit/Data Sovereignty). Das impliziert auch die Möglichkeit (neben der Entscheidung über die Aufnahme in den Data Space mittels Einwilligung in die Datenverarbeitung), deren Berichtigung und Löschung sowie eine Einschränkung der Verarbeitung zu verlangen.

Einem Löschbegehren ist ua nachzukommen, wenn die Daten für die Zwecke, für welche sie ursprünglich eingeholt wurden, nicht mehr notwendig sind bzw dieser Zweck nicht mehr besteht.[21] Die Löschung meint in diesem Zusammenhang die Unkenntlichmachung der Daten, sodass sie unter Anwendung

[21] DSB 15.11.2018, DSB-D122.944/0007-DSB/2018.

üblicher Verfahren nicht mehr ausgelesen werden können. Eine völlige Irreversibilität ist nicht gefordert.[22]

Neben dem Löschbegehren steht es betroffenen Personen darüber hinaus zu, die sie betreffenden Daten berichtigen zu lassen. Das Recht auf Berichtigung soll die betroffene Person in die Lage versetzen, unrichtige Daten, die der Verantwortliche grds rechtmäßigerweise verarbeitet, richtigzustellen; bei Unvollständigkeit der Daten hat sie ein Recht auf Vervollständigung.

Flankierend zu den Rechten der betroffenen Person auf Berichtigung, Löschung und Widerspruch sieht die DSGVO auch einen (temporären) Begleitanspruch auf Einschränkung der Datenverarbeitung vor. Der Anspruch zielt darauf ab, dass die Daten nur mehr gespeichert werden dürfen; alle sonstigen Verarbeitungsschritte dürfen nur mehr unter engen Voraussetzungen vorgenommen werden. Je nach konkreter Situation kann es daher ein "milderes Mittel zur Löschung" sein.[23]

Ferner besteht die Pflicht des Verantwortlichen, falls Daten auf Antrag einer betroffenen Person berichtigt, gelöscht oder eingeschränkt wurden, jeden Empfänger, dem er die Daten offengelegt hat, über diesen Umstand zu informieren, es sei denn, dies wäre unmöglich oder mit einem unverhältnismäßig hohen Aufwand verbunden. Die betroffene Person kann Auskunft über die Empfänger begehren.

Herausforderung

Üben Betroffene ihre Rechte aus, haben Verantwortliche darauf mitunter unverzüglich zu reagieren. Die Herausforderung bei einem Lösch- bzw. Berichtigungsbegehren ergibt sich daraus, dass der Data Space möglicherweise von verschiedenen Personen genutzt wird, die auf die betroffenen Daten (auf die sich das Begehren bezieht) zugegriffen haben. Dennoch muss dem Lösch- bzw. Berichtigungsbegehren von allen beteiligten Akteuren entsprochen werden. Außerdem sind alle Datenempfänger:innen, denen die betroffenen Daten offengelegt wurden, über ein Begehren betreffend Löschung, Berichtigung oder Einschränkung der Verarbeitung zu unterrichten, was wiederum effiziente Kommunikationskanäle zwischen den Akteuren erfordert.[24] Hierbei ist zu beachten, dass wegen einer Löschung auch Use Cases dezimiert werden könnten, weshalb auch der Nutzen gewisser Stakeholder, denen die betroffenen Daten offengelegt wurden, geschmälert werden kann.

[22] *Haidinger* in *Knyrim*, DatKomm Art 17 DSGVO, Rz 63.
[23] *Haidinger* in *Knyrim*, DatKomm Art 18 DSGVO, Rz 1.
[24] *Haidinger* in *Knyrim*, DatKomm Art 17 DSGVO, Rz 85.

4.4.2 Rechtliche Grundlagen

Art 16 DSGVO: Recht der Betroffenen, von Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu fordern.

Art 17 Abs 1 DSGVO: Recht der Betroffenen, von den Verantwortlichen die unverzügliche Löschung sie betreffender personenbezogener Daten zu fordern.

Art 18 DSGVO: Recht der Betroffenen, von den Verantwortlichen die Einschränkung der Datenverarbeitung zu verlangen.

Art 19 DSGVO: Pflicht der Verantwortlichen, allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Berichtigung oder Löschung personenbezogener Daten oder die Einschränkung der Verarbeitung nach Art 16, 17 oder 18 mitzuteilen.

4.5 Transparenzpflicht bei Information, Kommunikation und Modalitäten für die Ausübung der Betroffenenrechte

4.5.1 Beschreibung und Herausforderung

Beschreibung

Betroffene sind über die ihnen nach DSGVO zustehenden Rechte in transparenter Weise aufzuklären. Art 12 DSGVO stellt hierbei Anforderungen an die Art und Weise der Erteilung von Informationen und Mitteilungen. Diese haben in präziser, transparenter, verständlicher und leicht zugänglicher Form in klarer und einfacher Sprache zu erfolgen. Dies bedeutet, dass die Informationen in einfacher Art und Weise unter Vermeidung komplexer Satzstrukturen bereitgestellt werden müssen. Der Inhalt der Information sollte darüber hinaus leicht zu ermitteln sein, es ist daher auf mehrdeutige Begriffe und Interpretationsspielraum zu verzichten. Es gilt das Erfordernis der Schriftform; ggf kann die Information auch elektronisch erfolgen. Eine mündliche Auskunft kann erfolgen, sofern es die betroffene Person verlangt.

Ausdrücklich bezieht sich diese Regelung auf die proaktive Informationspflicht nach Artt 13 und 14 DSGVO, die weiteren Betroffenenrechte nach Artt 15 bis 22 DSGVO und die Benachrichtigung von einer Datenschutzverletzung an die betroffene Person nach Art 34 DSGVO. Die Zurverfügungstellung der Information hat grds unentgeltlich zu erfolgen.

Herausforderung

Betroffene Personen haben den Umfang und die Folgen der Verarbeitung im Vorfeld ermitteln zu können und sollen nicht im Nachhinein von der Art und Weise überrascht werden, in der ihre personenbezogenen Daten verwendet worden sind. Auch im Kontext des Data Spaces müssen Verantwortliche daher zum einen proaktiv Informationen über die Verarbeitung liefern. Zum anderen sollte bei komplexen, technischen oder unerwarteten Verarbeitungsvorgängen gesondert und eindeutig formuliert werden, welche Folgen mit der Verarbeitung der bereitgestellten Daten einhergehen. Das umfasst insb die Art von Auswirkungen, die sich durch die spezifische Verarbeitung von personenbezogenen Daten konkret für die betroffenen Personen ergeben. Betroffene sollen so darüber aufgeklärt werden, ob und welche Risiken mit der Verarbeitung der Daten einhergehen.[25] Im Zusammenhang mit Data Spaces können sich hier Herausforderungen ergeben, wenn die Zwecke der Datenverarbeitung bzw. die teilnehmenden Akteure wechseln. Die Erfüllung der Informationspflicht kann diesfalls mit einem erheblichen Aufwand verbunden sein.

Weiters sollte die Information leicht zugänglich für betroffene Personen sein. Es muss daher leicht und klar ersichtlich sein, wo und wie auf die Information zugegriffen werden kann. Dies kann bspw durch das Zurverfügungstellen der jeweiligen Informationen direkt erfolgen, durch die Bereitstellung eines Links, klare Kennzeichnungen oder auch Pop-Up Fenster.[26] Hierbei ist für die Umsetzung der Data Spaces zu überlegen, durch wen und auf welche Weise die Informationen zur Verfügung zu stellen sind.

4.5.2 Rechtliche Grundlagen

Art 12 DSGVO: Pflicht, die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke zu unterrichten und Modalitäten so festzulegen, dass betroffene Personen die Ausübung der zustehenden Rechte erleichtert wird.

Artt 13 und 14 DSGVO: Informationspflichten des Verantwortlichen.

Die einzelnen Betroffenenrechte (Artt 15 bis 22 DSGVO) sind stets in Verbindung mit Art 12 DSGVO zu lesen.

[25] Art 29-Datenschutzgruppe, Leitlinien für Transparenz gem der VO 2016/679, WP 260, 8.
[26] Art 29-Datenschutzgruppe, Leitlinien für Transparenz gem der VO 2016/679, WP 260, 9.

4.6 Auskunftsrecht der betroffenen Person

4.6.1 Beschreibung und Herausforderung

Beschreibung

Betroffene Personen haben das Recht, von den Verantwortlichen eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden. Hierbei kommt ihnen ua das Recht auf folgende Informationen zu: (i) die Verarbeitungszwecke, (ii) die Kategorien verarbeiteter personenbezogener Daten, (iii) Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt wurden, (iv) die geplante Dauer der Speicherung, sowie (v) das Bestehen eines Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung. Der EuGH hat dieses Recht betroffener Personen in einer rezenten Entscheidung[27] sogar verschärft: Demnach haben Betroffene das Recht, im Rahmen der Informationspflicht des Verantwortlichen Informationen über die konkreten Empfänger:innen zu erhalten, um ihre Rechte nach Artt 16 bis 18 DSGVO wirksam wahrnehmen zu können. Der EuGH stellte jedoch einschränkend fest, dass unter bestimmten Umständen Verantwortliche nicht in der Lage sind, eine detaillierte Auskunft über konkrete Empfänger zu geben. In derartigen Fällen kann die Angabe von Empfängerkategorien bereits ausreichen. Eine Information über die Kategorien von Empfängern statt konkreter Details genügt auch dann, wenn Verantwortliche die Auskunft berechtigterweise verweigern dürfen. Dies kann vor allem dann der Fall sein, wenn es sich um offenkundig unbegründete oder exzessive Anträge der betroffenen Personen handelt. Dabei ist jedoch zu beachten, dass Verantwortliche nachzuweisen haben, dass ein unbegründeter Antrag vorliegt.

Verantwortliche haben den betroffenen Personen zudem eine Kopie der Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen. Bei Auskunftserteilung ist darüber hinaus eine Rechtsbehelfsbelehrung anzuschließen, die das Bestehen weiterer Betroffenenrechte (dh Löschung, Einschränkung, Berichtigung und Widerspruch) sowie das Beschwerderecht bei der Aufsichtsbehörde zu umfassen hat. Der Verantwortliche muss diese Auskunft unverzüglich, dh ohne schuldhaftes Zögern, in der Regel aber innerhalb eines Monats nach Eingang des Antrags erteilen.

Sofern Betroffene einen Antrag auf Auskunftserteilung stellen, haben Verantwortliche die Pflicht, diesem nachzukommen, wenn keine berechtigte Verweigerungsmöglichkeit (siehe oben) vorliegt. Sollten von Verantwortlichen keine Daten mehr verarbeitet werden, sind diese zur "Negativauskunft" verpflichtet

[27] EuGH 12.1.2023, C-154/21 – *Österreichische Post*.

(dh es ist darüber Auskunft zu geben, dass keine Daten mehr verarbeitet werden). Die Nichtreaktion auf den Antrag stellt eine Verletzung des Auskunftsrecht der betroffenen Personen dar.[28]

Grds hat die Auskunft kostenlos zu erfolgen; möchte die betroffene Person mehr als eine Datenkopie erhalten, so können Verantwortliche hierfür ein angemessenes Entgelt auf Grundlage der Verwaltungskosten verrechnen.[29]

Herausforderung

Durch die Vielzahl an Teilnehmern in Data Spaces ist eine Auskunftserteilung gegenüber den betroffenen Personen mit erhöhten Schwierigkeiten verbunden. Oftmals wird vorab nicht klar feststehen, wer die personenbezogenen Daten erhalten bzw. darauf zugreifen wird. Eine Auskunft über die Empfänger der betroffenen Daten kann in solchen Fällen nur generisch erfolgen. Im Lichte der strengen Judikaturlinie des EuGH muss daher im Detail geprüft werden, ob die Angabe der Empfängerkategorien hierbei ausreichend ist.

Darüber hinaus ist insbesondere bei der Verarbeitung einer Vielzahl von Daten ("Big Data") auf eine genaue Zuordnung der jeweiligen Datensätze zu den betroffenen Personen zu achten, um ein allfälliges Auskunftsersuchen auch wahrheitsgetreu (ggf mit einer Negativauskunft) beantworten zu können. Hierbei darf auch nicht außer Acht gelassen werden, dass mit Einlangen des Ersuchens die (maximal) 30-tägige Frist zur Beantwortung zu laufen beginnt. Entsprechend müssen bereits vorab die erforderlichen internen Prozesse zur effektiven Abwicklung von Ansuchen eingerichtet worden sein.

4.6.2 Rechtliche Grundlagen

Art 15 Abs 1 DSGVO: Recht der betroffenen Person, von den Verantwortlichen eine Bestätigung zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden, bzw. ein Auskunftsrecht über die konkreten Umstände der Verarbeitung.

Art 15 Abs 3 DSGVO: Die Verantwortlichen haben eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen.

Art 12 Abs 3 DSGVO: Verantwortliche müssen diese Auskunft unverzüglich, in der Regel aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung stellen.

[28] *Haidinger* in *Knyrim*, DatKomm Art 15 DSGVO, Rz 26 ff.
[29] Art 15 Abs 3 DSGVO.

4.7 Recht auf Datenübertragbarkeit

4.7.1 Beschreibung und Herausforderung

Beschreibung

Verantwortliche haben der Anforderung nach Datenübertragbarkeit nachzukommen. Konkret bedeutet dies, dass Verantwortliche den Betroffenen auf deren Verlangen ihre Daten in einem strukturierten, gängigen und maschinenlesbaren Format zukommen lassen müssen. Ziel ist es hierbei, dass die Daten mit wenig Aufwand weiterverarbeitet werden können. Dementsprechend sind Verantwortliche dazu aufgefordert, interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen. Die Mitlieferung von Metadaten in bestmöglicher Granularitätsstufe wird idR notwendig sein, um die Bedeutung der Information zu erhalten. Zulässige Formate sind grds branchenabhängig, es kommen insb XML, JSON, CSV, HTML und ODF in Betracht.30

Liegen die folgenden vier Voraussetzungen vor, haben Verantwortliche der Pflicht nach Art 20 DSGVO nachzukommen:[31]

- Es muss sich um Daten handeln, welche die Person, die die Übertragung beantragt, betreffen. Ein Antrag, der sich auf anonyme oder ausschließlich auf Daten anderer Personen bezieht, ist abzulehnen.
- Die betroffene Person hat die Daten selbst bereitgestellt oder sie hat ein Verhalten gesetzt, welches dem/der Verantwortlichen die Daten zuführt. Daten, die ein Dritter den verantwortlichen Personen zur Verfügung stellt, unterliegen dem Recht nicht.
- Die Datenverarbeitung basiert auf Einwilligung oder Vertrag; dh das Recht besteht dann, wenn Daten mit Willen der betroffenen Person verarbeitet werden.
- Die Verarbeitung der Daten erfolgt mithilfe automatisierter Verfahren; dh das Recht besteht dann nicht, wenn die Daten mit nicht-automatisierten Dateisystemen verarbeitet wurden.

Verantwortliche Personen haben außerdem dafür Sorge zu tragen, dass die Daten der betroffenen Person ohne Behinderung an einen anderen Verantwortlichen weitergeleitet werden, wenn die betroffene Person dies beantragt. Jede rechtliche, technische oder finanzielle Hürde, durch die ein Verantwortlicher den Datenzugriff, die Datenübertragung oder die Datenwiederverwendung von Seiten

[30] *Haidinger* in *Knyrim*, DatKomm Art 20 DSGVO, Rz 24.

[31] *Jahnel* in *Jahnel*, DSGVO Art 20 Rz 10 ff; *Haidinger* in *Knyrim*, DatKomm Art 20 DSGVO, Rz 18 ff.

der betroffenen Person oder eines anderen Verantwortlichen verlangsamen oder verhindern möchte (z.B. fehlende Dateninteroperabilität) ist als Behinderung zu interpretieren.[32]

Dadurch, dass die betroffene Person selbst Zugriff auf die Daten erhält und diese einem Dritten ohne Behinderung übermitteln kann, verschafft die DSGVO den Betroffenen eine bessere Kontrolle über ihre durch die Verantwortlichen verarbeiteten Daten.[33]

Herausforderung

Data Spaces verfolgen das Ziel, möglichst große Mengen an Daten aus unterschiedlichen Quellen zu poolen und zugänglich zu machen. Unabhängig von datenschutzrechtlichen Erwägungen kommt der Frage der verwendeten Datenformate somit eine überragende Bedeutung zu, damit eine einfache Weiterverwendung der Daten für eine Vielzahl von Data Consumers/Service Providers ermöglicht werden kann.

Der Anspruch auf Datenübertragbarkeit nach DSGVO stellt in dieser Hinsicht noch weitere Anforderungen auf. Um sich einen allfälligen Aufwand, der uU durch die Notwendigkeit einer Umformatierung der Daten vor Herausgabe an die betroffene Person bzw. einen Dritten entsteht, zu ersparen, sollte bereits bei der Einrichtung der Data Spaces darauf geachtet werden, für die Data Provider Datenformate vorzuschreiben, die strukturiert, gängig und maschinenlesbar sind.

4.7.2 Rechtliche Grundlagen

Art 20 DSGVO: Recht auf Datenübertragbarkeit.

4.8 Verzeichnis von Verarbeitungstätigkeiten

4.8.1 Beschreibung und Herausforderung

Beschreibung

[32] *Haidinger* in *Knyrim*, DatKomm Art 20 DSGVO, Rz 25.
[33] ErwGr 68 DSGVO; *Jahnel* in *Jahnel*, DSGVO Art 20, Rz 1; *Haidinger* in *Knyrim*, DatKomm Art 20 DSGVO, Rz 1.

Die Verantwortlichen und Auftragsverarbeitenden trifft die Pflicht, ein schriftliches Verzeichnis aller Verarbeitungstätigkeiten zu führen. Darin enthalten sind ua (i) Name und Kontaktdaten der Verantwortlichen, (ii) die Zwecke der Verarbeitung, (iii) die Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, (iv) die Kategorien von Empfänger:innen, denen die personenbezogenen Daten offengelegt werden, sowie (v) Fristen für die Löschung verschiedener Datenkategorien. [34]

Dieses Verzeichnis ist auf Verlangen der Aufsichtsbehörde auch vorzulegen und soll als "Daten-Landkarte" der Aufsichtsbehörde dazu dienen, Verarbeitungsvorgänge beim Normadressaten zu kontrollieren.[35] Es muss daher anhand der Informationen im Verzeichnis möglich sein, die Rechtmäßigkeit der Verarbeitung der Daten zu überprüfen.[36] Das Verzeichnis hat aufgrund der Rechenschaftspflicht außerdem stets aktuell zu sein.[37]

Die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten gilt nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeitende beschäftigen. Eine Gegenausnahme liegt dann vor, wenn die von diesen Unternehmen vorgenommene Verarbeitung Risiken für die Rechte und Freiheiten betroffener Personen birgt,[38] die Verarbeitung nicht nur gelegentlich erfolgt oder es sich um die Verarbeitung besonderer Datenkategorien oder personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten (iSd Art 10 DSGVO) handelt.[39]

Herausforderung

Ähnlich wie beim Auskunftsrecht der betroffenen Person spielt auch hier die Vielzahl an Teilnehmern in den Data Spaces eine Rolle. Im Verarbeitungsverzeichnis sind ua die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, anzuführen, was im vorliegenden Kontext zu einer erhöhten Komplexität bei der Erstellung des Verarbeitungsverzeichnisses führt. Abhängig vom konkreten Use Case (so z.B. bei Big-Data-Anwendungen) kann es auch Schwierigkeiten bereiten, die relevanten Kategorien betroffener Personen bzw. personenbezogener Daten korrekt zu bestimmen.

[34] *Jahnel* in *Jahnel*, DSGVO Art 30, Rz 1.
[35] *Bogendorfer* in *Knyrim,* DatKomm Art 30 DSGVO, Rz 17.
[36] ErwGr 82 der DSGVO.
[37] *Horn* in *Bergauer/Jahnel/Mader/Staudegger*, jusIT Spezial: DS-GVO (2018) Die Dokumentationspflichten im Verarbeitungsverzeichnis nach Art 30 DS-GVO, 80 f.
[38] Vgl ErwGr 75 DSGVO.
[39] Art 30 Abs 5 DSGVO; Die Gegenausnahme ist damit relativ weit gefasst, sodass vor allem aufgrund des zweiten Tatbestandes (nicht nur gelegentliche Verarbeitung) viele Unternehmen zur Führung eines Verarbeitungsverzeichnisses verpflichtet sind.

4.8.2 Rechtliche Grundlagen

Art 30 DSGVO: Pflicht der Verantwortlichen, ein Verzeichnis aller Verarbeitungstätigkeiten zu führen.

4.9 Sicherheit personenbezogener Daten

4.9.1 Beschreibung und Herausforderung

Beschreibung

Verantwortliche (und Auftragsverarbeitende) haben geeignete technische und organisatorische Maßnahmen (sogenannte "TOMs") zu implementieren, um ein dem Risiko der Datenverarbeitung angemessenes Schutzniveau zu gewährleisten. Hierbei sind der Stand der Technik, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung, sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der von der Datenverarbeitung Betroffenen zu berücksichtigen.[40]

Die dabei von Verantwortlichen zu bedenkenden Risikofälle sind die Vernichtung, der Verlust, die zufällige oder unrechtmäßige Veränderung, sowie die unbefugte Weitergabe bzw der unberechtigte Zugang zu Daten.[41] Es gilt diese Risiken bei der Festlegung des Schutzniveaus zu beachten. Um die Erfüllung geeigneter Sicherheitsmaßnahmen nachzuweisen, kann es uU erforderlich sein, die Einhaltung genehmigter Verhaltensregeln gemäß Art 40 DSGVO oder das Vorhandensein eines genehmigten Zertifizierungsverfahrens gemäß Art 42 DSGVO vorzuweisen.

Herausforderung

Um das Vertrauen in die Data Spaces zu stärken und den betroffenen Personen die nötige Sicherheit zu geben, damit diese in die Verwendung ihrer personenbezogenen Daten einwilligen, muss bei der technischen Umsetzung ein hohes Maß an Cybersicherheit gewährleistet sein. Da sich ein Sicherheitsrisiko bei jedem einzelnen der beteiligten Akteure realisieren könnte, ist ua anzuraten, diese vertraglich auf die Einhaltung gewisser ISO-Normen bzw. Cybersecurity-Standards zu verpflichten.

---

[40] Art 32 DSGVO; *Pollirer* in *Knyrim,* DatKomm Art 32 DSGVO, Rz 20 f.

[41] *Wagner* in *Bergauer/Jahnel/Mader/Staudegger* (Hrsg), jusIT Spezial: DS-GVO (2018) Die Pflichten des Verantwortlichen nach der DS-GVO, 60.

4.9.2 Rechtliche Grundlagen

Art 32 DSGVO: Pflicht des Verantwortlichen und Auftragsverarbeiters geeignete technische und organisatorische Maßnahmen zu implementieren, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

4.10 Datentreuhand beim Datenaustausch

4.10.1 Beschreibung und Herausforderung

Beschreibung

Datentreuhänder können einen entscheidenden Beitrag zu einer fairen Datenordnung für personenbezogene Daten leisten, da sie als Mittler zwischen den die Daten verarbeitenden Akteuren und den von der Verarbeitung betroffenen Personen letztere bei der Ausübung ihrer Rechte unterstützen können. Datentreuhänder können nicht nur die Datensouveränität der betroffenen Personen im Umgang mit ihren Daten stärken, sondern zugleich deren damit verbundenen kommerziellen Verwertungsinteressen besser schützen.

Herausforderung

So vorteilhaft sich das Konzept des Datentreuhänders (gerade im Kontext der Data Spaces) darstellt, so komplex sind die datenschutzrechtlichen Fragen, die sich in diesem Zusammenhang ergeben. Zum einen besteht derzeit kein einheitliches Verständnis des Begriffs des "Datentreuhänders", weshalb unterschiedliche Ausformungen in der Praxis anzutreffen sind. Zum anderen ist nicht absehbar, welche Datentreuhänder-Modelle sich in Zukunft etablieren werden. Grundsätzlich fehlt es derzeit noch an vertieften rechtswissenschaftlichen Untersuchungen zu Datentreuhändern im geltenden Recht. [42]

Bereits die Übermittlung personenbezogener Daten an einen Datentreuhänder ist oftmals an die Zustimmung der Betroffenen gebunden. Eine Problematik kann sich hier daraus ergeben, dass für jene personenbezogenen Daten, die bereits in der Vergangenheit erhoben wurden, regelmäßig keine Einwilligung der betroffenen Person zur Weitergabe an einen Datentreuhänder vorliegen wird, weshalb ggf auf eine andere Rechtsgrundlage für die Datenverabeitung zurückgegriffen werden muss.[43]

[42] Vgl. *Specht-Riemenschneider/Blankertz/Sierek/Schneider/Knapp/Henne*, Die Datentreuhand, MMR 2021, 25 (26 ff); *Kühling*, Der datenschutzrechtliche Rahmen für Datentreuhänder, ZfDR 2021/1, 1 (2 ff).

[43] *Specht-Riemenschneider/Blankertz/Sierek/Schneider/Knapp/Henne*, MMR 2021, 25 (38).

Weitere Herausforderungen ergeben sich bei der Abwicklung datenschutzrechtlicher Einwilligungen über Datentreuhänder. Hierbei gilt es zu differenzieren: Sofern Datentreuhänder nur ein Tool zur Verfügung stellen, um Nutzern einen besseren Überblick über die bei unterschiedlichen Verantwortlichen verarbeiteten Daten zu bieten, birgt dies keine weiteren Herausforderungen, da der Treuhänder in diesem Fall nur als Bote des Nutzenden agiert. Werden dem Datentreuhänder aber eigene Entscheidungsspielräume eingeräumt, wodurch diese eigenen Einwilligungen in fremdem Namen abgibt, oder werden diesem datenschutzrechtliche Gestaltungsrechte abgetreten, stellen sich Fragen der rechtsgültigen Einwilligung iSd Art 7 DSGVO.

Ganz grundsätzlich stellt die Vertretungsmöglichkeit kein Problem hinsichtlich der Einwilligung betroffener Personen dar. Allerdings hat die Einwilligung iSd Art 4 Z 11 DSGVO in informierter Weise zu erfolgen. Dies ist schon für einzelne Anbieter:innen mit komplexen Datenschutzerklärungen und schwer verständlichen Datenverarbeitungsprozessen oftmals problematisch. Wenn nun der Datentreuhänder darüber hinaus in Bezug auf eine Vielzahl derartiger Akteure das Einwilligungsmanagement übernehmen soll, vervielfacht sich auch das Ausmaß an Informationen.

Eine weitere Herausforderung im Zusammenhang mit der Einwilligung ist die notwendige Zweckbestimmtheit. Die betroffene Person kann nur dann die Vorteile und Risiken der Einwilligung einschätzen, wenn sie zum einen in der Lage ist, den Inhalt der Einwilligung zu verstehen und wenn zum anderen die Einwilligungserklärung hinreichend konkret abgefasst ist. Blankoeinwilligungen und pauschal gehaltene Einwilligungserklärungen sind unwirksam. Dies ist bei einem Datentreuhänder, der über eine einzige Einwilligung eine Vielzahl von Datenverarbeitungsprozessen anderer Verantwortlicher legitimieren soll, besonders herausfordernd.[44] Auch das Kriterium der jederzeitigen Widerrufbarkeit der Einwilligung ist im Zusammenhang mit der Datentreuhand komplex.[45]

Insgesamt stellt sich die Einbindung von Datentreuhändern daher als datenschutzrechtlich hochkomplex dar, weshalb vorab eine entsprechende Kosten-Nutzen-Analyse erforderlich sein wird.

4.10.2 Rechtliche Grundlagen

Die datenschutzrechtlichen Anforderungen nach der DSGVO sind uneingeschränkt auf die Datentreuhand anzuwenden.

[44] *Kühling*, ZfDR 2021/1, 1 (9 f).
[45] *Kühling*, ZfDR 2021/1, 1 (11).

Ferner sieht der Data Governance Act spezifische Anforderungen an Datenvermittlungsdienste, dh Bestimmungen zur Regelung der Mittler für gemeinsame Nutzung personenbezogener Daten iSd DSGVO vor.

4.10.3 Lösungsansatz

Datenvermittler oder Datentreuhänder?

Jene Partei, welche die Rolle eines Datentreuhänders übernehmen möchte, sollte sich vorab über die eigene Rolle und Funktion im Klaren werden. Zwischen reinen Vermittlern und einem Treuhänder bestehen deutliche Unterschiede hinsichtlich Erwartung des Kunden sowie in Rechten und Pflichten. Die nachfolgende Gegenüberstellung soll hier ein wenig Klarheit bringen.

Ein **Datenvermittler** ist eine Partei oder eine Organisation, die als Vermittler zwischen Dateninhabern (die Daten bereitstellen) und Datenempfängern (die Daten verwenden) agiert. Datenvermittler erleichtern den Datenaustausch zwischen verschiedenen Parteien, indem sie Plattformen, Infrastruktur oder Dienstleistungen bereitstellen, die den Datenfluss unterstützen. Sie könnten technische Lösungen, Kommunikationskanäle oder sogar Vertragsvereinbarungen anbieten, um den sicheren und reibungslosen Datenaustausch zu ermöglichen. Datenvermittler könnten in verschiedenen Branchen eingesetzt werden, wie z. B. im E-Commerce, bei Datenmarktplätzen oder in der Cloud-Computing-Branche.

Ein **Datentreuhänder** ist eine vertrauenswürdige dritte Partei, die die Verantwortung für den Schutz und die Verwaltung von Daten im Auftrag von Dateninhabern oder Datenverarbeitern übernimmt. Der Datentreuhänder könnte spezifische Aufgaben im Zusammenhang mit dem Datenschutz wahrnehmen, wie beispielsweise die Überwachung der Einhaltung von Datenschutzbestimmungen, die Sicherung von sensiblen Daten oder die Kontrolle des Datenzugriffs. Sie können aber auch über diese Aufgaben hinaus gehen und Dienste wie zum Beispiel die Speicherung, die Aufbereitung, die Anonymisierung oder die Lizenzierung von Daten anbieten. Der Datentreuhänder handelt im besten Interesse der Dateninhaber und bemüht sich, die Datenschutzrechte und -pflichten zu wahren. Die konkrete Form des Datentreuhänders ist nach Modellen geregelt. Diese Modelle können je nach Anwendungsbereich, Zielsetzung und Rahmenbedingungen unterschiedlich gestaltet werden.

Insgesamt gesehen besteht der Hauptunterschied darin, dass ein Datenvermittler eher als Vermittler oder Dienstleister agiert, der den Datenaustausch zwischen Parteien erleichtert, während ein Datentreuhänder eine aktivere Rolle im Schutz und der Verwaltung der Daten übernimmt, um sicherzustellen, dass die Datenschutzprinzipien eingehalten werden.

Vertragliche Vereinbarungen

Gemäß Artikel 28 der DSGVO müssen Datenverantwortliche (Auftraggeber) und Datentreuhänder (Auftragsverarbeiter) eine schriftliche Vereinbarung treffen, in der die Modalitäten der Datenverarbeitung festgelegt werden. Diese Vereinbarung muss mindestens folgende Elemente enthalten:

a) **Gegenstand und Dauer der Verarbeitung:** Die Vereinbarung sollte den Gegenstand und die Dauer der Verarbeitung definieren, einschließlich des Zwecks der Verarbeitung sowie der Kategorien von personenbezogenen Daten und betroffenen Personen.
b) **Art und Zweck der Verarbeitung:** Es muss klargestellt werden, wie die personenbezogenen Daten verarbeitet werden, um den vertraglichen Anforderungen des Auftraggebers zu entsprechen.

c) **Pflichten des Datentreuhänders:** Die Vereinbarung muss die Pflichten des Datentreuhänders festlegen, darunter die Verpflichtung zur Einhaltung der Datenschutzbestimmungen, zur Implementierung von angemessenen Sicherheitsmaßnahmen und zur Unterstützung des Auftraggebers bei der Erfüllung seiner datenschutzrechtlichen Pflichten.

d) **Rechte und Pflichten des Auftraggebers:** Die Vereinbarung sollte die Rechte und Pflichten des Auftraggebers in Bezug auf die Kontrolle und Überwachung der Datenverarbeitung festlegen.

e) **Vertraulichkeit:** Die Vertraulichkeit der personenbezogenen Daten und die Verpflichtung zur Geheimhaltung müssen explizit festgehalten werden.

f) **Unterstützung bei Anfragen betroffener Personen:** Der Datentreuhänder muss den Auftraggeber bei der Erfüllung von Anfragen betroffener Personen, wie beispielsweise Anfragen zur Ausübung ihrer Datenschutzrechte, unterstützen.

g) **Überwachung und Kontrolle:** Die Modalitäten zur Überwachung und Kontrolle der Datenverarbeitung müssen festgelegt werden.

Einwilligung

Der Kunde muss der Verarbeitung der Daten durch einen Datentreuhändler zustimmen und ggf. rückwirkend der Verarbeitung bereits übergebener Daten zustimmen. Es sollte bei jedem Kunden eine umfangreiche Bestätigung für die Verarbeitung und Übermittlung bereits übermittelter Daten sowie zukünftiger Daten eingeholt werden. Dies sollte durch den Datenverantwortlichen (Auftraggeber) erfolgen.

Der Kunde muss in einem verständlichen und überschaubaren Format über die Art und Weise der zweckmäßigen Datenverarbeitung in Kenntnis gesetzt werden. Pauschal und Blanko Einwilligungen sind

nicht zulässig. Es gilt ein Format zu entwerfen, welches klar und übersichtlich über die Verwendbarkeit der Daten informiert. Nebst einer detaillierten rechtlichen Formulierung würde es sich anbieten einen leichter verständlichen Text, ein Schaubild oder eine Liste zu verwenden, um übersichtlicher über die Verwendung der Daten zu informieren.

Im Gegensatz zum Datentreuhänder, muss ein Datenvermittler eine solche Einwilligung nicht einholen, sofern er keine eigenständige Verarbeitung oder Nutzung der Daten durchführt, sondern lediglich den technischen und logistischen Aspekt des Datentransfers erleichtern. Sobald ein Datenvermittler jedoch im Rahmen seiner Dienstleistungen personenbezogene Daten verarbeitet (speichert), die ihm von Kunden oder anderen Datenquellen zur Verfügung gestellt wurden, gilt dies als Auftragsdatenverarbeitung. In diesem Fall muss der Datenvermittler als Auftragsverarbeiter handeln und die Anforderungen der ADV erfüllen.

Pflichten eines Datentreuhänders aus Sicht des Datenverantwortlichen

Ein Datentreuhänder spielt eine entscheidende Rolle bei der Gewährleistung des Datenschutzes und der Datensicherheit im Rahmen des Datenaustauschs. Die korrekte Umsetzung der Pflichten eines Datentreuhänders ist von größter Bedeutung, um die Vertraulichkeit, Integrität und Verfügbarkeit der übertragenen Daten zu wahren. Die nachfolgenden Punkte dienen als Leitfaden.

1. **Identifizierung des Bedarfs:** Überlegen Sie, welche Datenverarbeitungsvorgänge von einem externen Dienstleister durchgeführt werden könnten, um die Verantwortung für die Datenverarbeitung auszulagern.

2. **Klare Definition der Pflichten:**

3. **Auswahl eines Datentreuhänders:** Bevor Sie einen externen Dienstleister als Datentreuhänder in Betracht ziehen, recherchieren Sie sorgfältig und wählen Sie einen zuverlässigen Anbieter aus, der nachweislich Erfahrung in der datenschutzkonformen Datenverarbeitung hat.

4. **Vertragliche Vereinbarung und Pflichten:** Erstellen von vertraglicher Vereinbarung zwischen dem Unternehmen (Datenverantwortlicher) und dem Datentreuhänder (Auftragsverarbeiter). Stellen Sie sicher, dass die Pflichten des Datentreuhänders klar definiert sind. Dies umfasst die Überwachung des Datenaustauschs, die Sicherstellung der Einhaltung von Datenschutzvorschriften und die Verwaltung des Datenzugriffs. Die Vereinbarung sollte klar und präzise sein und alle erforderlichen rechtlichen Elemente gemäß Artikel 28 der DSGVO enthalten.

5. **Datensicherheit gewährleisten:** Sicherstellen, dass der Datentreuhänder angemessene technische und organisatorische Maßnahmen zum Schutz der verarbeiteten Daten implementiert hat. Dies umfasst Aspekte wie Zugangskontrolle, Verschlüsselung, Datensicherung und Notfallpläne.

6. **Schulung und Sensibilisierung:** Schulung der Mitarbeiter und des Managements über die Zusammenarbeit mit einem Datentreuhänder und die Bedeutung der Datenschutzkonformität. Sensibilisieren Sie sie für die Verantwortlichkeiten und Pflichten im Zusammenhang mit der Datenverarbeitung. Gleiches gilt für den Datentreuhänder und dessen Mitarbeiter:Innen.

7. **Überwachung und Kontrolle:** Implementieren eines Überwachungssystems, um sicherzustellen, dass der Datentreuhänder die vereinbarten Maßnahmen einhält und die Datenverarbeitung gemäß den Datenschutzvorschriften erfolgt.

8. **Dokumentation:** Halten Sie Vereinbarungen und Maßnahmen in schriftlicher Form fest. Dies dient sowohl der internen Dokumentation als auch möglichen Nachweisen gegenüber Datenschutzbehörden.

9. **Regelmäßige Überprüfung (Audit):** Führen Sie regelmäßige Überprüfungen der Zusammenarbeit mit dem Datentreuhänder durch, um sicherzustellen, dass die Datenschutzstandards aufrechterhalten werden und Änderungen in den datenschutzrechtlichen Bestimmungen berücksichtigt werden. Dies kann interne Überprüfungen und unabhängige externe Prüfungen umfassen.

10. **Datenminimierung und -speicherung:** Halten Sie den Datentreuhänder an, sich an das Prinzip der Datenminimierung zu halten und die übertragenen Daten nur so lange wie nötig zu speichern. Daten, die nicht mehr benötigt werden, sollten in Übereinstimmung mit den geltenden Gesetzen gelöscht werden.

Zusammenfassung

Ein Datentreuhänder sollte klar definieren welche Rolle (welches Modell) er übernimmt, inwieweit er die Daten selbst weiterverarbeiten und weitergeben darf und welche rechtlichen Implikationen sich somit ergeben. Definieren und Erstellen einer Matrix welche verwendende / verwaltete Daten basierend auf deren Einfluss auf Änderungen im Einwilligungsverhältnis darstellt, um zu verstehen ab welchem Grad und Verarbeitungsschritt durch einen Treuhändler neue Einwilligungen des Kunden benötigt werden.

Weiterführende Informationen

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) bietet eine Hotline und eine Website, die Hilfe bei Problemen mit Datenvermittlern und Datentreuhändern bietet.

https://www.bfdi.bund.de/SharedDocs/Adressen/DE/EuropaeischeDatenschutzbeauftragte/Oesterreich.html

EuroDaT ist ein europäischer Datentreuhänder, der mit seinem einzigartigen Prinzip der Datentransaktionen den sicheren und rechtskonformen Austausch von Daten zwischen beliebigen

Parteien sicherstellt und unabhängige Analysen auf gemeinsamen Daten ermöglicht1. EuroDaT bietet ein umfangreiches Paket an Dienstleistungen, Templates und Systemlösungen an, um eine maßgeschneiderte Datentransaktion aufzubauen. Man kann sich auf ihrer Webseite über ihr Angebot informieren.

https://www.eurodat.org/

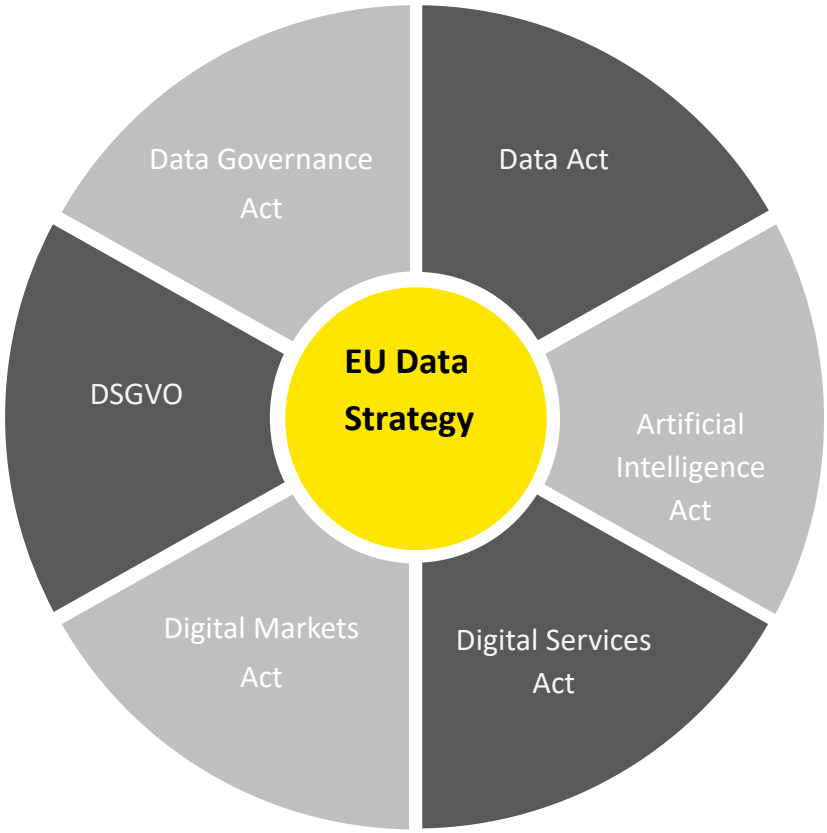
Datenschutzbehörde Österreich

https://www.dsb.gv.at/

5 Übersicht EU-Regelwerke, Herausforderungen und Ausblick auf zukünftige Rechtsfragen[46]

Dieses Kapitel enthält Informationen zur EU-Datenstrategie zum Stand September 2023.

5.1 Überblick über die EU Data Strategy im Einzelnen



Im Folgenden sollen die aus unserer Sicht für die Implementierung der Data Spaces zentralen EU-Regelwerke näher vorgestellt werden, wobei sich die Darstellung

[46] Bitte beachten Sie bei der Lektüre, dass einige der dargestellten Rechtsakte lediglich Entwürfe sind und es daher noch zu weitreichenden Änderungen kommen kann, wodurch die dargestellten Informationen nicht mehr aktuell / falsch werden können.

potenzieller Herausforderungen – wie mit dem Auftraggeber abgestimmt – auf jene im Zusammenhang mit dem Data Governance Act beschränken werden.

Regelwerk	Umfang und Datenart	Zielsetzung und Relevanz	Anwendungsbereich	Status
Data Governance Act (DGA)	• Personenbezogene sowie nicht personenbezogene Daten • vertrauliche Daten • Daten, die den Schutz geistigen Eigentums Dritter genießen	• Schaffung von Governance-Modellen für gemeinsame Nutzung • Stärkung des Vertrauens in Datenvermittler • Bereitstellung von Daten des öffentlichen Sektors zur Wiederverwendung • Erleichterung des Datenaustauschs in der EU und mit Drittländern durch Dienste für den Datenaustausch	• Öffentlicher Sektor • "vertrauenswürdige" Dienste zur gemeinsamen Nutzung von Daten • Einzelpersonen	• Vorschlag 25.11.2020; • politische Einigung 10.12.2021; • in Kraft getreten: 23.06.2022; • anwendbar: 24.09.2023
Data Act (DA)	• Daten, die durch die Nutzung eines vernetzten Produktes/ verbundenen Dienstes generiert werden • hauptsächlicher Anwendungsfall: IoT-Daten	• Aufbrechen von Datenmonopolen und -silos • Ordnungsgemäße Nutzung von und Zugang zu Daten • Schutz von KMU • Betroffene erhalten neue Rechte und alte Rechte werden gestärkt	• Organisationen, die über IoT-Daten verfügen • Öffentliche Einrichtungen und EU-Institutionen • Datenverarbeitungs- und Cloud-Computing-Dienste	• Vorschlag 23.02.2022 • Abänderung des Europäischen Parlaments vom 13.03.2023 (Annahme des Gesetzesentwurfs) • Einigung EU-Parlament und Mitgliedstaaten Juni 2023 • Formelle Bestätigung ist noch ausständig

Regelwerk	Umfang und Datenart	Zielsetzung und Relevanz	Anwendungsbereich	Status
Artificial Intelligence Act (AIA)	• primär Einstufung von KI-Systemen anhand eines risikobasierten Ansatzes • sekundär betrifft der AIA auch gemischte Daten, personenbezogene und nicht personenbezogene Daten	• Verbesserung der Vorhersehbarkeit • Optimierung der Abläufe und der Ressourcenzuweisung • Personalisierung der Dienstleistungserbringung durch den Einsatz von KI • Gewährleistung von Rechtssicherheit zur Erleichterung von Investitionen und Innovationen im KI-Bereich	• Anbieter:innen, die KI-Systeme auf dem EU-Binnenmarkt in Verkehr bringen • Nutzer:innen von KI-Systemen in der EU • Anbieter:innen und Nutzer:innen von KI-Systemen in einem Drittland, dessen Output in der EU verwendet wird	• Vorschlag[47] 21.04.2021 • Annahme der Verhandlungsposition des Parlaments am 14.06.2023 • Verhandlungen in EU-Mitgliedstaaten – Ziel: Einigung bis Ende 2023 • möglicherweise anwendbar: 2024

5.2 Data Governance Act (DGA)

Der DGA ist ein sektorübergreifendes Instrument, das darauf abzielt, eine Vielzahl von derzeit ungenutzten Daten verfügbar zu machen, indem es die Weiterverwendung öffentlich zugänglicher bzw. vorgehaltener Daten regelt. Der DGA gilt sowohl für personenbezogene als auch für nicht-personenbezogene Daten. Potenziell könnte der DGA z.B. die Wiederverwendung von GPS- oder Gesundheitsdaten, die vom öffentlichen Sektor gesammelt wurden, für kommerzielle oder nichtkommerzielle Zwecke bedeuten.

[47] Es können sich daher noch weitreichende Änderungen bei den Vorgaben des Data Acts ergeben, die die folgenden Ausführungen obsolet werden lassen können. Aktuelle Entwicklungen sind daher jedenfalls zu verfolgen.

Ziel ist daher nicht, Rechte an Daten zu gewähren, zu ändern oder aufzuheben, sondern einen Rahmen zu schaffen, in welchem die Verwendung geschützter Daten erlaubt ist.

Mit dem DGA werden darüber hinaus zuverlässige Datenvermittlungsdienste eingeführt, die Einzelpersonen bei der Ausübung ihrer Rechte gemäß der DSGVO helfen sollen. Nach der Intention des europäischen Gesetzgebers sollen diese Datenvermittler beim Aufbau einer gemeinsamen Datenökonomie eine zentrale Rolle spielen und sowohl von Dateninhaber:innen als auch von Datennutzer:innen unabhängig sein. Darüber hinaus soll der DGA auch den Datenaltruismus erleichtern, d.h. Verfahren, bei denen Unternehmen oder Einzelpersonen freiwillig Daten öffentlich zugänglich machen. Dementsprechend besteht die Möglichkeit, dass sich eine Organisation als altruistische Organisation registrieren lässt.

Insgesamt ist das Zusammenspiel mit den bestehenden Rechtsvorschriften, z.B. mit der DSGVO, nicht abschließend geklärt. Der DGA führt eine breite Definition von "Daten" ein, die auch personenbezogene Daten umfasst. Daher würden die DSGVO und der DGA gleichzeitig gelten, wobei der DGA die DSGVO nicht verdrängt. Vielmehr is bei Überschneidungen des DGA mit der DSGVO letztere vorrangig anwendbar.

5.2.1 Potenzielle Herausforderungen und Lösungsansätze

Bei der Umsetzung der Data Spaces ist neben der DSGVO auch der DGA zu berücksichtigen. Im Folgenden sollen die aus unserer Sicht zentralen Punkte des DGA kurz erläutert werden.

Einwilligung und Betroffenenrechte der DSGVO

Herausforderung: Die Einwilligung und Betroffenenrechte aus der DSGVO dürfen nicht delegiert werden, weshalb die Anforderungen der DSGVO für die rechtmäßige Verarbeitung personenbezogener Daten auch im Rahmen des DGA immer streng zu beachten sind (ErwGr 4, 7, 15 DGA). Demnach ist auch darauf zu achten, für welche bestimmten Zwecke und welche bestimmte Kategorie an Stakeholdern (oder Use Cases) die Daten zur Verfügung gestellt werden. Ggf sind mehrere konkrete Einwilligungen einzuholen (Problem der Generaleinwilligung in die Datenverarbeitung).

Dienste zur Einwilligungsverwaltung als Datenvermittlungsdienste im Sinne des Art 10 DGA

Herausforderung: Um einen direkten Austausch zwischen Daten-Anbieter:innen und Daten-Konsument:innen gewährleisten zu können, wird im DGA die Funktion der Datenvermittler:innen vorgesehen. Die Aufgaben der Vermittler:innen sind vielfältig, wobei sie insbesondere das Vertrauen zwischen den beiden Seiten stärken sollen (ErwGr 33 DGA). Dementsprechend müssen diese neutral sein, und dürfen die Daten nicht für eigene wirtschaftliche Zwecke nutzen.

Aufgrund dessen unterliegen Datenvermittlungsdienste einem Anmeldeverfahren nach Art 11 DGA: Die Anmeldung erfolgt bei der für Datenvermittlungsdienste zuständigen Behörde, wobei Art 11 Abs 6 DGA Anforderungen an die Anmeldung festlegt. Erst nach Anmeldung kann die Tätigkeit der Datenvermittlung aufgenommen werden (Art 11 Abs 4 DGA). Ferner sieht Art 12 DGA weitere Bedingungen für die Erbringung von Datenvermittlungsdiensten vor:

- Das Verfahren für den Zugang zu einem Dienst hat transparent, fair und nichtdiskriminierend zu sein, zudem haben die Anbieter über Verfahren zu verfügen, um betrügerische oder missbräuchliche Praktiken in Bezug auf Parteien zu verhindern, die über seine Datenvermittlungsdienste Zugang zu erlangen suchen.
- Der Austausch der Daten hat die Interoperabilität innerhalb und zwischen Sektoren zu verbessern.
- Datenvermittlungsdienste können ein Angebot zusätzlicher spezifischer Werkzeuge und Dienste für Dateninhaber:innen oder betroffene Personen umfassen, insbesondere um den Datenaustausch zu erleichtern (z. B. vorübergehende Speicherung, Pflege, Konvertierung, Anonymisierung und Pseudonymisierung), wobei diese Werkzeuge nur auf ausdrücklichen Antrag oder mit Zustimmung der Dateninhaber:innen oder der betroffenen Person verwendet werden.
- Die Art 10 bis 14 DGA sind jedoch nicht auf altruistische Organisationen und andere Einrichtungen ohne Erwerbszweck anwendbar, soweit deren Tätigkeit darin besteht, für Ziele von allgemeinem Interesse Daten zu erheben, die von natürlichen oder juristischen Personen auf Grundlage des Datenaltruismus zur Verfügung gestellt werden, es sei denn diese Organisationen und Einrichtungen sind bestrebt, Geschäftsbeziehungen zwischen einer unbestimmten Zahl von betroffenen Personen und Dateninhabern einerseits und Datennutzern andererseits herzustellen (Art 15

DGA).

Potenzielle Lösungsansätze:

In der Praxis fungieren Datenvermittler als neutrale Dritte, die Einzelpersonen und Unternehmen verbinden. Die Umsetzung der Pflichten für Datenvermittlungsdienste gemäß dem DGA ist von entscheidender Bedeutung, um den Schutz der Privatsphäre und die Sicherheit der Daten zu gewährleisten. In diesem Lösungsansatz werden praktische Schritte und Ansätze beleuchtet, wie Unternehmen diese Pflichten erfolgreich umsetzen können.

1. Registrierung und Meldepflichten:
Um die gesetzlichen Anforderungen zu erfüllen, sollten Unternehmen, die Datenvermittlungsdienste anbieten möchten, den Registrierungsprozess bei der zuständigen Aufsichtsbehörde sorgfältig durchlaufen. Dies beinhaltet die Bereitstellung aller erforderlichen Informationen über das Unternehmen, seine Geschäftspraktiken und Datenschutzrichtlinien. Zudem ist es entscheidend, klare Meldepflichten zu etablieren, um bei Sicherheitsverletzungen oder unbefugtem Zugriff schnell zu reagieren und die betroffenen Nutzer zu benachrichtigen.

2. Datenschutz und Sicherheit:

Die Implementierung von robusten Sicherheitsmaßnahmen ist unerlässlich, um den Schutz der übermittelten Daten sicherzustellen. Unternehmen sollten in fortschrittliche Verschlüsselungstechnologien, Zugangskontrollen und Intrusion-Detection-Systeme investieren. Regelmäßige Sicherheitsaudits und Penetrationstests sollten durchgeführt werden, um potenzielle Schwachstellen aufzudecken und zu beheben.

3. Neutralität und Fairer Zugang:

Um Neutralität sicherzustellen, sollten Unternehmen eine separate rechtliche Entität schaffen, die als Schnittstelle zwischen Dateninhabern und -nutzern fungiert. Dies gewährleistet, dass keine Interessenkonflikte auftreten. Der Zugang zum Dienst sollte transparent gestaltet sein und Diskriminierung vermeiden, um eine faire Nutzung für alle Beteiligten zu gewährleisten. Unternehmen sollten klare Richtlinien für den Zugang zum Datenvermittlungsdienst festlegen und sicherstellen, dass alle Nutzer gleichermaßen

behandelt werden. Dies bedeutet, dass keinem Nutzer aufgrund seiner Größe, seines finanziellen Status oder seiner Beziehung zum Anbieter bevorzugter Zugang gewährt wird.

4. Vergütung der Datenvermittlung:

Der Datenvermittler kann für seine Dienste eine Gebühr erheben. Im Sinne der DSGVO ist darauf zu achten, dass sich diese Gebühr nur auf die Vermittlung, jedoch nicht auf die Verarbeitung der Daten bezieht. Andernfalls sind weitere Voraussetzungen wie das Einholen der Einwilligung u.a. zu beachten. Im Sinne einer Vermittlung ziehen nur der Dateninhaber und der Datenverarbeiter einen direkten finanziellen Mehrwert aus der Verarbeitung der Daten.

5. Informationspflichten und Zweckgebundenheit:

Eine klare und verständliche Kommunikation mit den Nutzern ist entscheidend. Datenschutzrichtlinien und Nutzungsbedingungen sollten leicht zugänglich sein und die Art und Weise erklären, wie Daten verarbeitet und genutzt werden. Zudem ist es wichtig sicherzustellen, dass die vermittelten Daten ausschließlich für die vorgesehenen Zwecke genutzt werden und nicht missbraucht werden. Die Informationspflichten und Zweckgebundenheit konzentrieren sich auf die Handlungen der Auftraggeber der Datenvermittler selbst, während der Datentreuhänder eine externe Instanz ist, die in den Prozess einbezogen werden kann, um die Einhaltung der Datenschutzbestimmungen sicherzustellen.

6. Insolvenzabsicherung und Interoperabilität:

Die Implementierung eines Plans zur Aufrechterhaltung des Dienstes im Falle einer Insolvenz ist entscheidend, um die Kontinuität für Dateninhaber und -nutzer zu gewährleisten. Unternehmen sollten auch sicherstellen, dass ihre Datenvermittlungsdienste mit anderen Diensten interoperabel sind, indem sie ein standardisiertes Datenformat verwenden und Daten nicht eigenmächtig umwandeln.

7. Schulung und Zusammenarbeit:

Die Schulung der Mitarbeiter über die Pflichten gemäß dem DGA und die Bedeutung des Datenschutzes ist von großer Bedeutung. Unternehmen sollten eng mit den zuständigen

Aufsichtsbehörden zusammenarbeiten, um bei der Umsetzung der Pflichten Unterstützung und Klarheit zu erhalten.

Die Umsetzung der Pflichten für Datenvermittlungsdienste gemäß dem Data Governance Act erfordert eine ganzheitliche und proaktive Herangehensweise. Durch die Schaffung einer starken Sicherheitsinfrastruktur, klare Kommunikation mit den Nutzern und die enge Zusammenarbeit mit den Aufsichtsbehörden können Unternehmen das Vertrauen in den Datenaustausch stärken und die Vorteile einer vernetzten digitalen Wirtschaft maximieren.

Datenaltruismus

Herausforderung: Im Kontext des DGA bedeutet “Datenaltruismus“ die freiwillige gemeinsame Nutzung von Daten für Ziele von allgemeinem Interesse auf der Grundlage der Einwilligung betroffener Personen oder einer Erlaubnis anderer Dateninhaber zur Nutzung ihrer nicht personenbezogenen Daten, ohne hierfür ein Entgelt zu fordern oder zu erhalten, das über eine Entschädigung für die durch die Bereitstellung ihrer Daten entstandenen Kosten hinausgeht.

Datenaltruistische Organisationen haben sich zu registrieren (Art 17 ff DGA), wobei Art 18 DGA weitere Anforderungen an die Eintragung festlegt. Einrichtungen, die im Sinne des Art 18 DGA als altruistische Organisationen eingetragen sind, können einen Antrag auf Eintragung in das Register der anerkannten datenaltruistischen Organisationen stellen (Art 19 DGA). Daraus ergeben sich weitere Pflichten (wie Transparenzanforderungen gemäß Art 20 DGA, oder Anforderungen zum Schutz der Rechte und Interessen betroffener Personen und Dateninhaber gemäß Art 21 DGA).

Potenzielle Lösungsansätze:

Wenn Unternehmen Daten auf eine datenaltruistische Weise teilen möchten, indem sie Daten für gemeinnützige Zwecke freiwillig und ohne Entgelt zur Verfügung stellen, müssen sie bestimmte Schritte gemäß den Vorgaben des DGA befolgen.

Die notwendigen Tätigkeiten die für eine datenaltruistische Teilung notwendig sind:

- Unternehmen müssen sich im Register der Datenaltruistischen Unternehmen eintragen lassen, um altruistisch Daten teilen zu können.
- Unternehmen müssen einen Antrag auf Eintragung im Register der anerkannten datenaltruistischen Organisationen stellen.
- Unternehmen müssen die Transparenzanforderungen erfüllen und über die Nutzung, Ziele und Art der geteilten Daten informieren.
- Unternehmen müssen den Schutz der Rechte und Interessen der betroffenen Personen und Dateninhaber gewährleisten, einschließlich Maßnahmen zur Wahrung der Privatsphäre und Sicherheit der Daten.
- Unternehmen sollten Mechanismen zur Überwachung der Nutzung der geteilten Daten und zur regelmäßigen Berichterstattung über ihre datenaltruistischen Aktivitäten implementieren.

In Ergänzung sollten Unternehmen ihre gemeinnützigen Ziele klar und präzise definieren, um zu verdeutlichen, welche gesellschaftlichen Belange sie durch die uneigennützige Datenfreigabe unterstützen möchten. Diese Ziele können soziale, wissenschaftliche, gesundheitliche oder ökologische Aspekte umfassen. Zu berücksichtigen ist um eine datenaltruistische Datenfreigabe durchzuführen, ist die ausdrückliche Einwilligung der betroffenen Personen oder die ausdrückliche Erlaubnis anderer Dateninhaber zur Verwendung der nicht personenbezogenen Daten erforderlich. Diese Zustimmung sollte freiwillig und umfassend informiert sein. Es ist ratsam, die Einwilligung oder Erlaubnis vor dem Start der Datenerhebung einzuholen, die Betroffenen transparent über die Verwendung zu informieren und auch den Widerruf ermöglichen.

Um eine die Transparenz zu gewährleisten können Unternehmen wie folgt vorgehen:

- Sie führen vollständige und genaue Aufzeichnungen über alle Personen, denen sie die Datenverarbeitung erlaubt haben, sowie über den Zeitpunkt, die Dauer, den Zweck und die Gebühren der Datenverarbeitung
- Sie erstellen einen jährlichen Tätigkeitsbericht und übermitteln ihn der zuständigen Behörde, in dem sie Informationen über ihre Tätigkeiten, die geförderten Zwecke von allgemeinem Interesse, die Datenverarbeitenden, die Ergebnisse der Datenverarbeitung und ihre Einnahmen und Ausgaben darlegen
- Bei der Datenverteilung sollten Datenaltruistische Organisationen die Datennutzenden zusätzlich aufklären. Die Datennutzende sollten darauf hingewiesen werden, dass sie ihre Einwilligung oder Erlaubnis jederzeit widerrufen können, wenn

Personen die Erlaubnis zur Nutzung widerrufen. Somit ist eine Aktualisierung der Daten auch jederzeit möglich. Hierdurch kann es auch einen wiederholten Erlaubnisantrag benötigen.

Unternehmen, die Daten nutzen wollen, die durch Datenaltruismus freigegeben wurden, sollten darauf achten, dass die Datenschutzgesetze, Zweckbindung, Datensicherheit, Offenlegung der Verwendung (Transparenz) einhalten. Um Klarheit des Nutzungsrahmens und weitere Compliance-Regulierungen zu bekommen, können hier Lizenzvereinbarungen zwischen Datenaltruistische Organisationen und den Datennutzern abgeschlossen werden.

5.3 Data Act (DA)

Der Data Act, welcher noch formal beschlossen werden muss, legt gemeinsame Grundregeln dafür fest, wer Daten in allen Wirtschaftssektoren nutzen und darauf zugreifen darf. Nach Ansicht der Kommission wird dies dazu beitragen, eine Fülle von Industriedaten zu erschließen, die derzeit ungenutzt sind, und dabei für Fairness in der Datenwertschöpfungskette zwischen allen Beteiligten der Datenwirtschaft sorgen. Der Vorschlag zielt darauf ab, insbesondere den Zugang zu und die Nutzung von nicht-personenbezogenen Daten zu erleichtern, einschließlich Business-to-Business (B2B), Business-to-Consumer (B2C) und Business-to-Government (B2G). Außerdem sollen die Kunden von Datenverarbeitungsdiensten (einschließlich Cloud Computing) leichter den Dienstanbieter wechseln können.

Der DA soll den DGA-Rahmen für die gemeinsame Nutzung von Daten des privaten Sektors mit dem öffentlichen Sektor ergänzen. So sieht er unter anderem die Möglichkeit vor, dass öffentliche Einrichtungen und EU-Institutionen im Falle eines "außergewöhnlichen Bedarfs", z.B. bei öffentlichen Notfällen, Pandemien oder Katastrophen, freien Zugang zu den Daten von Unternehmen erhalten.

5.3.1 Datenverkauf und Weitergabe generiert aus vernetzten Produkten

Wenn Sie als Datenverkäufer im Rahmen des Data Act in der Europäischen Union (EU) tätig sind, gibt es einige wichtige Überlegungen und Maßnahmen, die Sie ergreifen sollten, um die Einhaltung sicherzustellen und die Vorteile des rechtlichen Rahmens optimal zu

nutzen. Zunächst ist es von entscheidender Bedeutung, ein klares Verständnis Ihrer Daten zu haben, einschließlich ihres Typs, ihrer Quelle, ihrer Qualität und eventueller damit verbundener Rechte oder Beschränkungen, bevor Sie Daten verkaufen. Zudem sollten Sie sicherstellen, dass die Daten, die Sie verkaufen, Qualitätsstandards erfüllen und den Datenschutzbestimmungen, wie der Datenschutz-Grundverordnung (DSGVO), entsprechen.

Wenn es sich um personenbezogene Daten handelt, ist es wichtig, Anonymisierungs- oder Pseudonymisierungstechniken anzuwenden, um die Privatsphäre der betroffenen Personen zu schützen. Ebenso sollten Sie detaillierte Aufzeichnungen und Dokumentationen über die von Ihnen verkauften Daten führen, einschließlich Datenverwendungsrichtlinien, Einwilligungen und relevanter Vereinbarungen.

Beachten Sie die Anforderungen des Data Act in Bezug auf faire Vertragsbedingungen, um unfairer Behandlung von Vertragspartnern, insbesondere kleinen und mittleren Unternehmen (KMUs), vorzubeugen. Schließlich ist es ratsam, rechtlichen Rat einzuholen, um sicherzustellen, dass Ihre Datenfreigabepraktiken und -vereinbarungen mit dem Data Act und anderen relevanten Vorschriften in Einklang stehen.

Um als Datenverkäufer einen Mehrwert den Konsumenten bieten zu können, könnte man statt nur Rohdaten anzubieten, Daten aggregieren und Analysen durchführen, um Kunden Einblicke und Erkenntnisse zu liefern, die über die Rohdaten hinausgehen. Hier gäbe es auch die Möglichkeit über Datenberatungen Einblicke in die Daten gewährleisten, sowie Vorschläge für die Nutzung zusätzlicher und passender Datenquellen zu geben. Zusätzlich könnte man den Kunden Garantien hinsichtlich der Qualität und Genauigkeit der bereitgestellten Daten gewähren. Dies kann die Attraktivität der Daten erhöhen.

Als Datenkonsument sollten Sie zunächst Ihre Datenbedürfnisse und -ziele klar definieren, bevor Sie Daten erwerben. Stellen Sie sicher, dass die von Ihnen beabsichtigten Datenkäufe mit Ihren geschäftlichen Zielen übereinstimmen. Bei der Auswahl von Datenanbietern ist es wichtig, die Qualität, Genauigkeit und Relevanz der angebotenen Daten sorgfältig zu bewerten. Mindern Sie das Risiko schlechter Entscheidungen und verschwendeter Ressourcen durch die Überprüfung der Datenqualität. Achten Sie darauf, dass die von Ihnen erworbenen Daten den Datenschutzvorschriften, insbesondere der DSGVO, entsprechen, und stellen Sie sicher, dass sensible Daten angemessen behandelt

und geschützt werden. Verstehen Sie die Nutzungsrichtlinien des Datenanbieters, einschließlich etwaiger Einschränkungen bei der Datennutzung und -weitergabe. Bei Verhandlungen über Datenfreigabevereinbarungen sollten Sie auf faire und transparente Bedingungen achten, die Ihren Anforderungen entsprechen. Nutzen Sie die Rechte zur Datenportabilität, die Ihnen durch den Data Act gewährt werden, um die Übertragung von Daten zwischen Dienstleistern zu erleichtern, falls dies erforderlich ist.

Beide Seiten, sowohl Datenverkäufer als auch -konsumenten, sollten den Datenhandel und -erwerb mit Transparenz, Fairness und Einhaltung als grundlegende Prinzipien angehen, da der Data Act darauf abzielt, eine ausgewogene und florierende Datenwirtschaft in der EU zu schaffen. Die Einhaltung seiner Bestimmungen ist für alle Beteiligten von entscheidender Bedeutung, um die Vorteile des Datenaustauschs in vollem Umfang zu nutzen.

5.3.2 Nutzung Mustervertragsklauseln in Verträgen, um missbräuchliche Klauseln zu vermeiden.

Die Einführung von Mustervertragsklauseln durch die Kommission dient dazu, in Verträgen eine einheitliche und rechtlich akzeptable Formulierung für bestimmte Klauseln bereitzustellen. Diese Klauseln sind vor allem in internationalen Verträgen wichtig, um sicherzustellen, dass die darin enthaltenen Bestimmungen den gesetzlichen Anforderungen entsprechen und die Rechte und Pflichten der Vertragsparteien klar definiert sind. Hier ist eine kurze Erklärung dazu, wie Sie diese Mustervertragsklauseln in eigene Verträge einpflegen können und was sie bedeuten:

Identifizieren Sie die relevanten Mustervertragsklauseln: Zuerst müssen Sie die spezifischen Mustervertragsklauseln identifizieren, die für Ihren Vertrag relevant sind. Diese Klauseln können je nach Art des Vertrags variieren und könnten beispielsweise Datenschutzbestimmungen, Geheimhaltungspflichten oder Haftungsausschlüsse umfassen.

Kopieren und Einfügen: Sie können die von der Kommission bereitgestellten Mustervertragsklauseln in Ihren eigenen Vertrag kopieren und an den entsprechenden

Stellen einfügen. Beachten Sie dabei, dass Sie die Klauseln möglicherweise an die spezifischen Bedürfnisse und Anforderungen Ihres Vertrags anpassen müssen.

Anpassung an den Vertrag: Es ist wichtig sicherzustellen, dass die eingefügten Mustervertragsklauseln mit dem Rest Ihres Vertrags in Einklang stehen und dass sie die spezifischen Details und Vereinbarungen widerspiegeln. Dies kann Änderungen oder Ergänzungen der Klauseln erfordern.

Rechtliche Beratung: Bei komplexen Verträgen oder wenn Sie unsicher sind, wie Sie die Mustervertragsklauseln am besten anpassen sollen, sollten Sie rechtliche Beratung in Anspruch nehmen. Ein Anwalt kann Ihnen helfen, sicherzustellen, dass Ihr Vertrag den geltenden Gesetzen entspricht und Ihre Interessen angemessen schützt.

Was die Bedeutung der Mustervertragsklauseln betrifft, so dienen sie dazu, eine rechtliche Grundlage für bestimmte Vertragsbedingungen zu schaffen, die häufig in internationalen Geschäftsbeziehungen auftreten. Sie sollen sicherstellen, dass die Vertragsparteien klare und faire Bedingungen haben, die die Einhaltung der geltenden Gesetze und Vorschriften gewährleisten. Die genaue Bedeutung jeder Klausel hängt von ihrem Inhalt und ihrem Zweck ab, daher ist es wichtig, diese sorgfältig zu prüfen und gegebenenfalls anzupassen, um sicherzustellen, dass sie Ihren Anforderungen entsprechen.

5.4 AI Act (AIA)

Der AIA baut weitgehend auf einem risikobasierten Ansatz auf, bei dem zwischen unterschiedlichen Leveln an Risiko aufgrund der Anwendung künstlicher Intelligenz (KI) differenziert wird:

- 1. ein inakzeptables Risiko, wie Social Scoring oder der Einsatz von KI zur Ausbeutung von Kindern oder schutzbedürftigen Personen;
- 2. ein hohes Risiko, wie dem Einsatz von KI zur Bewertung des Rückfallrisikos eines ehemaligen Häftlings, dem Einsatz von KI zur Bewertung von Prüfungen oder dem Einsatz einer KI-Anwendung bei robotergestützten Operationen;
- 3. ein geringes Risiko, wie der Einsatz von KI-Systemen wie Chatbots;

- 4. ein minimales Risiko, das die bei weitem größte Kategorie darstellt und beispielsweise den Einsatz von KI-gestützten Videospielen oder Spam-Filtern umfasst.

Der AIA wird sich hauptsächlich auf Systeme konzentrieren, die ein hohes Risiko für die Grundrechte und Sicherheit darstellen, und diesen Transparenz- und Dokumentationspflichten auferlegen. Eine begrenzte Anzahl von Systemen mit "inakzeptablem Risiko" wird vollständig verboten: Diese Systeme werden als im Widerspruch zu grundlegenden EU-Werten angesehen. Je niedriger das Risiko, welches mit der Nutzung des KI-Systems verbunden ist, desto geringere Pflichten wird der AIA vorsehen.

5.5 Weitere potenzielle Herausforderungen und thematisch relevante Rechtsgebiete

Neben den in diesem Orientierungsbericht erwähnten Rechtsakten, können etliche weitere Rechtsgebiete und damit zusammenhängende Rechtsfragen zur Beurteilung des Datenaustausches relevant sein.

Zu beachten sind etwa folgende weitere Herausforderungen.

Einräumung von Nutzungsrechten an Daten / Vertragsrecht

Herausforderung: Häufig sollen Daten bzw. aus Daten gewonnene Erkenntnisse / Produkte / Dienstleistungen kommerzialisiert werden. Es ist daher von Bedeutung, bereits frühzeitig zu klären, wer über Daten verfügungsberechtigt ist. Von diesen Personen ist eine entsprechende Rechteeinräumung zu erhalten (abseits von etwaig datenschutzrechtlich relevanten Sachverhalten). Es ist daher wichtig bereits frühzeitig ein möglichst umfassendes Vertragswerk iZm der Nutzung von Daten aufzusetzen.

Potenzielle Lösungsansätze:

Folgende Informationen sollten in einem Vertrag festgehalten werden, um die Einräumung von Nutzungsrechten an Daten im Einklang mit den geltenden Gesetzen und Best Practices im Vertragsrecht sicherzustellen:

2. **Zweck und Verwendungszweck:** Der Vertrag sollte ausführlich beschreiben, zu welchem Zweck die Daten werden aus dem Blickwinkel beider Parteien verwendet werden. Einerseits zu welchem Zweck die Daten aus Sicht des Bereitstellers verwendet werden dürfen. Aus Sicht des Datenverwerters kann dies eine detaillierte Aufschlüsselung der geplanten Verwendungszwecke und Aktivitäten umfassen, um Missverständnisse zu vermeiden.
3. **Geistiges Eigentum:** Berücksichtigen Sie die Frage des geistigen Eigentums an den Daten. Klären Sie, ob die Daten gemeinsames Eigentum sind oder ob eine Partei alleiniges Eigentum hat oder etwaige Dritte ein teilweises Eigentum an den Daten haben. Dies kann Auswirkungen auf die Rechteeinräumung und die Nutzung haben. Sollten dritte Parteien involviert sein, so sollte klar hervorgehen, wie das Nutzungsrecht und das geistige Eigentum geregelt ist und welche Partei diese pflegen muss.
4. **Dauer der Lizenz:** Legen Sie fest, wie lange die Nutzungsrechte an den Daten gelten sollen. Dies kann eine zeitlich begrenzte Lizenz sein oder eine unbegrenzte, jedoch sollte die Dauer klar definiert sein.
5. **Einschränkungen und Verbote:** Bestimmen Sie, welche Handlungen oder Verwendungen der Daten ausdrücklich verboten sind. Dies kann beispielsweise die Weitergabe der Daten an Dritte ohne Zustimmung, die Dekompilierung von Daten oder die Erstellung von abgeleiteten Werken umfassen.
6. **Datensicherheit:** Der Vertrag sollte Anforderungen an die Datensicherheit und den Schutz personenbezogener Daten festlegen, um sicherzustellen, dass die Daten angemessen geschützt werden.
7. **Datenschutz und Compliance:** Erwähnen Sie ausdrücklich, dass die Parteien sich dazu verpflichten, alle geltenden Datenschutz- und Datenschutzbestimmungen einzuhalten, insbesondere in Bezug auf personenbezogene Daten.
8. **Aktualisierungen und Änderungen:** Klären Sie, wie Aktualisierungen oder Änderungen an den Daten behandelt werden. Dies könnte erfordern, dass Änderungen schriftlich vereinbart werden, um Missverständnisse zu vermeiden.
9. **Geheimhaltung:** Legen Sie fest, dass die Parteien vertrauliche Informationen und Daten vertraulich behandeln und angemessene Maßnahmen zum Schutz der Vertraulichkeit ergreifen müssen.
10. **Auflösung bei Verstoß:** Definieren Sie die Konsequenzen im Falle eines Verstoßes gegen die Vertragsbedingungen, einschließlich der Möglichkeit zur Vertragskündigung und etwaiger Schadenersatzforderungen.
11. **Anwendbares Recht und Gerichtsstand:** Bestimmen Sie, welches Recht und welcher Gerichtsstand im Falle von Streitigkeiten gilt, um Rechtssicherheit zu schaffen.

Um **Data Consumer** bei der Nutzung der Daten zu unterstützen, könnten folgende Lösungen genutzt werden:

- Online-Foren und Communities: Durch das Einrichten von Online-Foren oder Communities, in denen Datennutzer Erfahrungen, Best Practices und Fragen austauschen können, fördert man die Zusammenarbeit und den Wissensaustausch.
- Webinare und Schulungen: Voreingerichtete Webinare, Schulungen und Workshops anbieten, um den Umgang mit den Daten sowie die rechtlichen Rahmenbedingungen näherzubringen.
- Use-Case-Beispiele: Das teilen von praktischen Beispielen und Anwendungsfällen, wie Daten erfolgreich genutzt und korrekt kommerzialisiert wurden. Dies kann anderen Datennutzern Ideen und Inspiration geben.

Abgrenzung, ob urheberrechtlich geschützte "Datenbankwerke" vorliegen

Herausforderung: Es ist stets zu klären, ob urheberrechtlich geschützte Datenbankwerke betroffen sind; das Ergebnis ist in den vertraglichen Dokumenten entsprechend festzuhalten.

Potenzielle Lösungsansätze:

Die Herausforderung, festzustellen, ob urheberrechtlich geschützte Datenbankwerke betroffen sind und dies in den vertraglichen Dokumenten festzuhalten, erfordert eine sorgfältige Prüfung und rechtliche Klarheit. Hier sind einige Möglichkeiten, wie Sie diese Herausforderung angehen können:

- **Urheberrechtsprüfung:** Führen Sie gründliche Recherchen durch, um festzustellen, ob die verwendeten Datenbankwerke urheberrechtlich geschützt sind. Dies kann die Überprüfung von Datenbankregistern und Rechteinhaberinformationen einschließen.
- **Lizenzvereinbarungen:** Wenn die Datenbankwerke urheberrechtlich geschützt sind, überprüfen Sie die existierenden Lizenzvereinbarungen oder Nutzungsbedingungen, um festzustellen, ob und wie Sie die Daten nutzen dürfen.
- **Urheberrechtliche Einwilligung:** Wenn die Datenbankwerke urheberrechtlich geschützt sind und keine bestehenden Nutzungsrechte vorliegen, holen Sie schriftliche

Einwilligung von den Rechteinhabern ein, um die Daten zu verwenden. Dies kann in Form von Lizenzverträgen oder Genehmigungsschreiben erfolgen.

- **Vertragliche Klarheit:** Passen Sie Ihre vertraglichen Dokumente an, um die klare Zustimmung zur Nutzung urheberrechtlich geschützter Datenbankwerke zu reflektieren. Dies sollten die genauen Bedingungen, Dauer und den Umfang der Nutzung festhalten.
- **Rückversicherung durch Rechtsberatung:** Wenn Sie unsicher sind oder komplexe urheberrechtliche Fragen auftreten, konsultieren Sie einen Anwalt oder eine Anwältin, um sicherzustellen, dass Ihre vertraglichen Vereinbarungen den rechtlichen Anforderungen entsprechen.
- **Haftungsregelungen:** Klären Sie in den Vertragsdokumenten die Haftung im Falle von urheberrechtlichen Verstößen oder Streitigkeiten. Dies kann die Verantwortung für Schäden und Rechtskosten regeln.
- **Überwachung und Aktualisierung:** Halten Sie die Verträge regelmäßig auf dem neuesten Stand, um sicherzustellen, dass sie den aktuellen rechtlichen Anforderungen entsprechen, insbesondere wenn sich die rechtliche Situation ändert.
- **Dokumentation:** Halten Sie alle Schritte zur Klärung des Urheberrechts und zur Erlangung von Nutzungsrechten sorgfältig schriftlich fest. Dies dient der Nachweisbarkeit und rechtlichen Absicherung.

Nachfolgend sind einige Möglichkeiten aufgeführt, welche in Zukunft diese Prüfungen einfacher gestalten können:

- **Datenbank-Metadaten und Lizenzinformationen:** Erstellen Sie eine umfassende Datenbank mit Metadaten und Lizenzinformationen für alle Datenbankwerke. Diese Datenbank kann Informationen über den Urheber, die Lizenzbedingungen und die Verwendungsmöglichkeiten enthalten.
- **Lizenzierungstools:** Entwickeln Sie benutzerfreundliche Online-Tools, mit denen Datennutzer die Lizenzbedingungen für jedes Datenbankwerk schnell und einfach überprüfen können. Diese Tools könnten Symbole oder Farbcodes verwenden, um die Lizenzbedingungen zu kennzeichnen.
- **Lizenzmanager:** Bieten Sie einen Lizenzmanager an, der Datennutzern hilft, die von ihnen erworbenen Lizenzen zu verwalten. Dieser Manager kann Erinnerungen für Lizenzverlängerungen senden und den Status der Lizenzen verfolgen.
- **Training und Schulungen:** Bieten Sie Schulungen und Schulungsmaterialien an, die Datennutzer dar-über informieren, wie sie urheberrechtlich geschützte

Datenbankwerke rechtmäßig nutzen können. Dies kann Schulungen zur Fair Use-Doktrin und zur korrekten Zitierweise von Datenbanken umfassen.

- **Nutzerbewertungen und Feedback:** Implementieren Sie eine Plattform für Nutzerbewertungen und -feedback, auf der Datennutzer ihre Erfahrungen mit der Nutzung von Datenbankwerken und den Um-gang mit Lizenzen teilen können. Dies kann anderen Nutzern bei der Auswahl von Datenbanken helfen.
- **Clearing-Stelle für Urheberrechte:** Richten Sie eine Clearing-Stelle oder einen Kundendienst ein, an die sich Datennutzer wenden können, wenn sie Fragen zur Lizenzierung oder zur rechtmäßigen Nutzung von Datenbankwerken haben. Fachleute können ihnen dann weiterhelfen.
- **Community für Lizenzexpertise:** Schaffen Sie eine Community von Lizenzexperten und -nutzern, die ihr Wissen teilen und Fragen zur Lizenzierung und Nutzung von Datenbankwerken beantworten können.
- **Open Access Initiativen:** Ermutigen Sie zur Teilnahme an Open Access Initiativen, bei denen Datenbankwerke unter offenen Lizenzbedingungen verfügbar gemacht werden. Dies erleichtert die Nutzung und den Austausch von Daten.

Zusammenspiel der geplanten Regelwerke mit bereits bestehenden nationalen Gesetzen und Verordnungen der EU

Herausforderung: Die Begrifflichkeit "Daten" wird beispielsweise vom DGA breiter definiert als in der DSGVO, wonach "Daten" auch nicht-personenbezogene Daten umfassen. Für jeden konkreten Sachver-halt ist daher zu klären, welche "Daten" vorliegen und damit verbundene Rechtsfolgen bzw. Wechselwir-kungen zwischen den einzelnen (EU) Rechtsakten.

Potenzielle Lösungsansätze:

- **Datenkatalog und Metadaten:** Data Producer sollten einen detaillierten Datenkatalog erstellen, der Informationen über die Art der Daten, ihre Herkunft, ihre Qualität und ihre Bedeutung enthält. Data Consumer können diese Metadaten verwenden, um die Daten besser zu verstehen.
- **Standardisierung:** Wenn möglich, sollten Data Producer und Data Consumer gemeinsame Standards und Terminologien verwenden, um Missverständnisse zu vermeiden. Dies kann die Interoperabilität verbessern.
- **Klare Kommunikation:** Eine offene und klare Kommunikation ist entscheidend. Data Consumer und Data Producer sollten frühzeitig miteinander sprechen, um ihre

Erwartungen, Anforderungen und Beschränkungen zu besprechen.

Datensicherheit und einzuhaltende technische Standards

Herausforderung: Nationale bzw. branchenspezifische Regelungen sehen oftmals spezielle Anforderungen an die technische Umsetzung von Datenverarbeitungsvorgängen vor.

Notwendigkeit des Schutzes als "Geschäftsgeheimnisses"

Herausforderung: Daten verfügen oftmals über einen kommerziellen Wert. Sofern diese Geschäftsge-heimnisse darstellen, sind entsprechende (vertragliche) Schutzmechanismen vorzusehen, um die Ver-traulichkeit auch bei Herausgabe an Dritte weiterhin gewährleisten zu können.

Potenzielle Lösungsansätze zur Sicherung von Geschäftsgeheimnissen und Vertraulichkeit unter Einfluss des Data Governance Act (DGA):

Herausforderung: Daten verfügen oftmals über einen kommerziellen Wert. Sofern diese Geschäftsgeheimnisse darstellen, sind entsprechende (vertragliche) Schutzmechanismen vorzusehen, um die Vertraulichkeit auch bei Herausgabe an Dritte weiterhin gewährleisten zu können.

- **Vertragsabschlüsse und Vertraulichkeitsvereinbarungen:** Unternehmen sollten mit Dritten, die Zugang zu ihren geschäftlichen Daten und Informationen benötigen, strenge Non-Disclosure Agreements (NDAs) abschließen. Diese Verträge legen fest, dass die Dritten vertrauliche Informationen nicht weitergeben oder für eigene Zwecke verwenden dürfen. Dies gilt insbesondere bei der Weitergabe von Daten an Dritte, um sicherzustellen, dass Geschäftsgeheimnisse geschützt werden.
    - Werden Daten an öffentliche Stellen übermittelt, so sollten spezielle Vertraulichkeitsvereinbarungen ausgehandelt werden. Diese Vereinbarungen können sicherstellen, dass Dritte die Daten nur für die vereinbarten Zwecke verwenden dürfen und dass die Vertraulichkeit der Daten gewahrt bleibt, selbst wenn Dritte die Daten von der öffentlichen Stelle erhalten haben. Öffentliche Stellen sind beispielsweise staatliche oder kommunale Institutionen.

- **Begrenzung des Datenzugangs und Sicherheit:** Die Begrenzung des Datenzugangs bedeutet, dass Unternehmen den Zugang zu geschäftlichen Daten auf das Notwendigste beschränken sollten. Nur autorisierten Personen oder autorisierten dritten Parteien sollte der Zugang gewährt werden. Dies stellt sicher, dass sensible Informationen nicht in die falschen Hände geraten.
    - Zusätzlich zur Begrenzung des Zugangs sollten Unternehmen angemessene Sicherheitspraktiken implementieren, um die Daten vor unbefugtem Zugriff oder Verlust zu schützen. Dies kann die Verwendung von Verschlüsselungstechnologien, Firewall-Systemen und Zugriffskontrollen umfassen.

    - Die Pseudonymisierung und Anonymisierung von Daten sind Techniken, die verwendet werden können, um die Vertraulichkeit zu wahren, während die Daten für bestimmte Zwecke weiterverwendet werden. Pseudonymisierung beinhaltet die Ersetzung von Identifikatoren durch andere Kennungen, während Anonymisierung die Entfernung aller Identifikationsmerkmale aus den Daten bedeutet.

    - Der Zugang zu Daten sollte auf personalisierte (personenbezogene) Zugänge beschränkt sein und nicht rollenbasiert (Gruppe) umgesetzt werden. So sind erlaubte und unerlaubte Zugriffe nachvollziehbar. Änderungen an den Zugängen sollten möglichst automatisch festgehalten werden. Dies umfasst die betroffene Person sowie die die Änderung auslösende Person.

- **Integration von DGA-Bestimmungen in Verträge:** Dieser Schritt bezieht sich darauf, dass Unternehmen sicherstellen sollten, dass die Anforderungen des Data Governance Act (DGA) in ihre bestehenden Verträge und Vereinbarungen mit Dritten integriert werden. Die DGA-Anforderungen betreffen die Weiterverwendung der Daten durch öffentliche Stellen und die damit verbundenen Vertraulichkeitsanforderungen.

    - Das bedeutet, dass Unternehmen explizite DGA-Klauseln in ihre Verträge aufnehmen sollten. Diese Klauseln sollten die Einhaltung der DGA-Vorschriften sicherstellen, insbesondere in Bezug auf die Vertraulichkeit von Daten, wenn sie von öffentlichen Stellen weitergegeben werden.

    - Durch die Integration von DGA-Bestimmungen in Verträge stellen Unternehmen sicher, dass sie gesetzliche Anforderungen erfüllen und die

Vertraulichkeit von Daten wahren, wenn diese Daten mit Dritten geteilt werden.

- **Prüfung von Datenübertragungen:** Dieser Schritt bezieht sich auf die Überprüfung von Datenübertragungen in Nicht-EU-Drittländer. Wenn Daten an Dritte außerhalb der Europäischen Union übertragen werden, müssen Unternehmen sicherstellen, dass diese Übertragungen den Anforderungen des Data Governance Act (DGA) entsprechen.

    - Die DGA kann Anforderungen an die Datenübertragung in Drittländer vorsehen, einschließlich der Prüfung der Gleichwertigkeit der Schutzmaßnahmen in diesen Ländern. Dies bedeutet, dass Unternehmen sicherstellen sollten, dass die Schutzmaßnahmen in Nicht-EU-Drittländern den Standards der DGA entsprechen.

    - Standardvertragsklauseln können verwendet werden, um sicherzustellen, dass Datenübertragungen in Nicht-EU-Drittländer rechtmäßig und sicher erfolgen. Unternehmen sollten sicherstellen, dass solche Klauseln in den Vereinbarungen mit Dritten enthalten sind, um die DGA-Anforderungen zu erfüllen.

- **Nutzung des Single Information Point (SIP) gemäß DGA:** Der "Single Information Point" ist eine Einrichtung, die gemäß Artikel 8 des Data Governance Act (DGA) eingerichtet wird. Diese Einrichtung wird von den zuständigen Behörden der Mitgliedsstaaten bereitgestellt und soll als zentrale Anlaufstelle dienen. Unternehmen können den SIP nutzen, um Informationen über öffentliche Datenquellen zu erhalten und sicherzustellen, dass sie die gesetzlichen Anforderungen bei der Anfrage und Nutzung dieser Daten einhalten. Der SIP trägt zur Transparenz und Effizienz bei der Nutzung von öffentlichen Daten bei. Der SIP hat zwei Hauptfunktionen:

    - Informationen für Dritte bereitstellen: Der SIP stellt Informationen über die verfügbaren öffentlichen Daten und die Bedingungen für deren Weiterverwendung bereit. Dies ermöglicht Dritten, die Interesse an der Nutzung dieser Daten haben, den rechtlich sicheren Zugriff auf relevante Informationen.

- Unterstützung bei Datenanfragen: Der SIP kann bei Datenanfragen behilflich sein, indem er sicherstellt, dass die Anfragen den gesetzlichen Anforderungen entsprechen. Dies trägt zur Einhaltung der DGA-Vorschriften bei.

- **Förderung der Datennutzung durch Startups und KMU gemäß DGA:** Der Data Governance Act (DGA) fördert die Nutzung von Daten, insbesondere durch Startups (neugegründete Unternehmen) und kleine und mittlere Unternehmen (KMU). Ziel ist es Innovationen und wirtschaftliches Wachstum zu unterstützen.
    - Unternehmen können diese Initiative unterstützen, indem sie sicherstellen, dass die Vertraulichkeit und der Schutz von Geschäftsgeheimnissen gewährleistet sind, wenn sie Daten an Startups und KMUs weitergeben. Dies kann durch den Abschluss von Vertraulichkeitsvereinbarungen und die Überprüfung der Sicherheitspraktiken der Empfänger erfolgen.

    - Die Förderung der Datennutzung durch Startups und KMUs trägt zur Entwicklung von datengesteuerten Innovationen bei und ermöglicht es kleinen Unternehmen, auf öffentliche Daten zuzugreifen, um neue Produkte und Dienstleistungen zu entwickeln.

Zusammengefasst stellen die Integration von DGA-Bestimmungen in Verträge und die Prüfung von Datenübertragungen sicher, dass Datenübertragungen in Übereinstimmung mit den gesetzlichen Anforderungen erfolgen und die Vertraulichkeit der Daten gewahrt bleibt, insbesondere wenn Daten in Nicht-EU-Drittländer übertragen werden. Dies trägt zur Einhaltung der DGA-Vorschriften bei.

Nationale Gegebenheit iZm Daten

Herausforderung: Es sind stets allfällige Öffnungsklauseln in den EU-Verordnungen und darauf aufbauend die jeweiligen Umsetzungsbestimmungen in den Mitgliedstaaten zu beachte

6 Disclaimer

Dieser Orientierungsbericht ist lediglich als allgemeine, unverbindliche Information gedacht und kann daher nicht als Ersatz für eine detaillierte Recherche oder eine fachkundige Beratung oder Auskunft dienen. Diese Orientierungsbericht ist stellt keine Rechtsberatung dar und hat keinen Anspruch auf Vollständigkeit, sondern dient lediglich als Diskussionsgrundlage. Es wurden von DIO mit Unterstützung durch EY erstellt und beleuchtet lediglich einzelne von DIO ausgewählte Schwerpunkte. Explizit nicht vereinbart – und nicht durchgeführt – war/wurde eine ganzheitliche Analyse.

Etliche der in diesem Orientierungsbericht besprochenen Rechtsakte befinden sich derzeit noch im Entwurfsstadium. Diese Rechtsakte können daher entweder gar nicht oder in (vollständig) abgeänderter Form beschlossen und damit rechtsverbindlich werden. Folglich können die in diesem Orientierungsbericht getroffenen Aussagen ungültig bzw. falsch werden. Ebenso gibt es zu diesen Rechtsakten – mögen sie auch beschlossen sein – keine/kaum juristische Literatur. Die in diesem Orientierungsbericht dargestellte Ansicht / Zusammenfassung der Rechtsakte kann daher – selbst bei beschlossenen Rechtsakten – von der Interpretation von Behörden, der herrschenden Meinung, sich entwickelnder Literatur oder Dritten abweichen. Es besteht daher kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität. Jegliche Haftung wird ausgeschlossen.

Dieser durch EY unterstützte Orientierungsbericht beruht auf den an EY von DIO überlassenen Unterlagen und mündlich und/oder schriftlich erteilten Auskünften sowie dem auf dieser Basis zu Grunde gelegten Sachverhalt bzw. den getroffenen Annahmen. Dieser Orientierungsbericht beschränkt sich auf die darin ausdrücklich getroffenen Aussagen; er enthält keine darüber hinaus gehenden ausdrücklichen oder schlüssigen Aussagen oder Zusicherungen. Der Orientierungsbericht behandelt keine steuerlichen, finanziellen, strategischen, operativen, kommerziellen, umwelt- oder versicherungsrechtlichen Fragen.

Dieser Orientierungsbericht wurde für und gemeinsam mit DIO im Rahmen der geschlossenen Leistungs-vereinbarung erstellt. Dieser Orientierungsbericht enthält keinen Rat, keine Auskunft und kein Gutachten und ist nicht dazu bestimmt als Entscheidungsgrundlage zu dienen. Wir übernehmen ohne ausdrückliche gesonderte

abweichende Vereinbarung Dritten gegenüber keinerlei Verpflichtungen, Verantwortung oder Sorgfaltspflichten (keine Dritthaftung).

Tabellenverzeichnis

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

Abbildungsverzeichnis

Literaturverzeichnis

Nachname, Vorname: Titel des Buchabschnitts. In: Nachname, Vorname/Nachname, Vorname (Hg.): Titel des Buches. Münster: Musterverlag 1889, Bd. 12, 10. Aufl., S. 21–25.

Nachname, Vorname/Nachname, Vorname: Titel des Buchabschnitts. In: Nachname, Vorname/Nachname, Vorname (Hg.): Titel des Buches. Münster: Musterverlag 1889, Bd. 12, 10. Aufl., S. 21–25.

Abkürzungen

Abk.	Abkürzung
BGBl.	Bundesgesetzblatt
Art.	Artikel
usw.	und so weiter

Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Radetzkystraße 2, 1030 Wien
+43 (0) 800 21 53 59
servicebuero@bmk.gv.at
bmk.gv.at