universität wien

# MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

**„Datenverarbeitung auf Grundlage einer Once-Only-Plattform“**

verfasst von / submitted by

Mag. Verena Schmid

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

Master of Laws (LL.M.)

Wien, 2023 / Vienna 2023

| | |
|---|---|
| Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet: | UA 992 942 |
| Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet: | Informations- und Medienrecht |
| Betreut von / Supervisor: | Ao. Univ.-Prof. Dr. Dietmar Jahnel |

# Inhaltsverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| DSB | Datenschutzbehörde |
| DSG | Datenschutzgesetz, BGBl I 1999/165 idF BGBl I 2021/148 |
| DSGVO | Datenschutz-Grundverordnung, Verordnung (EU) 2016/679 |
| E-GovG | E-Government-Gesetz, BGBl I 2004/10 idF BGBl I 2022/119 |
| EMRK | Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten, BGBl 1958/210 |
| ErwGr | Erwägungsgrund |
| GRC | Charta der Grundrechte der Europäischen Union |
| ISMS | Informationssicherheits-Managementsystem |
| IVDB | Informationsverpflichtungsdatenbank |
| IVP | Informationsverpflichtungen |
| Prozess ZAWAS | Prozess zur Auswahl angemessener Sicherheitsmaßnahmen |
| RSV | Register- und Systemverbund |
| SDG-VO | Single-Digital-Gateway-Verordnung, Verordnung (EU) 2018/1724 |
| stRsp | ständige Rechtsprechung |
| USPG | Unternehmensserviceportalgesetz, BGBl I 2009/52 idF BGBl I 2021/142 |

# Einleitung

Die Digitalisierung schreitet in allen Lebensbereichen voran, weshalb auch Staat und Verwaltung tiefgreifenden Veränderungen gegenüberstehen. Diese Veränderungen haben sie nicht nur anzunehmen, sondern auch aktiv zu gestalten, wodurch sie die vielfältigen Aufgaben noch besser erfüllen und ihrer Verantwortung gerecht werden können.[1] Die Potenziale der Digitalisierung im Bereich des Verwaltungshandelns reichen von der Gestaltung optimaler Rahmenbedingungen für Wirtschaft und Gesellschaft über die Verbesserung der Infrastruktur bis hin zu einer effektiveren Verwaltungsarbeit.[2] Beispielsweise kann die Auslastung der Verwaltung präziser prognostiziert werden, Ressourcen können effektiver eingesetzt, Prozesse vereinfacht und Schnittstellen automatisiert werden.[3]

Eine der Grundlagen für effizientes und verlässliches Verwaltungshandeln sind Daten aus Registern, die von verschiedenen Behörden zur Erfüllung öffentlicher Aufgaben verwendet werden.[4] Oftmals sind Anbringen an die Behörden mit zahlreichen Nachweispflichten verbunden, wobei bestimmte Informationen immer wieder von Bürger:innen und Unternehmen abgefragt werden.[5] Entsprechend dem Grundsatz „Once Only" sollen bei der Datenverarbeitung durch Verwaltungsbehörden zuerst alle zur Verfügung stehenden Daten genutzt werden, bevor sie von Bürger:innen und Unternehmen erneut abgefragt werden. Der Grundsatz der einmaligen Erfassung von Daten führt zu einer Entbürokratisierung und Effizienzsteigerung und ermöglicht die Durchführung automatisierter Verfahren.[6] Das „Once-Only-Prinzip" ist Teil des EU-E-Government-Aktionsplans 2016-2020[7] und wird von zahlreichen Mitgliedstaaten in verschiedenen Projekten umgesetzt.

---

[1] *Stocksmeier*, Potenziale der digitalen Transformation für die deutsche Verwaltung in Bertelsmann Stiftung (Hrsg), Digitale Transformation der Verwaltung (2017) 10.
[2] *Stocksmeier*, Potenziale der digitalen Transformation für die deutsche Verwaltung 10.
[3] *Stocksmeier*, Potenziale der digitalen Transformation für die deutsche Verwaltung 11.
[4] *Parycek* in *Mayrhofer/Parycek*, Digitalisierung des Rechts – Herausforderungen und Voraussetzungen, 21. ÖJT Band IV/1 (2022) 34 f.
[5] *Jahnel* in *Jahnel/Mader/Staudegger* (Hrsg), IT-Recht[4] (2020) 507.
[6] Vgl *Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung in *Raschauer*, Forschungen aus Staat und Recht 174 (2014) 9.
[7] *Stocksmeier/Wimmer/Führer/Essmeyer*, Once-Only in Deutschland und Europa: Eine Roadmap grenzüberschreitender Vernetzung im Bereich Steuern in *Räckers* et al (Hrsg), Digitalisierung von Staat und Verwaltung, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2019, 87.

In Österreich konnten bereits einige „Once-Only-Initiativen“ etabliert werden.[8] So werden seit 2015 die Anspruchsvoraussetzungen für die Familienbeihilfe antragslos und automatisiert geprüft und erforderliche Informationen durch den Datenaustausch mit anderen öffentlichen Stellen eingeholt.[9] Der Zugang zu relevanten Daten setzt unter anderem eine Verknüpfung mit digitalen Nachweisen und Registern sowie standardisierten Schnittstellen zu den Datenquellen voraus, was eine Vielzahl an datenschutzrechtlichen Fragestellungen eröffnet.[10]

Mit Kundmachung der Änderung des Unternehmensserviceportalgesetzes am 26. Juli 2021 wurde die Errichtung einer Once-Only-Plattform vorgesehen.[11] Diese Once-Only-Plattform soll nach § 6 USPG aus dem Register- und Systemverbund und der Informationsverpflichtungsdatenbank bestehen, wobei diese zwei Konstrukte unterschiedliche Zwecke verfolgen. Über den Register- und Systemverbund soll der Datenaustausch erfolgen und die Informationsverpflichtungsdatenbank soll Informationen über Meldepflichten enthalten, jedoch keine Daten selbst. Im Rahmen dieser Arbeit werden datenschutzrechtliche Fragestellungen hinsichtlich des auf dem Register- und Systemverbund basierenden Datenaustauschs unter Behörden behandelt. Neben den datenschutzrechtlichen Grundlagen und der Rechtmäßigkeit der Datenverarbeitung werden Anforderungen hinsichtlich der Betroffenenrechte sowie der technischen und organisatorischen Maßnahmen erörtert. Ebenso wird die Rolle der Informationsverpflichtungsdatenbank als Teil der Once-Only-Plattform sowie mögliche Herausforderungen diskutiert.

Das Ziel dieser Arbeit ist die Schaffung eines Überblicks über die datenschutzrechtlichen Anforderungen für die Einrichtung und den Betrieb des Register- und Systemverbunds als Datendrehscheibe. Aufgrund der Tatsache, dass in der Informationsverpflichtungsdatenbank keine personenbezogenen Daten verarbeitet

---

[8] Vgl *Martini/Wenzel*, „Once only“ versus „only once”: Das Prinzip einmaliger Erfassung zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit, DVBl 2017, 749 ff.
[9] Vgl § 10a Bundesgesetz vom 24. Oktober 1967 betreffend den Familienlastenausgleich durch Beihilfen (Familienlastenausgleichsgesetz 1967), BGBl 1967/376 idF BGBl I 2020/28.
[10] *Parycek* in *Mayrhofer/Parycek*, Digitalisierung des Rechts 41.
[11] Bundesgesetz über die Einrichtung und den Betrieb eines Unternehmensserviceportals (Unternehmensserviceportalgesetz – USPG), BGBl I 2009/52 idF BGBl I 2021/142.

werden,[12] liegt der klare Schwerpunkt auf dem Register- und Systemverbund, auf dem der Datenaustausch basiert.

Für die Erarbeitung wird neben den entsprechenden Rechtsgrundlagen, österreichischen Kommentaren, Lehrbüchern und Fachzeitschriften auch relevante Literatur aus Deutschland herangezogen. Die einschlägigen Normen werden mit Hilfe der gängigen Interpretationsmethoden analysiert.

[12] § 2 Z 5 USPG idF BGBl I 2021/142.

# 1. Once-Only-Plattform

## *1.1. Das Once-Only-Prinzip*

Die Digitalisierung und digitale Transformation als deren Auswirkung in der Verwaltung wird von der Europäischen Union als unerlässlich für das Gelingen des digitalen Binnenmarkts angesehen.[13] Der vermehrte Einsatz von IT in der öffentlichen Verwaltung kann durch einen schnellen Austausch zwischen Behörden und Registerabfragen die Sachverhaltsermittlung erleichtern bzw verbessern.[14] Das Once-Only-Prinzip ist Teil des EU-E-Government-Aktionsplans 2016-2020 und beschreibt als elementarer Baustein einer modernen digitalen Verwaltung den Grundsatz des einmaligen Erfassens von Daten.[15]

Mit der Single Digital Gateway-Verordnung vom 2. Oktober 2018 wurde eine Verordnung über die Einrichtung eines einheitlichen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten beschlossen.[16] Bestimmte Verfahren für Bürger:innen und für die Wirtschaft sollen grenzüberschreitend online durchführbar sein.[17] Artikel 14 der SDG-VO bildet die Grundlage für die Schaffung eines technischen Systems für den automatisierten grenzüberschreitenden Austausch von Nachweisen und die Anwendung des Once-Only-Prinzips.[18] Das Once-Only-Prinzip, das auch als Möglichkeit umschrieben wird, aus wirtschaftlichen, „möglicherweise auch Bequemlichkeitsgründen, statt der Menschen die Daten laufen zu lassen“[19] wirft im Hinblick auf die Zweckbindung erhobener personenbezogener Daten durchaus rechtliche

---

[13] *Höchtl/Lampoltshammer*, E-Government in Österreich: Ein Überblick, in *Stember* et al (Hrsg), Handbuch E-Government (2019) 69.
[14] *Guckelberger*, Öffentliche Verwaltung im Zeitalter der Digitalisierung – Analysen und Strategien zur Verbesserung des E-Governments aus rechtlicher Sicht (Nomos 2019) 585.
[15] *Martini/Wenzel*, „Once only“ versus „only once”: Das Prinzip einmaliger Erfassung zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit, DVBl 2017, 749 ff.
[16] Verordnung (EU) 2018/1724 des europäischen Parlaments und des Rates vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr 1024/2012.
[17] Bis 12.12.2023 sind 17 Verfahren für Bürger:innen und in 4 Verfahren für die Wirtschaft grenzüberschreitend online zur Verfügung zu stellen.
[18] *Heine/Wessel*, E-Government und Datensouveränität – Einblicke und Lösungsansätze, HMD 2021 58, 1081 ff.
[19] *Guckelberger*, Öffentliche Verwaltung im Zeitalter der Digitalisierung 200.

Fragestellungen und Herausforderungen auf,[20] vor allem hinsichtlich der Bereitstellung des Zugriffs auf Daten nur für zuständige Behörden.[21]

Das Ziel des EU-weiten Vorhabens des Once-Only-Prinzips ist es, dass Bürger:innen und Unternehmen bestimmte Standardinformationen der Verwaltung nur noch einmal mitteilen müssen und diese dann innerhalb der Institutionen und über Ländergrenzen hinweg geteilt werden.[22] Die SDG-VO stellt mit Art 14 die Anforderung an die Mitgliedstaaten, ein technisches System für den grenzüberschreitenden automatisierten Austausch von Nachweisen und die Anwendung des Once-Only-Prinzips zu schaffen.[23] In Österreich soll zu diesem Zweck zunächst ein gesetzlicher Rahmen geschaffen werden.[24] Bisher ist das Once-Only-Prinzip im vierten Abschnitt des E-Government-Gesetzes[25] verankert, wobei hier die technischen Voraussetzungen noch nicht berücksichtigt sind.[26] §§ 16-18 E-GovG wurden mit der Absicht des Gesetzgebers und auch auf Wunsch der Verwaltung eingeführt, um die Vorlage bestimmter, immer wieder gebrauchter Dokumente wie Geburtsurkunden, Staatsbürgerschaftsnachweise oder Gewerbeberechtigungen überflüssig zu machen.[27] Während § 16 E-GovG normiert, dass elektronische Nachweise betreffend selbstständige wirtschaftliche Tätigkeiten und über das Vorliegen dafür notwendiger Berufsberechtigungen durch Inanspruchnahme des Dokumentationsregisters nach § 114 Abs 2 BAO[28] geführt werden können, bietet § 17 E-GovG die Grundlage für den elektronischen Nachweis des Personenstandes und der Staatszugehörigkeit.[29] § 17 Abs 2 E-GovG sieht vor, dass Behörden, wenn die Richtigkeit von personenbezogenen Daten zu beurteilen ist und diese Daten in einem elektronischen Register eines Verantwortlichen des öffentlichen Bereichs enthalten sind, sie – sofern die technischen Möglichkeiten bestehen – die Daten aus dem Register selbst abzurufen

[20] *Guckelberger*, Öffentliche Verwaltung im Zeitalter der Digitalisierung 200.
[21] *Schafferer/Horn/Schönbauer*, The Austrian Approach Concerning the European Data Retention Directive's Translation into National Law and its Technical Implementation, in Proceedings of the 12th European Conference on e-Government (ECEG 2012), 644.
[22] https://www.brz.gv.at/was-wir-tun/services-produkte/registersystemverbund.html. (abgefragt am 01.12.2022).
[23] Art 14 VO (EU) 2018/1724.
[24] Aus dem Ministerratsvortrag, BMDW 2020-0.644.727
[25] Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG), StF BGBl I 2004.
[26] Vgl auch *Höchtl/Lampoltshammer*, Rechtliche Rahmenbedingungen und technische Umsetzung von E-Government in Österreich in *Stember* et al, Handbuch E-Government (2019) 145.
[27] *Spornberger*, E-Government in *Zankl* (Hrsg), Rechtshandbuch der Digitalisierung (2021) 345.
[28] Bundesabgabenordnung, BGBl 1961/194 idF BGBl I 2018/32.
[29] *Spornberger*, E-Government 346.

haben. Voraussetzung dafür ist, dass die Betroffenen entweder dem Abruf aus dem Register zustimmen oder die Behörde aufgrund einer gesetzlichen Bestimmung zur Durchführung einer Abfrage berechtigt ist.[30] Die Datenermittlung durch die Behörde ersetzt in diesen Fällen den Nachweis durch die Partei oder Bürger:in.[31]

Mit der Novelle des Unternehmensserviceportalgesetzes vom 26. Juli 2021[32] wird die „Errichtung einer Once-Only-Plattform"[33] vorgesehen. Die Once-Only-Plattform soll aus einer Informationsverpflichtungsdatenbank und einem Register- und Systemverbund bestehen.[34] Als Ziele der Novelle werden die Reduktion von Doppel- und Mehrfachmeldungen sowohl mit Fokus auf Unternehmen als auch auf Behörden genannt, ebenso wie die Anbindung Österreichs an das Once-Only Technical System.[35] Durch die Vereinfachung und Verringerung von Datenmeldungen zwischen Unternehmen und Verwaltung soll die Entbürokratisierung und Modernisierung der Verwaltung vorangetrieben werden.[36] Zunächst liegt der Fokus auf unternehmensbezogenen Daten und in weiterer Folge sollen auch Daten von Bürger:innen nur noch einmal gemeldet werden müssen.[37] Die Daten sollen nicht zentral gespeichert werden, sondern bei den in den Materiengesetzen festgelegten Stellen und über eine einheitliche Schnittstelle – den Register- und Systemverbund – zwischen berechtigten Stellen ausgetauscht werden.[38] Die technische Basis für die Umsetzung des Once-Only-Prinzips stellt das Unternehmensserviceportal des Bundes dar. Dieses weist bereits eine hohe Schnittstellendichte zu anderen Systemen der Verwaltung und die technischen Voraussetzungen für die Vorbefüllung elektronischer Formulardatenfelder auf.[39] Mit der Einrichtung der Once-Only-Plattform im Sinne einer digitalen Infrastruktur und der Schaffung von Rahmenbedingungen zur Umsetzung von optimierten digitalen Services,

---

[30] *Höchtl/Lampoltshammer*, Rechtliche Rahmenbedingungen und technische Umsetzung von E-Government 145 f.
[31] § 17 Abs 2 E-GovG idF BGBl I 2018/32.
[32] Bundesgesetz, mit dem das Unternehmensserviceportalgesetz geändert wird, BGBl I 2021/142.
[33] § 6 USPG idF BGBl I 2021/142.
[34] § 1 Abs 3 USPG idF BGBl I 2021/142.
[35] Vorblatt und WFA zur Regierungsvorlage: 944 BlgNR XXVII. GP 1.
[36] Vgl Österreichische Bundesregierung, Regierungsprogramm 2020-2024, 64.
[37] Aus dem Ministerratsvortrag, BMDW 2020-0.644.727 vom 06.10.2020, https://www.ris.bka.gv.at/Dokumente/Mrp/MRP_20201007_33/011_000.pdf (abgefragt am 15.10.2022).
[38] Aus dem Ministerratsvortrag, BMDW 2020-0.644.727
[39] Erläuterungen zur Regierungsvorlage: ErlRV 944 BlgNR XXVII. GP 1.

soll eine zentrale E-Government-Infrastruktur etabliert werden, die von allen Ressorts bzw Ländern und Gemeinden nutzbar sein soll.[40]

## *1.2. Bestandteile der Once-Only-Plattform*

### *1.2.1. Einleitung*

Die Once-Only-Plattform besteht aus dem Register- und Systemverbund (RSV) und der Informationsverpflichtungsdatenbank (IVDB).[41] Der Register- und Systemverbund ermöglicht als zentrale Datenscheibe den Datenaustausch zwischen Verwaltungseinheiten direkt aus angebundenen Datenquellen. Die Informationsverpflichtungsdatenbank dient der Erfassung und Administration von Informationsverpflichtungen.[42]

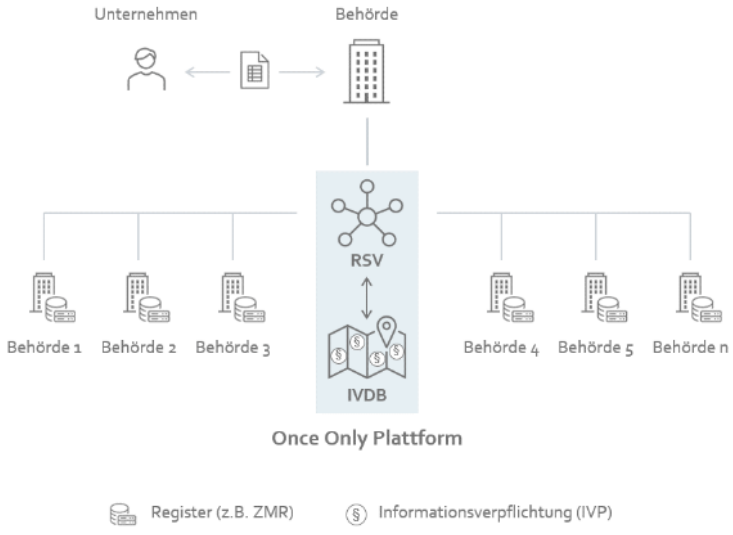


Abbildung 1: Kernkomponenten der Once-Only-Plattform[43]

### *1.2.2. Register- und Systemverbund*

Der sogenannte Register- und Systemverbund wurde bereits 2020 im Rahmen der Umsetzung des Once-Only-Prinzips initiiert.[44]

Beim Register- und Systemverbund handelt es sich um einen zentralen Datenbus für den behördenübergreifenden Informationsaustausch.[45] Dieser bildet als

[40] Aus dem Ministerratsvortrag, BMDW 2020-0.644.727
[41] § 1 Abs 3 USPG idF BGBl I 2021/142.
[42] https://www.usp.gv.at/ivdb-hilfe/Aufgaben-und-Zielsetzung.html (abgefragt am 15.10.2022).
[43] https://www.usp.gv.at/ivdb-hilfe/Aufgaben-und-Zielsetzung.html (abgefragt am 15.10.2022).
[44] https://www.brz.gv.at/was-wir-tun/services-produkte/registersystemverbund.html (abgefragt am 15.10.2022).

Datenübertragungsschicht den Kern der technischen Umsetzung und soll die Kommunikation zwischen einzelnen Datenbanken und Registern technisch ermöglichen.[46] Register sind Datensammlungen der öffentlichen Hand, in denen Daten über Bürger:innen oder Objekte erfasst sind und von verschiedenen Behörden zur Erfüllung öffentlicher Aufgaben genutzt werden.[47] Derzeit bilden Register die Grundlage für die Speicherung personenbezogener Daten und können von Behörden aller Verwaltungsebenen geführt werden. Standardisierte technische Schnittstellen für den Austausch von Daten zwischen beteiligten Behörden können zu einer digitalen Transformation der Verwaltung auch beitragen, insofern als dadurch Voraussetzungen für den Einsatz von automatisierter Rechtsanwendung geschaffen werden können.[48]

Als Kern der Once-Only-Plattform soll über den Register- und Systemverbund künftig der behördenübergreifende Austausch von Informationen, die aufgrund einer Informationsverpflichtung zu melden sind, jedoch bereits bei einer Behörde vorhanden sind, auf einfache und sichere Weise ermöglicht werden.[49] Autorisierte und gesetzlich beauftragte IT-Anwendungen können an einer zentralen Stelle Informationen aus angebundenen Registern anfragen und nach einem strikten „Need-to-Know-Prinzip" beziehen.[50] Als Datendrehscheibe werden über den Register- und Systemverbund lediglich Daten zur Verfügung gestellt, die für eine Verarbeitung unbedingt benötigt werden und für die eine rechtliche Zugriffsberechtigung existiert.[51] Im Register- und Systemverbund selbst werden dabei keine Daten aus den angebundenen Registern gespeichert, angefragte Informationen werden lediglich weitergeleitet.[52]

---

[45] ErlRV 944 BlgNR XXVII. GP 1.
[46] ErlRV 944 BlgNR XXVII. GP 1.
[47] *Von Lucke*, Hochleistungsportale für die öffentliche Verwaltung (2008) 254; *Peuker*, Registermodernisierung und Datenschutz, NVwZ 2021, 1168.
[48] *Mohabbat Kar/Thapa/Hunt/Parycek*, Recht Digital: Maschinenverständlich und automatisierbar – Impuls zur digitalen Vollzugstauglichkeit von Gesetzen, Kompetenzzentrum Öffentliche IT 2019, 14.
[49] Vorblatt und WFA zur Regierungsvorlage: 944 BlgNR XXVII. GP 1 f.
[50] https://www.brz.gv.at/was-wir-tun/services-produkte/registersystemverbund.html (abgefragt am 15.10.2022).
[51] https://www.brz.gv.at/was-wir-tun/services-produkte/registersystemverbund.html (abgefragt am 15.10.2022).
[52] https://www.brz.gv.at/was-wir-tun/services-produkte/registersystemverbund.html (abgefragt am 15.10.2022).

Am Datenaustausch über den RSV sind zwei Nutzergruppen beteiligt: der Data Consumer und der Data Provider.[53] Beim Data Consumer handelt es sich grundsätzlich um eine abfragende und beim Data Provider um eine registerführende Stelle. Nach Anlegen einer Registerabfrage durch den Data Consumer wird diese automatisch an den oder die betroffenen Data Provider übermittelt.[54] Durch die Data Provider können Anfragen freigegeben oder abgelehnt werden. Bei einer Freigabe eines Data Providers für sein Register wird der Datenaustausch für dieses ermöglicht, unabhängig davon, ob andere Data Provider die Anfrage möglicherweise abgelehnt haben.[55]

### *1.2.3. Informationsverpflichtungsdatenbank*

Die Informationsverpflichtungsdatenbank (IVDB) soll als weiterer Bestandteil der Once-Only-Plattform errichtet werden. Sie ist ebenso gesetzlich im USPG verankert und soll von der Bundesrechenzentrum GmbH betrieben und weiterentwickelt werden.[56] Die IVDB dient der Erfassung und Administration von Informationsverpflichtungen (IVP) und damit verbunden erforderlichen Meldungen.[57] Der Begriff der Informationsverpflichtung ist in § 2 Z 1 USPG definiert. Demzufolge handelt es sich hierbei um „eine aus einer Rechtsvorschrift resultierende Pflicht eines Unternehmens oder einer Bürgerin oder eines Bürgers, Informationen zusammenzustellen oder bereitzuhalten und diese – unaufgefordert oder auf Verlangen – einer Behörde oder anderen Institutionen zur Verfügung zu stellen oder zu übermitteln“.[58]

Die Informationsverpflichtungsdatenbank soll ein zentraler Teil des Berechtigungsmanagements für den Register- und Systemverbund sein und sicherstellen, dass Datenabfragen bzw -übermittlungen nur bei Bestehen entsprechender Berechtigungen der abfragenden Stellen erfolgen.[59] In der Informationsverpflichtungsdatenbank werden keine personenbezogenen Daten verarbeitet.[60] Als Metadatenbank konzipiert, enthält diese lediglich allgemeine, abstrakte

[53] https://www.usp.gv.at/rsv-hilfe/Rollen.html (abgefragt am 15.10.2022).
[54] https://www.usp.gv.at/rsv-hilfe.html (abgefragt am 15.10.2022).
[55] https://www.usp.gv.at/rsv-hilfe/Arbeitsobjekte.html (abgefragt am 15.10.2022).
[56] ErlRV 944 BlgNR XXVII. GP 2.
[57] https://www.usp.gv.at/ivdb-hilfe/Aufgaben-und-Zielsetzung.html (abgefragt am 15.10.2022).
[58] § 2 Z 1 UPSG idF BGBl I 2021/142.
[59] ErlRV 944 BlgNR XXVII. GP 2.
[60] § 2 Z 5 USPG idF BGBl I 2021/142.

Angaben über Informationsverpflichtungen, aber nicht die Inhalte selbst.[61] Die Informationsverpflichtungsdatenbank soll der Optimierung bestehender Informationsverpflichtungen dienen, aber auch im Fall der Schaffung neuer Informationsverpflichtungen herangezogen werden.[62]

Durch die Erhebung von Informationsverpflichtungen und eine kontinuierliche Aktualisierung dieser soll mit der IVDB eine Grundlage für einen effizienten behördenübergreifenden Datenaustausch geschaffen werden.[63] Derzeit kommt es aufgrund einer Vielzahl bestehender Informationsverpflichtungen von Unternehmen zu Doppel- bzw Mehrfachmeldungen. Das kann darauf zurückzuführen sein, dass Nachweise von behördeninternen Informationen vorgelegt werden müssen oder gleiche Informationen bei verschiedenen Meldeverpflichtungen abgefragt werden. Mit der IVDB kann das Ziel der Entlastung von Unternehmen erreicht werden, indem zunächst eine Übersicht über bestehende IVP geschaffen und diese in weiterer Folge reduziert werden. Durch eine Schnittstelle, wie sie mit dem RSV angedacht ist, können Behörden Daten von anderen Behörden beziehen. Wichtig hierfür wäre zu identifizieren, welche Stelle für ein Datenfeld die führende Datenquelle ist.[64] Die Erfassung von Informationsverpflichtungen in der IVDB führt nicht automatisch zu einer Entlastung von Unternehmen. Dies kann erst durch eine Reduktion von Meldeverpflichtungen erfolgen, was durch die einzelnen Ressorts durchzuführen ist. Durch ein Aufzeigen des generierten Aufwands, der Übersicht ähnlicher Informationsverpflichtungen, der Darstellung des Mehrwerts bei Reduktion oder dem Sichtbarmachen von fehlenden führenden Registern kann jedenfalls ein größeres Problembewusstsein geschaffen werden.

§ 7 USPG sieht vor, dass bei der beabsichtigten Schaffung von neuen Informationsverpflichtungen zunächst bei der IVDB abzufragen ist, ob eine diesbezügliche IVP bereits begründet wird. Ist dies nicht der Fall, sollte geprüft werden, ob eine Abstimmung auf eine bereits bestehende ähnliche Informationsverpflichtung möglich ist.[65] Durch die Abfragemöglichkeit bestehender IVP soll erreicht werden, dass

---

[61] ErlRV 944 BlgNR XXVII. GP 2.
[62] ErlRV 944 BlgNR XXVII. GP 2.
[63] Vorblatt und WFA zur Regierungsvorlage: 944 BlgNR XXVII. GP 8.
[64] Siehe dazu auch Vorblatt und WFA zur Regierungsvorlage: 944 BlgNR XXVII. GP 8.
[65] § 7 USPG idF BGBl I 2021/142.

bei legistischen Maßnahmen nicht neuerlich gleiche oder ähnliche IVP normiert werden bzw erneut von Rechtsunterworfenen abgefragt werden müssen.[66]

[66] ErlRV 944 BlgNR XXVII. GP 3.

# 2. Datenschutzrechtliche Grundlagen für die Datenverarbeitung

## *2.1. Einleitung*

Die Datenverarbeitung im Sinne eines Datenaustauschs zwischen Behörden soll über den Register- und Systemverbund als Datendrehscheibe stattfinden. Grundsätzlich lässt sich die behördliche Datenverarbeitung in das System des allgemeinen Verwaltungsrechts als eigene Handlungsform, und zwar als besondere Ausprägung des schlichten Verwaltungshandelns einordnen.[67] Da bei diesen Datenverarbeitungsvorgängen auch personenbezogene Daten verarbeitet werden, sind datenschutzrechtliche Vorschriften zu beachten. Der Grundgedanke des Once-Only-Prinzips, dass die Verwaltung alle ihr vorliegenden Daten nutzen soll, bevor sie diese von den Bürger:innen erneut abfragt, steht in einem Spannungsverhältnis zum Grundsatz der Zweckbindung nach der DSGVO.[68] Über die Informationsverpflichtungsdatenbank erfolgt kein Datenverarbeitungsvorgang, weshalb hier keine datenschutzrechtlichen Vorschriften einschlägig sind.[69]

## *2.2. Anwendbarkeit des Datenschutzrechts*

Die DSGVO bezieht öffentliche ebenso wie private Datenverarbeitung mit ein.[70] Die Regelungen des Anwendungsbereichs der DSGVO weisen Besonderheiten für die öffentliche Verwaltung auf, wonach die DSGVO keine Anwendung auf Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, findet.[71] Das bezieht sich vor allem auf den öffentlichen Bereich, da für die gemeinsame Außen- und Sicherheitspolitik und in Hinblick auf die nationale Sicherheitspolitik keine Kompetenzen der Union bestehen.[72]

---

[67] *Reimer*, Verwaltungsdatenschutzrecht – Das neue Recht für die behördliche Praxis (2019) 17 mit Verweis auf *Pitschas* in *Hoffmann-Riem/Schmidt-Aßmann/Schupert* (Hrsg), Reform des Allgemeinen Verwaltungsrechts (1993) 301.
[68] *Martini/Wenzel*, „Once only" versus „only once": Das Prinzip einmaliger Erfassung zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit, DVBl 2017, 749.
[69] Vorblatt und WFA zur Regierungsvorlage: 944 BlgNR XXVII. GP 3.
[70] *Lachmayer*, Die DSGVO im öffentlichen Bereich – Europarechtliche Vorgaben im öffentlichen Bereich, ÖJZ 2018/03, 113.
[71] Art 2 Abs 2 lit a DSGVO.
[72] ErwGr 16 DSGVO.

Während vom persönlichen Schutzbereich der DSGVO nur natürliche Personen erfasst sind, kommen die in § 1 DSG[73] normierten Rechte neben natürlichen Personen auch juristischen Personen zu.[74] Das in § 1 DSG verankerte Grundrecht auf Datenschutz besteht aus dem Recht auf Geheimhaltung personenbezogener Daten (§ 1 Abs 1 DSG), dem Recht auf Auskunft (§ 1 Abs 3 Z 1 DSG), dem Recht auf Richtigstellung unrichtiger Daten (§ 1 Abs 3 Z 2 DSG) sowie dem Recht auf Löschung unzulässiger Weise verarbeiteter Daten (§ 1 Abs 3 Z 2 DSG).

In den territorialen Anwendungsbereich nach Artikel 3 der DSGVO fallen folgende Szenarien: Die personenbezogenen Daten werden im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Europäischen Union verarbeitet, die personenbezogenen Daten beziehen sich auf betroffene Personen, die sich in der Union befinden, oder die personenbezogenen Daten werden an einem Ort außerhalb der Union verarbeitet, an dem jedoch das Recht eines Mitgliedstaats nach dem Völkerrecht gilt. Das zweite Szenario, bei dem sich die personenbezogenen Daten auf betroffene Personen in der Union beziehen, unterliegt zusätzlichen Bedingungen für die Anwendung der DSGVO. So gibt es zwei alternative Bedingungen, die zur Anwendung der DSGVO führen. Die erste ist, dass die Datenverarbeitung mit dem Angebot von Waren oder Dienstleistungen an betroffene Personen in der Union zusammenhängt, unabhängig davon, ob dies kostenlos oder gegen eine Gebühr erfolgt (Art 3 Abs 2 lit a). Die zweite Alternative besteht darin, dass die Datenverarbeitung mit der Überwachung des Verhaltens der betroffenen Personen zusammenhängt, sofern deren Verhalten innerhalb der Union stattfindet (Art 3 Abs 2 lit b). Der auf dem RSV basierende Datenaustausch von personenbezogenen Daten ist jedenfalls vom territorialen Anwendungsbereich erfasst. Zum einen soll die Verarbeitung sowohl in der Europäischen Union stattfinden und zum anderen sollen Daten von Personen in der Europäischen Union verarbeitet werden.

Der sachliche Anwendungsbereich der DSGVO ist in Artikel 2 so definiert, dass er die Verarbeitung personenbezogener Daten in drei Formen umfasst: die vollautomatisierte

---

[73] Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl I 1999/165 idF BGBl I 2021/148.
[74] *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG) (2022) § 1 Rz 1.

Verarbeitung, die teilautomatisierte Verarbeitung und die nichtautomatisierte Verarbeitung. Die nichtautomatisierte Verarbeitung ist nur dann als Verarbeitung im Sinne der DSGVO einzustufen, wenn die verarbeiteten personenbezogenen Daten entweder in einem Dateisystem gespeichert sind oder in ein Dateisystem integriert werden sollen.[75] Die Verarbeitung über den RSV ist jedenfalls auch vom sachlichen Anwendungsbereich erfasst, da die Verarbeitung automatisiert erfolgen soll und das übergeordnete Ziel der Once-Only-Plattform entsprechend der SDG-VO die Schaffung eines Systems für den grenzüberschreitenden automatisierten Austausch von Nachweisen ist. [76]

Personenbezogene Daten enthalten nach Art 4 Z 1 DSGVO Informationen, die eine natürliche Person identifizieren oder identifizierbar machen. Eine natürliche Person gilt als eindeutig identifiziert, wenn die Identität der Person unmittelbar aus der Information selbst hervorgeht, etwa bei direkter Namensnennung. Identifizierbar ist eine Person, wenn die Information an sich nicht ausreichend ist, um sie einer Person zuzuordnen, eine Zuordnung jedoch bei Verknüpfung mit weiteren Informationen möglich wird.[77] Die Natur dieser Informationen ist irrelevant. Entscheidend ist, dass sie mit einer Person in Verbindung gebracht werden können.[78] Darunter fallen Daten wie Name, Geburtsdatum, Adresse, Einkommen, Geschlecht, Größe oder Gewicht, aber auch Werturteile, Schätzdaten und statistische Wahrscheinlichkeitsaussagen, sowie biometrische Daten wie Fingerabdrücke oder Gesichtszüge.[79] Besondere Kategorien personenbezogener Daten werden in Art 9 Abs 1 DSGVO definiert. Zu dieser Kategorie der sensiblen Daten[80] zählen beispielsweise Informationen über die rassische und ethische Herkunft, politische Meinungen, religiöse Überzeugungen, Gesundheitsdaten und biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person. Art 9 Abs 1 DSGVO stellt darauf ab, dass aus der Verarbeitung personenbezogener Daten diese Informationen

---

[75] Art 2 Abs 1 DSGVO.
[76] ErlRV 944 BlgNR XXVII. GP 1.
[77] *Jahnel/Pallwein-Prettner*, Datenschutzrecht[3] (2021) 51.
[78] *Hödl* in *Knyrim*, DatKomm Art 4 DSGVO (Stand 1.12.2018, rdb.at) Rz 12.
[79] *Haidinger*, Grundbegriffe und Definitionen in *Knyrim* (Hrsg), Praxishandbuch Datenschutzrecht[4] (2020) 26.
[80] So die Bezeichnung nach dem DSG 2000 (Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), StF BGBl I 1999/165).

„hervorgehen“.[81] Grundsätzlich werden über den RSV personenbezogene Daten verarbeitet, wobei die Verarbeitung von besonderen Kategorien personenbezogener Daten nicht ausgeschlossen werden kann, denkbar ist beispielsweise die Verarbeitung von Gesundheitsdaten.

## *2.3. Zum Begriff der Verarbeitung*

Jede Verarbeitung von personenbezogenen Daten muss sich auf eine rechtliche Grundlage stützen können (Verbot mit Erlaubnisvorbehalt) und eine der Rechtsgrundlagen in Art 6 DSGVO erfüllen, um rechtmäßig zu sein.[82] Der Begriff der Verarbeitung ist äußerst weit gefasst, was dazu führt, dass beinahe jeglicher Umgang mit personenbezogenen Daten als Verarbeitung zu qualifizieren ist.[83] Gemäß der demonstrativen Aufzählung in Art 4 Z 2 DSGVO sind vom Begriff der Verarbeitung jedenfalls Vorgänge mit personenbezogenen Daten wie das Abfragen, die Übermittlung, Verbreitung oder andere Formen der Bereitstellung umfasst.

Während das Abfragen die Zurückgewinnung von Informationen aus gespeicherten Daten mit Hilfe von Suchroutinen meint,[84] beschreibt die Offenlegung durch Übermittlung, Verbreitung oder andere Formen der Bereitstellung alle Vorgänge, „durch die der Verantwortliche personenbezogene Daten anderen Stellen in einer Weise zugänglich macht, die es diesen erlauben, vom Informationsgehalt Kenntnis zu haben.“[85] Die Offenlegung meint den Vorgang, Dritten Kenntnis oder die Möglichkeit der Kenntnisnahme zu verschaffen.[86] Eine Unterform der Offenlegung ist die Übermittlung iSd DSGVO, die die Mitteilung an individuell bestimmte Adressaten bezeichnet.[87] Eine Übermittlung liegt erst vor, wenn die Daten auch tatsächlich abgerufen werden, die bloße Bereithaltung zur Abrufung stellt noch keine Übermittlung dar.[88] Das Abfragen bzw Übermitteln der Daten über den RSV ist somit vom Begriff der Verarbeitung erfasst.

---

[81] *Haidinger* in Praxishandbuch Datenschutzrecht 29 f.
[82] *Jahnel/Pallwein-Prettner*, Datenschutzrecht 69.
[83] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 4 Z 2 DSGVO (Stand 1.12.2020, rdb.at) Rz 18.
[84] *Hödl* in *Knyrim*, DatKomm Art 4 DSGVO (Stand 1.12.2018, rdb.at) Rz 33.
[85] *Hödl* in *Knyrim*, DatKomm Art 4 DSGVO (Stand 1.12.2018, rdb.at) Rz 35.
[86] *Hödl* in *Knyrim*, DatKomm Art 4 DSGVO (Stand 1.12.2018, rdb.at) Rz 35.
[87] *Hödl* in *Knyrim*, DatKomm Art 4 DSGVO (Stand 1.12.2018, rdb.at) Rz 36.
[88] *Hödl* in *Knyrim*, DatKomm Art 4 DSGVO (Stand 1.12.2018, rdb.at) Rz 36.

## *2.4. Zum Begriff der Behörden*

In der DSGVO wird sowohl der Begriff „Behörde“ (public autority) als auch der Begriff „öffentliche Stelle“ (public authority) verwendet,[89] was darauf schließen lässt, dass die Unionsgesetzgebung grundsätzlich von einer Unterscheidung ausgeht. Jedoch werden die beiden Begriffe nicht näher bestimmt.[90] Die Art-29-Datenschutzgruppe verweist darauf, dass die Begriffe nationalstaatlich auszulegen seien, wobei sich in der DSGVO selbst dafür kein Anhaltspunkt findet.[91] Die weitgehende Nebeneinanderstellung der Begriffe lässt vermuten, dass der gesamte staatliche Bereich erfasst werden soll. Geht es um die Ausübung hoheitlicher Befugnisse, wird die Bezeichnung „Behörde“ allein verwendet.[92] Während der Begriff der „öffentlichen Stelle“ in europäischen Richtlinien definiert wird,[93] ist für den Begriff der Behörde eine Anknüpfung an das österreichische Recht denkbar. Demnach werden unter dem Begriff „Behörde“ jene Organe verstanden, denen hoheitliche Aufgaben übertragen sind.[94] Das österreichische Datenschutzgesetz verwendet in § 1 den Terminus „staatliche Behörden“. Behörden im Sinne des § 1 Abs 2 DSG sind im funktionellen Sinn zu verstehen,[95] und ebenso umfasst sind Selbstverwaltungskörper und alle Stellen der Hoheitsverwaltung, die dem Legalitätsprinzip des B-VG[96] unterliegen.[97]

---

[89] Beispielsweise in Art 37 Abs 3 DSGVO, wonach für mehrere Behörden oder öffentliche Stellen ein gemeinsamer Datenschutzbeauftragter beauftragt werden kann.
[90] *Reimer*, Verwaltungsdatenschutzrecht 54.
[91] *Bergauer* in *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 37 DSGVO (Stand 1.12.2020, rdb.at) Rz 7 mit Verweis auf WP 243 rev.01, 6.
[92] *Reimer*, Verwaltungsdatenschutzrecht 54.
[93] Der Begriff der „öffentlichen Stelle“ wird beispielsweise in der Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates vom 26. Oktober 2016 über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen bestimmt. Nach Art 3 Z 1 leg cit bezeichnet der Ausdruck der öffentlichen Stelle „den Staat, Gebietskörperschaften, Einrichtungen des öffentlichen Rechts im Sinne der Definition in Artikel 2 Abs 1 Nummer 4 der Richtlinie 2014/24/EU oder Verbände, die aus einer oder mehreren solcher Körperschaften oder Einrichtungen des öffentlichen Rechts bestehen, sofern diese Verbände zu dem besonderen Zweck gegründet wurden, im Allgemeininteresse liegende Aufgaben nicht gewerblicher Art zu erfüllen.“ Auch in der Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors wird in Art 2 Z 1 der Begriff der „öffentlichen Stelle“ bestimmt.
[94] *Raschauer*, Allgemeines Verwaltungsrecht[6] (2021) 62.
[95] *Thiele/Wagner*, Praxiskommentar zum DSG § 1 Rz 49, Vgl dazu auch *Raschauer*, Allgemeines Verwaltungsrecht mit Verweis auf VwGH 30.1.2014, 2012/10/0227, wonach es ausschließlich Behörden im funktionellen Sinn gibt.
[96] Art 18 des Bundes-Verfassungsgesetzes vom 1. Oktober 1920 (B-VG), BGBl 1920/1 idF BGBl 2022/141.
[97] Vgl *Thiele/Wagner*, Praxiskommentar zum DSG § 1 Rz 49; DSB 9.9.2016, DSB-D123.438/0002/2016; DSB 23.11.2018, DSB-D122.956/0007-DSG/2018 (Intelligente Wasserzähler).

In den Erläuterungen zum USPG wird festgehalten, dass das USPG hinsichtlich der Informationsverpflichtungen jedenfalls von einem organisatorischen Behördenbegriff ausgeht, womit Informationen im Rahmen der Privatwirtschaftsverwaltung, etwa im Bereich des Förderwesens, als mitumfasst gelten.[98]

Im Zuge des Datenaustauschs über den RSV treten Behörden einerseits als abfragende Behörden (Data Consumer) und andererseits als auskunftserteilende (Register-)Behörden (Data Provider) auf.

## *2.5. Grundsätze der DSGVO*

### *2.5.1. Rechtmäßigkeit, Treu und Glauben, Transparenz (Art 5 Abs 1 lit a DSGVO)*

Jede Verarbeitung personenbezogener Daten muss auf einer Rechtsgrundlage beruhen. Ohne Rechtsgrundlage, die die Verarbeitung zulässt, ist jede Verarbeitung personenbezogener Daten verboten (Verbotsprinzip).[99] Für die Rechtmäßigkeit der Datenverarbeitung muss daher ein sogenannter Erlaubnistatbestand vorliegen. Die Erlaubnistatbestände sind in Art 6 Abs 1 lit a bis f DSGVO normiert und bestehen nebeneinander, wobei mindestens eine der Bedingungen erfüllt sein muss. Die Datenverarbeitung kann rechtmäßig sein aufgrund einer erteilten Einwilligung (lit a), zur Erfüllung eines Vertrags (lit b), zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt (lit c) oder um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen (lit d). Des Weiteren kann die Verarbeitung für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, erforderlich sein (lit e) bzw aufgrund eines berechtigten Interesses des Verantwortlichen oder eines Dritten (lit f). Die Erlaubnistatbestände sind grundsätzlich abschließend normiert, wobei mit Art 6 Abs 1 lit f eine Art „Auffangklausel" besteht, die eine Interessenabwägung und damit eine Einzelfallbewertung ermöglicht.[100] Die für die Tätigkeit des RSV in Frage kommenden Erlaubnistatbestände werden in Kapitel 3 erörtert.

---

[98] ErlRV 944 BlgNR XXVII. GP 2.
[99] *Jahnel/Pallwein-Prettner,* Datenschutzrecht 31.
[100] *Jahnel/Pallwein-Prettner,* Datenschutzrecht 32.

Der Grundsatz der Verarbeitung nach Treu und Glauben gilt als eine Art Auffangklausel, um gegebenenfalls Verarbeitungen als rechtswidrig qualifizieren zu können, wenn ihnen keine datenschutzrechtliche Bestimmung eindeutig entgegensteht.[101]

Gemäß dem Grundsatz der Transparenz muss für die Betroffenen zunächst erkennbar sein, dass personenbezogene Daten verarbeitet werden und darüber hinaus, zu welchen Zwecken und durch wen diese verarbeitet werden.[102] Betroffene müssen über Risiken, Vorschriften, Garantien und Rechte in Zusammenhang mit der Verarbeitung informiert werden, wobei die Informationen präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst sein müssen.[103] Inwieweit vom RSV der Grundsatz der Transparenz und die Betroffenenrechte zu berücksichtigen sind, wird in Kapitel 4 näher erläutert.

### *2.5.2. Zweckbindung (Art 5 Abs 1 lit b DSGVO)*

Der Grundsatz der Zweckbindung gilt als zentraler Grundsatz der europäischen Datenschutztradition und besteht aus zwei Elementen. Einerseits dürfen personenbezogene Daten nur erhoben werden, wenn spätestens zum Zeitpunkt der Erhebung ein eindeutiger und legitimer Zweck festgelegt wurde.[104] Andererseits dürfen die erhobenen Daten nur zu Zwecken weiterverarbeitet werden, die mit den ursprünglich festgelegten Zwecken vereinbar sind.[105] Dieser Grundsatz ist für den RSV besonders bedeutend, da dieser selbst keine Daten von Personen erhebt und fraglich ist, ob die Tätigkeit des RSV eine Weiterverarbeitung darstellt oder eine Verarbeitungstätigkeit iSd Art 4 Z 2. Handelt es sich um eine Weiterverarbeitung, muss diese jedenfalls mit den ursprünglichen Zwecken vereinbar sein. Die Frage, ob die Tätigkeit des RSV als eine Weiterverarbeitung iSd Art 6 Abs 4 DSGVO darstellen kann, wird im Rahmen von Kapitel 3 behandelt.

### *2.5.3. Datenminimierung (Art 5 Abs 1 lit c DSGVO)*

Nach dem Grundsatz der Datenminimierung sollen Art und Umfang der verarbeiteten Daten den Verarbeitungszwecken angemessen sein und auf das für die Zwecke

---

[101] *Hötzendorfer/Tschohl/Kastelitz* in *Knyrim*, DatKomm Art 5 DSGVO (Stand 7.5.2020, rdb.at) Rz 17.
[102] *Hötzendorfer/Tschohl/Kastelitz* in *Knyrim*, DatKomm Art 5 DSGVO (Stand 7.5.2020, rdb.at) Rz 18.
[103] *Hötzendorfer/Tschohl/Kastelitz* in *Knyrim*, DatKomm Art 5 DSGVO (Stand 7.5.2020, rdb.at) Rz 18.
[104] *Hötzendorfer/Tschohl/Kastelitz* in *Knyrim*, DatKomm Art 5 DSGVO (Stand 7.5.2020, rdb.at) Rz 22.
[105] *Feiler/Forgó*, EU-DSGVO Kurzkommentar (2017) 9.

notwendige Maß beschränkt sein.[106] Daten dürfen über den RSV nur nach einem Need-to-Know-Prinzip ausgetauscht werden.[107] Demnach dürfen die Behörden nicht beliebig Daten austauschen, sondern nur nach expliziter Abfrage und auch nur bei entsprechender Berechtigung der abfragenden Stelle.

### *2.5.4. Richtigkeit (Art 5 Abs 1 lit d DSGVO)*

Der Grundsatz der Richtigkeit sieht vor, dass personenbezogene Daten richtig und auf dem neuesten Stand sein müssen.[108] Der RSV als Datendrehscheibe erhebt selbst keine Daten und prüft bzw ändert diese inhaltlich nicht. Dieser Grundsatz ist für den RSV daher nicht bedeutend.

### *2.5.5. Speicherbegrenzung (Art 5 Abs 1 lit e DSGVO)*

Der Grundsatz der Speicherbegrenzung besagt, dass personenbezogene Daten nur so lange gespeichert werden dürfen, wie dies für die festgelegten Verarbeitungszwecke erforderlich ist.[109] Datenverarbeiter haben organisatorische Maßnahmen zu treffen, um regelmäßig feststellen zu können, ob gespeicherte personenbezogene Daten noch benötigt werden oder nicht. Beim RSV werden schon von vornherein keine personenbezogenen Daten gespeichert. Log-Daten, die aufgrund des Datenaustausches gespeichert werden, enthalten keine personenbezogenen Informationen. Der Grundsatz der Speicherbegrenzung ist daher für die Datenverarbeitung durch den RSV unproblematisch.

### *2.5.6. Integrität und Vertraulichkeit (Art 5 Abs 1 lit f DSGVO)*

Der Grundsatz der Integrität und Vertraulichkeit steht in engem Zusammenhang zu den Bestimmungen über die Datensicherheit bei der Verarbeitung nach Art 32 DSGVO. Demnach sollen personenbezogene Daten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist. Die Datensicherheit für die Verarbeitung und die Auswahl der dafür zu treffenden technischen und organisatorischen Maßnahmen wird in Kapitel 5 erörtert.

---

[106] *Feiler/Forgó*, EU-DSGVO 9.
[107] https://www.brz.gv.at/was-wir-tun/services-produkte/registersystemverbund.html (abgefragt am 15.10.2022).
[108] *Jahnel/Pallwein-Prettner*, Datenschutzrecht 36.
[109] *Feiler/Forgó*, EU-DSGVO 9.

### *2.5.7. Rechenschaftspflicht (Art 5 Abs 2 DSGVO)*

Die Rechenschaftspflicht ergänzt die Grundsätze der Datenverarbeitung und besagt, dass der Verantwortliche die Einhaltung der Grundsätze nachweisen können muss.[110] Der Verantwortliche muss die Einhaltung sowohl gegenüber betroffenen Personen als auch gegenüber der Aufsichtsbehörde nachweisen können.[111]

## *2.6. Verantwortlicher und Auftragsverarbeiter*

Die Rolle des Verantwortlichen ist vor allem von großer Bedeutung, da dieser für die Einhaltung der Datenschutzbestimmungen verantwortlich ist und sich betroffene Personen bei der Geltendmachung ihrer Rechte an ihn wenden können.[112] Nach Art 4 Z 7 DSGVO ist Verantwortlicher jene „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Der Verantwortliche gilt als Adressat der Pflichten aus der DSGVO und Ansprechstelle für Maßnahmen der Aufsichtsbehörde.[113] Der Verantwortliche hat die Kontrolle über die Verarbeitung von personenbezogenen Daten inne und verfügt über die Entscheidungshoheit, zu welchem Zweck und mit welchen Mitteln die Datenverarbeitung erfolgen soll.[114] Er ist der primäre Adressat der Verpflichtungen aus der DSGVO bzw dem DSG und hat umfassende Informations- und Handlungspflichten gegenüber den betroffenen Personen, hat für ausreichende Datensicherheit zu sorgen und gegebenenfalls eine Datenschutz-Folgenabschätzung durchzuführen.[115] Die beteiligten Stellen sind für die Verarbeitungsvorgänge entweder gemeinsam oder separat datenschutzrechtlich verantwortlich. Die Rolle des Verantwortlichen kann gesetzlich geregelt sein oder sich aus den Umständen des konkreten Falls ergeben. In Erwägungsgrund 45 der DSGVO findet sich die ausdrückliche Anleitung an den Gesetzgeber, den Verantwortlichen im öffentlichen Bereich gesetzlich festzulegen. Aus dem Vorblatt zum USPG geht hervor, dass die datenschutzrechtliche Verantwortlichkeit „einerseits bei den für die Register

---

[110] Art 5 Abs 2 DSGVO.
[111] *Jahnel/Pallwein-Prettner*, Datenschutzrecht 37.
[112] *Jahnel/Pallwein-Prettner*, Datenschutzrecht 61.
[113] *Hödl* in *Knyrim*, DatKomm Art 4 DSGVO (Stand 1.12.2018, rdb.at) Rz 77.
[114] *Jahnel/Pallwein-Prettner*, Datenschutzrecht 37.
[115] *Jahnel/Pallwein-Prettner*, Datenschutzrecht 37.

zuständigen Stellen und andererseits bei den für die Abfrage zuständigen Stellen“ liegt.[116] Dies führt dazu, dass für die Datenverarbeitung durch den RSV mehrere Stellen datenschutzrechtlich verantwortlich sind.

Auftragsverarbeiter ist gemäß Art 4 Z 8 DSGVO jene „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“. Auftragsverarbeiter haben die Weisungen vom Auftraggeber hinsichtlich des Zwecks der Verarbeitung und der wesentlichen Elemente der Mittel zu befolgen.[117] Die Rechtmäßigkeit der Datenverarbeitungstätigkeit des Auftragsverarbeiters wird durch den erteilten Auftrag bestimmt.[118] In § 6 Abs 3 USPG ist normiert, dass die Bundesrechenzentrum GmbH als Betreiberin der Once-Only-Plattform gesetzliche Auftragsverarbeiterin im Sinne des Art 4 Z 8 DSGVO ist und daher verpflichtet ist, die Datenschutzpflichten gemäß Art 28 Abs 3 lit a bis h DSGVO wahrzunehmen.

[116] Vorblatt und WFA zur Regierungsvorlage: 944 BlgNR XXVII. GP 3.
[117] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 4 Z 8 DSGVO (Stand 1.12.2020, rdb.at) Rz 5.
[118] *Jahnel/Pallwein-Prettner*, Datenschutzrecht 37.

# 3. Rechtmäßigkeit der Datenverarbeitung

## *3.1. Zulässigkeit nach der DSGVO*

Die Verarbeitung von Personendaten durch den Staat darf nur auf Basis einer gesetzlichen Grundlage erfolgen.[119] Entsprechend der DSGVO ist die Verarbeitung personenbezogener Daten präventiv verboten, soweit nicht ein Erlaubnistatbestand einschlägig ist (Art 6 Abs 1 DSGVO). Als Ausnahmen stehen sechs Erlaubnistatbestände bereit, wovon zumindest einer verwirklicht sein muss, damit das Verbot nicht greift.[120]

Der Erlaubnistatbestand des berechtigten Interesses gemäß Art 6 Abs 1 lit f DSGVO, der insbesondere für die Privatwirtschaft eine bedeutende Rolle spielt, wird für die von Behörden vorgenommene Verarbeitung von vornherein ausgeschlossen (Art 6 Abs 1 lit f UAbs 2 DSGVO). In Erwägungsgrund 47 der DSGVO wird ausgeführt, dass es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Behörden zu schaffen und diese Rechtsgrundlage daher nicht für Verarbeitungen durch Behörden in Erfüllung ihrer Aufgaben gelten soll. Auch die Datenschutzbehörde hat bereits klar ausgesprochen, dass Art 6 Abs 1 lit f DSGVO nicht auf Behörden in Erfüllung ihrer Aufgaben anwendbar ist.[121]

### *3.1.1. Einwilligung*

*Reimer* erachtet die verwaltungsbehördliche Datenverarbeitung grundsätzlich als unproblematisch, wenn eine Einwilligung der betroffenen Person vorliegt.[122] Bereits aus Art 8 Abs 2 GRC ergibt sich, dass die Einwilligung die Verarbeitung personenbezogener Daten rechtfertigen kann.[123] Die Einwilligung ist in Art 4 Z 11 DSGVO definiert und beschreibt „jede freiwillig für einen bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten

---

[119] *Braun Binder*, Künstliche Intelligenz und automatisierte Entscheidungen in der öffentlichen Verwaltung, SJZ/RSJ 15/2019, 475.
[120] *Reimer*, Verwaltungsdatenschutzrecht 73.
[121] DSB 12.04.2019, DSB-D123.591/0003-DSB/2019 (BVT-Affäre Tweets).
[122] *Reimer*, Verwaltungsdatenschutzrecht 88.
[123] *Veil*, Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis, NJW 2018, 3337.

einverstanden ist.“ Für die Wirksamkeit einer Einwilligung müssen gemäß Art 7 DSGVO einige Bedingungen erfüllt sein. Für eine DSGVO-konforme Einwilligung leitet die DSB folgende Kriterien ab: Freiwilligkeit, Bestimmtheit, Information, Verständlichkeit, leichte Zugänglichkeit, klare und einfache Sprache.[124]

Die Beweislast für die Erteilung der Einwilligung und ihren Umfang trägt gemäß Art 7 Abs 1 DSGVO der Verantwortliche.[125] Aus Art 7 Abs 1 DSGVO geht jedoch auch hervor, dass der Verantwortliche die Einwilligung für jede einzelne erfolgte Einwilligung der jeweils betroffenen Person nachweisen können muss und die Nachweisbarkeit eines abstrakten Einwilligungsprozesses nicht ausreichend ist.[126] Darüber hinaus haben Betroffene nach Art 7 Abs 3 Satz 1 DSGVO ein Widerrufsrecht, welches wie die Einwilligung selbst eine Verwirklichung des Selbstbestimmungsrechts darstellt[127] und dazu führt, dass die Datenverarbeitung unverzüglich zu beenden ist. Aus dem Erwägungsgrund 43 geht hervor, dass die Einwilligung bei Bestehen eines klaren Ungleichgewichts, „insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt und es in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig erteilt wurde, keine gültige Rechtsgrundlage liefern“ sollte. Die Datenschutzbehörde schließt die Möglichkeit der Einwilligung gegenüber Behörden nicht von vornherein aus.[128] Nach *Buchner/Petri* soll eine Einwilligung übereinstimmend mit dem Erwägungsgrund mangels Freiwilligkeit nicht möglich sein, wenn die Behörde die Datenverarbeitung auch zwangsweise durchsetzen kann.[129] Für den Fall, dass die Freiwilligkeit unzweifelhaft gegeben ist, wäre nach *Kastelitz et al* eine Verarbeitung auf Basis einer Zustimmung denkbar.[130] Für die Verarbeitung durch den RSV würde dies bedeuten, dass für jede erteilte Einwilligung die Freiwilligkeit unzweifelhaft nachzuweisen wäre. Darüber hinaus müsste für Betroffene jedenfalls auch die Möglichkeit des Erteilens eines Widerrufs möglich sein, was vor allem Fragen zur technischen Umsetzbarkeit auslöst. Die Einwilligung muss zudem so präzise wie möglich ausgestaltet sein und kann nicht als pauschale Einwilligung erteilt

[124] DSB 31. 7. 2018, DSB-D213.642/0002-DSB/2018.
[125] Vgl ErwGr 42 Satz 1 DSGVO.
[126] *Kastelitz* in *Knyrim*, DatKomm Art 7 DSGVO (Stand 7.5.2020, rdb.at) Rz 13.
[127] *Jahnel/Pallwein-Prettner*, Datenschutzrecht 75.
[128] DSB 21.02.2019, DSB-123.311/0003-DSB/2019.
[129] *Buchner/Petri* in *Kühling/Buchner* (Hrsg), DS-GVO – BDSG[2] (2018) Art 6 Rz 22.
[130] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 24.

werden.[131] Demnach könnte eine Einwilligung wohl nur für die Durchführung eines einmaligen Abfragens eines Registers erteilt werden und wäre nur auf einen konkreten Anwendungsfall beschränkt.

### *3.1.2. Erfüllung einer rechtlichen Verpflichtung*

Die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt (Art 6 Abs 1 lit c DSGVO) bedarf einer Grundlage im Unionsrecht oder im Recht eines Mitgliedstaats. In Art 6 Abs 1 lit c DSGVO wird zwischen öffentlichem und nicht-öffentlichem Bereich nicht unterschieden, weshalb auch die behördliche Datenverarbeitung darunterfällt.[132] Mit der Öffnungsklausel in Art 6 Abs 2 DSGVO wird den Mitgliedstaaten die Möglichkeit eingeräumt, spezifischere Bestimmungen zur Anpassung der Zulässigkeitstatbestände der rechtlichen Verpflichtung nach Art 6 Abs 1 lit c DSGVO und der Verarbeitung durch die öffentliche Hand nach Art 6 Abs 1 lit e DSGVO beizubehalten oder einzuführen.[133]

In den Erwägungsgründen wird ausgeführt, dass nicht für jede einzelne Verarbeitung ein spezifisches Gesetz erforderlich ist, sondern ein Gesetz als Grundlage für mehrere Verarbeitungsvorgänge ausreichend sein kann.[134] Im Unionsrecht oder im Recht der Mitgliedstaaten sollte geregelt werden, für welche Zwecke die Daten verarbeitet werden dürfen. Darüber hinaus geht aus den Erwägungsgründen hervor, dass in diesem Recht auch die allgemeinen Bedingungen der DSGVO zur Regelung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten präzisiert und festgelegt werden könnten, etwa „wie der Verantwortliche zu bestimmen ist, welche Arten von personenbezogenen Daten verarbeitet werden, welche Personen betroffen sind, welchen Einrichtungen die personenbezogenen Daten offengelegt, für welche Zwecke und wie lange sie gespeichert werden dürfen und welche anderen Maßnahmen ergriffen werden, um zu gewährleisten, dass die Verarbeitung rechtmäßig und nach Treu und Glauben erfolgt."[135]

---

[131] *Jahnel/Pallwein-Prettner*, Datenschutzrecht 72.
[132] *Heberlein* in *Ehmann/Selmayr* (Hrsg), DS-GVO[2] (2018) Art 6 Rz 15.
[133] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 56; *Jahnel/Pallwein-Prettner*, Datenschutzrecht 79.
[134] ErwGr 45 DSGVO.
[135] ErwGr 45 DSGVO.

§ 6 Abs 2 USPG besagt, dass die Übermittlung nicht-personenbezogener und personenbezogener Daten sowie entsprechender Metadaten nur soweit zulässig ist, als dafür eine ausreichende datenschutzrechtliche Grundlage besteht. Entsprechend den Erläuterungen kann sich diese Grundlage sowohl aufgrund von unionsrechtlichen als auch bundes- und landesrechtlichen Vorschriften ergeben.[136] In den Erläuterungen wird ausdrücklich festgehalten, dass die Bestimmungen des USPG keine Generalermächtigung zum behördenübergreifenden Informationsaustausch darstellen, sondern lediglich der Vorbereitung der technischen und organisatorischen Grundlagen für die Anwendung des Once-Only-Prinzips dienen.[137]

### *3.1.3. Öffentliches Interesse oder Ausübung öffentlicher Gewalt*

Der Erlaubnistatbestand nach Art 6 Abs 1 lit e DSGVO umfasst die Datenverarbeitung durch Behörden und andere öffentliche Stellen als auch die Wahrnehmung von Aufgaben im öffentlichen Interesse durch eine natürliche oder juristische Person des Privatrechts, sofern ihr eine eigenverantwortliche Datenverarbeitung für diese Zwecke übertragen wurde.[138] Dieser Tatbestand ist für die öffentliche Verwaltung am bedeutendsten, stellt für sich allein aber noch keinen Rechtfertigungsgrund dar.[139] Ebenso wie die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung bedarf es für diesen Tatbestand einer Regelung durch das Unionsrecht oder das Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, wofür den Mitgliedstaaten mit der Öffnungsklausel nach Art 6 Abs 2 DSGVO gestattet ist, spezifischere Bestimmungen zu erlassen.[140] Nach Art 6 Abs 3 S 2 DSGVO muss sichergestellt werden, dass der Zweck notwendig zur Erfüllung der gesetzlich übertragenen und zugleich auch hinreichend bestimmten Aufgabe ist.[141]

Die Bestimmung des Art 6 Abs 1 lit e DSGVO eröffnet zwar ein großes Anwendungsspektrum, dies erfordert aber nach der Artikel-29-Datenschutzgruppe eine

---

[136] ErlRV 944 BlgNR XXVII. GP 2.
[137] ErlRV 944 BlgNR XXVII. GP 2.
[138] *Jahnel/Pallwein-Prettner*, Datenschutzrecht 79.
[139] Vgl Art 6 Abs 3 DSGVO.
[140] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 45 und 56.
[141] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 47.

strenge Auslegung und klare Benennung des öffentlichen Interesses.[142] Die Anforderungen der DSB an die Qualität der gesetzlichen Grundlage bei staatlichen Behörden gelten als besonders streng.[143] Nach der Rechtsprechung des EuGH zu Art 7 lit e DS-RL[144] ist die Tätigkeit eines Hoheitsträgers, die darin besteht, Daten, die Unternehmen aufgrund gesetzlicher Pflichten übermitteln müssen, in einer Datenbank zu speichern, interessierten Person Einsicht zu gewähren und ihnen Kopien dieser Daten zur Verfügung zu stellen, zur Ausübung hoheitlicher Befugnisse zu zählen. Zudem wird festgehalten, dass eine solche Tätigkeit auch eine im öffentlichen Interesse liegende Aufgabe im Sinne dieser Bestimmung darstellt.[145]

Die Tätigkeit des RSV besteht darin, als Datendrehscheibe den behördenübergreifenden Austausch von Daten zu ermöglichen. Der RSV bildet den Kern der Once-Only-Plattform und soll künftig für nationale und grenzüberschreitende Anwendungsfälle eingesetzt werden.[146] Der Datenaustausch über den RSV soll zur Umsetzung des Once-Only-Grundsatzes beitragen und Bürger:innen, Unternehmen und Behörden gleichermaßen entlasten. Maßnahmen, die zur Umsetzung einer digitalen und effizienten Verwaltung beitragen, können wohl als öffentliches Interesse betrachtet werden. Unter der Prämisse der Schaffung einer entsprechenden gesetzlichen Regelung wäre dieser Tatbestand eine geeignete Rechtsgrundlage.

### *3.1.4. Weiterverarbeitung*

Grundsätzlich wäre auch denkbar, dass die Datenverarbeitung durch den RSV eine Weiterverarbeitung im Sinne des Art 6 Abs 4 DSGVO darstellt. Mit dieser Bestimmung wird ermöglicht, dass eine Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, verarbeitet werden.[147] Damit erfolgt eine Durchbrechung des Zweckbindungsgrundsatzes (Art 5 Abs 1 lit b DSGVO). Die Daten, die über den RSV übermittelt werden, bestehen bereits in Registern. Hier stellt

---

[142] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim,* DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 47; Artikel-29-Datenschutzgruppe, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der RL 95/46/EG, WP217, 28.
[143] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim,* DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 47.
[144] Datenschutzrichtlinie, Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
[145] EuGH 9. 3. 2017, C-398/15, *Manni,* Rn 43.
[146] Vorblatt und WFA zur Regierungsvorlage: 944 BlgNR XXVII. GP 1.
[147] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim,* DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 4.

sich die Frage, ob die Tätigkeit des RSV einen Verarbeitungsvorgang im Sinne des Art 4 Z 2 DSGVO oder eine Weiterverarbeitung darstellt. In weiterer Folge kommt es auf die Art der Weiterverarbeitung an, wobei für die Zulässigkeit der Zweckänderung ein „Kompatibilitätstest" zur Anwendung kommt.[148] Der neue geänderte Zweck darf nicht mit dem bei der erstmaligen Datenverarbeitung festgelegten Zweck unvereinbar sein. Eine unvereinbare Weiterverwendung wäre nur erlaubt, wenn eine Einwilligung in die zweckändernde Weiterverarbeitung erteilt wurde oder eine Rechtsvorschrift der Union oder der Mitgliedstaaten dies erlaubt.[149]

Zur Feststellung der Vereinbarkeit kann vom Verantwortlichen ein Kompatibilitätstest durchgeführt werden, wobei Art 6 Abs 4 lit a bis e DSGVO Kriterien enthält, sowie die Art-29-Datenschutgruppe Kriterien darlegt.[150] Die Kriterien umfassen im Wesentlichen den Primärzweck und das Verhältnis zum Sekundärzweck, den Kontakt der Datenerhebung, die Qualität der Daten, Folgen für die betroffenen Person sowie Schutzmechanismen. Grundsätzlich wäre denkbar, dass die Datenübermittlung durch den RSV mit den Zwecken der erstmaligen Datenverarbeitung vereinbar wäre, allerdings wäre dieser Kompatibilitätstest für jeden Anwendungsfall zu prüfen. Eine Berufung auf eine Weiterverarbeitung im Sinne des § 6 Abs 4 DSGVO wäre daher für die Verarbeitung durch den RSV wenig praxistauglich.

## *3.2. Zulässigkeit nach dem DSG*

Das in § 1 Abs 1 DSG verankerte Recht auf Geheimhaltung umfasst einerseits den Schutz der Betroffenen vor Ermittlung ihrer Daten und andererseits den Schutz vor der Weitergabe der über sie ermittelten Daten.[151] Die Tätigkeit des RSV kann als eine solche Weitergabe bereits ermittelter Daten gesehen werden. Nach § 1 Abs 2 DSG setzt ein Eingriff in das Grundrecht auf Datenschutz durch eine staatliche Stelle voraus, dass der Eingriff zur Wahrung überwiegender berechtigter Interessen eines anderen erfolgt (Interessenabwägung), nur aufgrund von Gesetzen erfolgt, die aus den in Art 8 Abs 2 EMRK genannten Gründen notwendig sind (materieller Gesetzesvorbehalt) und in der

[148] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 4.
[149] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 60.
[150] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 61 f mit Verweis auf Artikel-29-Datenschutzgruppe, Opinion 03/2013 on purpose limitation (WP203) Annex 1, 43 f.
[151] *Thiele/Wagner*, Praxiskommentar zum DSG § 1 Rz 12.

gelindesten, zum Ziel führenden Art vorgenommen wird.[152] Nach stRsp muss ein Eingriffsgesetz zudem dem Bestimmtheitsgebot entsprechen.[153] Bei Eingriffen in sensible Daten muss die Wichtigkeit des Eingriffstatbestandes zur Wahrung wichtiger öffentlicher Interessen nachgewiesen werden.[154] Während aus den Erläuterungen zum DSG hervorgeht, dass sich das Erfordernis einer Gesetzgrundlage für Behörden nur auf die überwiegenden Interessen eines anderen bezieht und demnach das lebenswichtige Interesse des Betroffenen und die Zustimmung mögliche Rechtfertigungsgründe wären,[155] wird teilweise in der Literatur bzw auch von der DSB die Ansicht vertreten, dass Eingriffe von staatlichen Behörden nur auf Grund von Gesetzen zulässig sind.[156]

Die gesetzliche Grundlage muss gemäß § 1 Abs 2 DSG notwendig iSd Art 8 Abs 2 EMRK[157] sein. Nach der Judikatur des VfGH hat der Gesetzgeber eine materienspezifische Regelung vorzusehen, die die Fälle zulässiger Eingriffe in das Grundrecht auf Datenschutz konkretisieren und begrenzen.[158] Für die Beurteilung des überwiegenden berechtigten Interesses ist das Interesse des Betroffenen an der Geheimhaltung mit dem Interesse am staatlichen Eingriff abzuwägen.[159]

### *3.3. Fazit*

Als Rechtsgrundlage für die Datenverarbeitung durch den RSV ist der Tatbestand des Art 6 Abs 1 lit e iVm Abs 6 Abs 2 und 3 DSGVO am naheliegendsten. Die Rechtmäßigkeit der Verarbeitung nach Art 6 Abs 1 lit e bedarf demnach einer zusätzlichen rechtlichen Regelung, die sich an Art 6 Abs 2 und 3 messen lassen muss.[160]

In der Rechtsgrundlage muss der Zweck festgelegt oder hinsichtlich der Verarbeitung für die Erfüllung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung

---

[152] *Thiele/Wagner*, Praxiskommentar zum DSG § 1 Rz 51 mit Verweis auf *Jahnel*, Verfassungsrechtliche Fragen der elektronischen Gesundheitsakte in FS Stolzlechner 2014, 309 (313).
[153] *Thiele/Wagner*, Praxiskommentar zum DSG § 1 Rz 51 mit Verweis auf VfGH 1.10.2013, G 2/2013 (Beweisverwertungsverbot).
[154] *Thiele/Wagner*, Praxiskommentar zum DSG § 1 Rz 51; *Jahnel*, Verfassungsrechtliche Fragen der elektronischen Gesundheitsakte in FS Stolzlechner 2014, 313.
[155] ErlRV 1613 BlgNR XX. GP 35.
[156] *Thiele/Wagner*, Praxiskommentar zum DSG § 1 Rz 55; DSB 12.04.2019, DSB-D123.591/0003-DSB/2019.
[157] Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl 1958/210.
[158] *Thiele/Wagner*, Praxiskommentar zum DSG § 1 Rz 55 mit Verweis auf VfGH 23.6.2014, G 90/2013).
[159] VfGH 17.12.2009, B504/09.
[160] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 47.

öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, erforderlich sein.[161] Die Erforderlichkeit muss im Sinne der Verhältnismäßigkeit gemäß Art 52 Abs 1 GRC und Art 6 Abs 3 S 4 DSGVO sowie § 1 Abs 2 DSG iVm Art 8 Abs 2 EMRK hohe Maßstäbe erfüllen.[162] Diese ist aufgrund des Beitrags des RSV zur Umsetzung des Once-Only-Prinzips im Sinne der Single-Digital-Gateway-Verordnung und damit einer digitalen und effizienteren Verwaltung als eine von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen zu betrachten. Der Erlaubnistatbestand gemäß Art 6 Abs 1 lit e DSGVO würde daher für die Datenverarbeitung auf Grundlage der Once-Only-Plattform, unter der Voraussetzung der Schaffung einer gesetzlichen Grundlage, in Frage kommen. Obwohl die Einrichtung des RSV im USPG gesetzlich vorgesehen ist, wird in den Erläuterungen festgehalten, dass dies keine Generalermächtigung zum Datenaustausch darstellt.

Bei Betrachtung der Umstände eines Einzelfalls wäre grundsätzlich denkbar, die Einwilligung als Rechtsgrundlage heranzuziehen. Dafür müsste neben den inhaltlichen Voraussetzungen (Freiwilligkeit, Bestimmtheit, Information, Verständlichkeit, leichte Zugänglichkeit, klare und einfache Sprache) sichergestellt werden, dass der Verantwortliche nachweisen kann, dass in die Verarbeitung eingewilligt wurde[163] und dass Betroffene jederzeit ihre Einwilligung widerrufen können.[164] Abgesehen davon, dass die Einwilligung wie oben ausgeführt gegenüber Behörden nicht unumstritten ist, ist die Umsetzung in der Praxis für die Verarbeitung des RSV mit zahlreichen Herausforderungen verbunden. Als langfristige Lösung empfiehlt sich eine gesetzliche Grundlage, vor allem auch aufgrund des Umstands, dass für die Tätigkeit von Behörden „andere Rechtsgrundlagen“ (insb Art 6 Abs 1 lit c und lit e DSGVO) grundsätzlich als angemessener gelten als Einwilligungen.[165]

---

[161] Art 6 Abs 1 lit e DSGVO.
[162] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO (Stand 7.5.2020, rdb.at) Rz 47.
[163] Vgl Art 7 Abs 1 DSGVO.
[164] Vgl Art 7 Abs 3 DSGVO.
[165] Art 29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP259rev.01, 7 ff; ErwGr 42 f DSGVO.

# 4. Betroffenenrechte und Transparenz

## *4.1. Einleitung*

Über den Register- und Systemverbund wird eine Vielzahl personenbezogener Daten verarbeitet werden. Die Bestimmungen der DSGVO räumen Betroffenen bestimmte Rechte ein und stellen Transparenzanforderungen an die Verarbeitung. In Zusammenhang mit Betroffenenrechten und Anforderungen an die Transparenz der Datenverarbeitung durch den RSV ist grundlegend, welche konkreten personenbezogenen Daten verarbeitet werden, auf welcher Grundlage dies erfolgt, wer für die Datenverarbeitung verantwortlich ist und welche Rechte Betroffene geltend machen können. In weiterer Folge ist entscheidend, welche Daten beim RSV protokolliert werden bzw was protokolliert werden müsste, um der Erfüllung der Transparenzanforderungen und der Erfüllung der Betroffenenrechte gerecht werden zu können. Der Grundsatz der Transparenz, der vorsieht, dass bestimmte Daten gespeichert werden sollen, um eine Nachvollziehbarkeit der Verarbeitung zu gewährleisten, steht im Spannungsverhältnis zum Grundsatz der Datenminimierung, wonach möglichst wenig personenbezogene Daten gespeichert werden sollen.

Kapitel III der DSGVO enthält entsprechend seinem Titel „Rechte der betroffenen Person" eine beinahe abschließende Regelung der Rechte der betroffenen Personen.[166] Darüber hinaus wird in Art 34 DSGVO das Recht auf Benachrichtigung im Falle einer Verletzung des Schutzes personenbezogener Daten geregelt. Nach der Systematik der DSGVO wird zunächst das Verfahren zur Erfüllung der Betroffenenrechte durch den Verantwortlichen geregelt und der Grundsatz der Transparenz präzisiert. Art 12 Abs 3 S 1 DSGVO sieht für die Erledigung von Betroffenenanträgen durch den Verantwortlichen unverzügliches Handeln vor und räumt eine Frist von einem Monat ein, die in komplexen Fällen bis auf drei Monate ausgedehnt werden kann.[167] Anschließend kann unterschieden werden zwischen aktiven Informationsverpflichtungen des Verantwortlichen („push") und Betroffenenrechten als Ausdruck des Selbstdatenschutzes der betroffenen Person

[166] *Haidinger/Illibauer*, Informationspflichten und Betroffenenrechte in Praxishandbuch Datenschutzrecht 199.
[167] *Haidinger/Illibauer* in Praxishandbuch Datenschutzrecht 215; *Hödl* in *Knyrim*, DatKomm Art 4 DSGVO (Stand 1.12.2018, rdb.at) Rz 79.

(„pull“).[168] Den Betroffenen werden neben den Informationspflichten des Verantwortlichen sieben verschiedene Begleitrechte gegenüber dem Verantwortlichen eingeräumt, die in den Art 15 bis 22 DSGVO festgeschrieben sind.[169] Grundlegende Voraussetzung für die Anwendbarkeit der Betroffenenrechte ist, dass die Datenverarbeitung in den Anwendungsbereich der DSGVO fällt, dh automatisiert oder in einem Dateisystem verarbeitet werden und nur von betroffenen bzw potenziell betroffenen Personen geltend gemacht werden können.[170]

Der Grundsatz der Transparenz gemäß Art 5 Abs 1 lit a DSGVO war in der DS-RL und im DSG 2000 implizit in Form der Bestimmungen zur Informationspflicht enthalten und wird in der DSGVO durch Art 13 und 14 sowie Art 12 zu den Modalitäten konkretisiert. Art 5 Abs 1 lit a DSGVO wird im Verhältnis der Behörde zum Bürger durch eine Reihe von Informationspflichten präzisiert. Diese treten im Gegensatz zu Auskunftsansprüchen von Amts wegen ein.[171] Die Informationsverpflichtungen und Betroffenenrechte bestehen nebeneinander und schließen einander nicht aus, weisen allerdings gewisse Überschneidungen auf.[172]

§ 1 Abs 1 DSG sieht explizit das Recht des Betroffenen auf Geheimhaltung vor. Die Rechte auf Auskunft, Berichtigung und Löschung sind durch § 1 Abs 3 DSG verfassungsrechtlich gewährleistet, die Rechte auf Auskunft und Berichtigung sind auch in Art 8 Abs 2 GRC verankert.[173]

Ein transparenter Umgang mit personenbezogenen Daten ist insbesondere im Bereich der öffentlichen Verwaltung unerlässlich. Behörden erheben und speichern Daten der Bürger:innen, wobei Bürger:innen nicht immer erfahren oder überblicken können, wann und zu welchem Zweck Daten abgefragt wurden.[174] Können Bürger:innen einsehen, welche Behörden welche Daten zu welchen Zwecken verarbeiten, schafft dies nicht nur Vertrauen, sondern stärkt auch das Recht auf informationelle Selbstbestimmung.[175]

---

[168] *Haidinger/Illibauer* in Praxishandbuch Datenschutzrecht 199.
[169] *Haidinger/Illibauer* in Praxishandbuch Datenschutzrecht 214.
[170] *Haidinger/Illibauer* in Praxishandbuch Datenschutzrecht 215.
[171] *Reimer*, Verwaltungsdatenschutzrecht 148 ff.
[172] *Haidinger/Illibauer* in Praxishandbuch Datenschutzrecht 199.
[173] *Haidinger/Illibauer* in Praxishandbuch Datenschutzrecht 214.
[174] *Krimmer/Margraf*, Empfehlungen zur digitalen Transformation der Verwaltung Deutschlands in Bertelsmann Stiftung (Hrsg), Digitale Transformation der Verwaltung 2017, 36.
[175] *Krimmer/Margraf*, Empfehlungen zur digitalen Transformation der Verwaltung Deutschlands 36.

## *4.2. Die Betroffenenrechte im Überblick*

### *4.2.1. Das Recht auf Information (Art 13 und 14 DSGVO)*

Bei einer Erhebung von Daten durch eine Behörde, hat diese im Anwendungsbereich der DSGVO die betroffene Person darüber grundsätzlich zu informieren und bestimmte ergänzende Angaben zu machen.[176] Die Informationspflicht entfällt, wenn die Person über die Erhebung als solche und über die Gegenstände der ergänzenden Angaben bereits informiert ist.[177] Die Pflicht muss zum Zeitpunkt der Erhebung oder bis zu den in Art 14 Abs 3 DSGVO genannten Zeitpunkten erfüllt werden.[178]

Art 14 ist anzuwenden, wenn Daten nicht bei der betroffenen Person direkt erhoben werden, sondern bei anderen Verantwortlichen oder öffentlichen Quellen.[179] Die Informationspflichten werden frühestens zum Zeitpunkt der Datenerhebung schlagend. Da es keine Legaldefinition von „Erheben" gibt, wird diese unter „Verarbeitung" iSd Art 4 Z 2 DSGVO subsumiert. Mit „Erheben" wird nach ständiger Literatur jedenfalls der Beginn eines Datenverarbeitungsvorgangs verstanden und setzt ein aktives Tun voraus.[180] Die Möglichkeit, die Daten inhaltlich zur Kenntnis nehmen zu können, ist ausreichend, eine tatsächliche Kenntnisnahme ist nicht erforderlich.[181] Lediglich wenn die Daten ohne jegliches aktives Handeln des Verantwortlichen in dessen Verfügungsbereich gelangen und dieser die Daten auch nicht in irgendeiner Form verwendet, liegt kein Erheben iSd Art 4 Z 2 DSGVO vor.[182] Die Weiterleitung der Daten über den RSV erfolgt auf Anfrage eines Data Consumers. Somit liegt ein aktives Handeln vor und die Daten werden auch zumindest in irgendeiner Form verwendet. Die Verarbeitungstätigkeit, die auf dem RSV als Datendrehscheibe erfolgt, stellt daher ein „Erheben" iSd Art 4 Z 2 DSGVO dar.

Grundsätzlich gilt, dass diese Informationspflicht durch Mitteilungen im Einzelfall zu erfüllen sind, jedoch können Informationen an die Öffentlichkeit, etwa durch Veröffentlichung einer Datenschutzerklärung auf der Behördenwebsite zur Erfüllung

---

[176] *Reimer*, Verwaltungsdatenschutzrecht 149.
[177] *Reimer*, Verwaltungsdatenschutzrecht 149.
[178] *Reimer*, Verwaltungsdatenschutzrecht 149.
[179] *Illibauer* in *Knyrim*, DatKomm Art 14 DSGVO (Stand 1.10.2018, rdb.at) Rz 11; *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 14 DSGVO (Stand 1.12.2020, rdb.at) Rz 1.
[180] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung (2020) Art 4 Z 2 DSGVO 8.
[181] *Hödl* in *Knyrim*, DatKomm Art 4 DSGVO (Stand 1.12.2018, rdb.at) Rz 29.
[182] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung (2020) Art 4 Z 2 DSGVO 8.

genügen, wenn die betroffenen Personen darüber individuell und gezielt erreicht werden können.[183] In der Datenschutzerklärung sollte jedenfalls der Verantwortliche, der Verarbeitungszweck, die Rechtsgrundlage für die Datenverarbeitung, Angaben ob bzw wie lange Daten gespeichert werden und Hinweise auf die Rechte auf Auskunft, Berichtigung, Löschung und Einschränkung enthalten sein.[184]

### *4.2.2. Das Recht auf Auskunft (Art 15 DSGVO)*

Das Recht auf Auskunft nach Art 15 DSGVO ist „zentraler Bestandteil des Selbstdatenschutzes."[185] Es ermöglicht der betroffenen Person Grundlegendes über die Verarbeitung zu erfahren, insbesondere ob und welche verarbeitet werden und auf welcher Rechtsgrundlage die Verarbeitung basiert.[186] Vom Recht auf Auskunft ist das Recht auf Auskunft über konkret verarbeitete Daten (Art 15 Abs 1), das Recht auf Datenkopie (Art 15 Abs 3) sowie bestimmte Zusatzinformationen (Art 15 Abs 1 lit a-h, Abs 2) erfasst, etwa Kategorien der Daten, die verarbeitet werden oder Empfänger der Daten oder alle verfügbare Informationen über die Herkunft der Daten.

Das Auskunftsrecht kann sich grundsätzlich auch auf Daten erstrecken, die auch andere Personen betreffen („auch sie betreffende Daten").[187] Vom Auskunftsrecht nicht erfasst sind Zugangsprotokolle, aus denen hervorgeht, welche Mitarbeiter:innen des Verantwortlichen wann welche Daten verarbeitet haben, da diese nicht als zur betroffenen Person verarbeitete Daten zählen und es der betroffenen Person in der Regel keinen Vorteil verschafft, wenn sie die Namen der Personen kennt, die ihre Daten eingegeben haben.[188] Eine Ausnahme wäre zu machen, wenn die betroffene Person ein besonderes Interesse an einer Benennung der konkreten Person für Zwecke der Verfolgung ihrer Rechte darlegen kann.[189]

Nach der DSGVO kann eine Auskunft bei „Exzessivität" des Antrags iSd Art 12 Abs 5 DSGVO verweigert werden oder wenn die Auskunft das Recht und die Freiheit anderer

---

[183] *Reimer*, Verwaltungsdatenschutzrecht 148.
[184] *Haidinger/Illibauer* in *Knyrim*, Datenschutzrecht[4] Kap 8 (Stand 1.4.2020, rdb.at) Rz 8.124.
[185] *Haidinger* in *Knyrim*, DatKomm Art 15 DSGVO (Stand 1.10.2018, rdb.at) Rz 1.
[186] *Haidinger/Illibauer* in Praxishandbuch Datenschutzrecht 218.
[187] *Haidinger* in *Knyrim*, DatKomm Art 15 DSGVO (Stand 1.10.2018, rdb.at) Rz 31.
[188] *Haidinger* in *Knyrim*, DatKomm Art 15 DSGVO (Stand 1.10.2018, rdb.at) Rz 31.
[189] *Haidinger* in *Knyrim*, DatKomm Art 15 DSGVO (Stand 1.10.2018, rdb.at) Rz 31 mit Verweis auf DSK 2. 8. 2005, K121.038/0006-DSK/2005 sowie BVwG 11. 7. 2017, W214 2117640-1.

Personen beeinträchtigt.[190] Mit Art 23 DSGVO wird den mitgliedstaatlichen Gesetzgebern die Möglichkeit eröffnet, Rechtsvorschriften zu schaffen, die unter bestimmten Voraussetzungen Beschränkungen von Betroffenenrechten und damit unter anderem die Ablehnung von Auskünften vorsehen. Die Beschränkungsmöglichkeiten auf Grundlage von Art 23 DSGVO werden in Kapitel 4.3 erörtert.

Um dem Auskunftsrecht entsprechen zu können, muss für die Datenverarbeitung auf Grundlage des RSV sichergestellt werden, dass der Datenaustausch entsprechend protokolliert wird. Es ist nicht ausreichend, dass gespeichert wird, dass eine Anfrage gestellt und eine Antwort erfolgt ist, sondern es muss die Möglichkeit bestehen, konkret verarbeitete Daten zu beauskunften. Der Register- und Systemverbund selbst speichert die Daten, die über ihn übermittelt werden, nicht. Um dem Auskunftsrecht entsprechen zu können, wäre technisch sicherzustellen, dass bei den verantwortlichen Stellen die Abfragen entsprechend protokolliert werden. Diese Protokollierung sollte in der Auftragsvereinbarung zwischen den Verantwortlichen und dem Auftragsverarbeiter festgelegt werden.

### *4.2.3. Die Rechte auf Berichtigung und Löschung (Art 16, 17 und 19 DSGVO)*

Mit dem nach Art 16 DSGVO gewährten Recht auf Berichtigung können betroffene Personen die Berichtigung unrichtiger Daten, die der Verantwortliche verarbeitet, verlangen. Allenfalls haben sie ein Recht auf Vervollständigung.[191] Der RSV speichert in seiner Funktion als Datendrehscheibe keine Daten und prüft diese auch inhaltlich nicht. Das Recht auf Berichtigung oder Löschung kann gegenüber registerführenden Behörden daher unabhängig von der Tätigkeit des RSV ausgeübt werden.

### *4.2.4. Das Recht auf Einschränkung der Verarbeitung (Art 18 DSGVO)*

Mit Art 18 DSGVO wird den betroffenen Personen ein temporärer Begleitanspruch auf Einschränkung der Verarbeitung iZm den Rechten auf Berichtigung, Löschung sowie Widerspruch (Art 21 DSGVO) eingeräumt. Damit können Betroffene erreichen, dass ihre Daten nur mehr gespeichert, aber nicht mehr wie sonst verarbeitet werden.[192] Wie bereits dargelegt, sind die Rechte auf Berichtigung und Löschung für die unmittelbare Tätigkeit

[190] *Haidinger/Illibauer* in Praxishandbuch Datenschutzrecht 222 f.
[191] *Haidinger/Illibauer* in Praxishandbuch Datenschutzrecht 224.
[192] *Haidinger/Illibauer* in Praxishandbuch Datenschutzrecht 225.

auf Basis des RSV nicht relevant, weshalb der temporäre Anspruch auf Einschränkung der Verarbeitung diesbezüglich keine Wirkung entfalten kann. Das Recht auf Einschränkung der Verarbeitung in Zusammenhang mit einem Widerspruch nach Art 21 DSGVO kann hingegen durchaus von Bedeutung sein, da die betroffene Person mit dem Recht auf Widerspruch eine grundsätzlich zulässige Datenverarbeitung unter Umständen untersagen kann.[193] Das Recht auf Widerspruch wird in Kapitel 4.2.6 näher erörtert.

### *4.2.5. Das Recht auf Datenübertragbarkeit (Art 20 DSGVO)*

Das Recht auf Datenübertragbarkeit verfolgt das Ziel, dass betroffene Personen „ihre" Daten erhalten und für eigene Zwecke und verschiedene Dienste wiederverwenden einschließlich durch andere Verantwortliche verarbeiten lassen können. In der öffentlichen Verwaltung kommt das Recht auf Datenübertragbarkeit nur eingeschränkt zur Anwendung.[194] Voraussetzung hierfür ist, dass die Verarbeitung mithilfe automatisierter Verfahren erfolgt und auf einer Einwilligung (Art 6 Abs 1 lit a DSGVO) oder einem Vertrag mit der betroffenen Person (Art 6 Abs 1 lit b DSGVO) beruht. Dieses Recht ist für die Datenverarbeitung auf Grundlage des RSV schon aufgrund der Tatsache, dass beim RSV selbst keine Daten gespeichert werden, die an Betroffene übertragen werden könnten, nicht relevant.

### *4.2.6. Das Recht auf Widerspruch (Art 21 DSGVO)*

Art 21 DSGVO gewährt Betroffenen ein Widerspruchrecht, womit eine grundsätzlich zulässige Datenverarbeitung aufgrund bestimmter persönlicher Umstände untersagt werden kann.[195] Das Widerspruchrecht besteht nach Art 21 Abs 1 DSGVO vor allem bei der Verarbeitung aufgrund einer Aufgabe im öffentlichen Interesse (Art 6 Abs 1 lit e DSGVO) bzw bei der Verarbeitung aufgrund berechtigter Interessen (Art 6 Abs 1 lit f DSGVO). Der Verantwortliche darf die Daten weiterverarbeiten, wenn er zwingende schutzwürdige Gründe nachweisen kann, die den Interessen, Rechten und Freiheiten Betroffener überwiegen oder die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.[196] Betroffenen Personen wird in Art 21 Abs 2 DSGVO ein absolutes Widerspruchsrecht eingeräumt, wonach Datenverarbeitungen zum

---

[193] *Haidinger* in *Knyrim*, DatKomm Art 21 DSGVO (Stand 1.10.2018, rdb.at) Rz 1.
[194] *Lachmayer*, Die DSGVO im öffentlichen Bereich, ÖJZ 2018/17.
[195] ErwGr 69 S 1 DSGVO.
[196] *Sommer*, Betroffenenrechte in *Lühr/Jabkowski/Smentek*, Handbuch Digitale Verwaltung (2019) 239.

Zwecke der Direktwerbung und Profiling in diesem Zusammenhang ohne Angabe von Gründen untersagt werden können.[197] Das relative Widerspruchsrecht gemäß Art 21 Abs 1 und Abs 6 DSGVO greift nur dann, wenn die Daten der betroffenen Person in Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt oder zur Wahrung berechtigter Interessen des Verantwortlichen verarbeitet werden.[198] Daraus folgt, dass bei einer rechtlichen Verpflichtung zur Verarbeitung (Art 6 Abs 1 lit c DSGVO) kein Widerspruch möglich wäre.[199]

Für die Geltendmachung des Widerspruchsrechts müssen betroffene Personen besondere persönliche Gründe nachweisen, warum die Verarbeitung unzulässig ist (Widerspruchsinteresse).[200] Die vorgebrachten Gründe müssen vom Unionsrecht oder nationalen Recht iwS anerkannt sein und derart „besonders" sein, dass sie bei einem Durchschnittsbetroffenen nicht vorliegen.[201] Ein erfolgreicher Widerspruch erfüllt den Löschungsanspruch des Art 17 Abs 1 lit c DSGVO und berechtigt für die Dauer der Prüfung zur Einschränkung der Datenverarbeitung nach Art 18 Abs 1 lit d DSGVO.[202] Wie bereits ausgeführt ist das Recht auf Löschung bei der Datenverarbeitung auf Grundlage des RSV nicht zielführend, da dieser selbst keine Daten speichert. Jedoch könnte unter der Prämisse, dass die Datenverarbeitung des RSV auf Grundlage von Art 6 Abs 1 lit e DSGVO erfolgt und die Betroffenen die Anforderungen für persönliche Gründe, die Verarbeitung zu untersagen, vorweisen können, ein Widerspruch zu einer Einschränkung der Verarbeitung im Sinne eines Unterbindens des Datenaustauschs zwischen Behörden führen.

### *4.2.7. Das Recht auf Intervention bei einer automatisierten Entscheidung im Einzelfall (Art 22 DSGVO)*

Betroffene Personen haben das Recht auf Intervention bei einer automatisierten Entscheidung im Einzelfall, die ausschließlich auf automatisierter Verarbeitung einschließlich Profiling beruht, sofern diese rechtliche Wirkungen entfaltet oder die

---

[197] *Jahnel/Pallwein-Prettner*, Datenschutzrecht 119.
[198] *Haidinger* in *Knyrim*, DatKomm Art 21 DSGVO (Stand 1.10.2018, rdb.at) Rz 19.
[199] *Haidinger/Illibauer* in Praxishandbuch Datenschutzrecht 235.
[200] *Haidinger* in *Knyrim*, DatKomm Art 21 DSGVO (Stand 1.10.2018, rdb.at) Rz 20.
[201] *Haidinger* in *Knyrim*, DatKomm Art 21 DSGVO (Stand 1.10.2018, rdb.at) Rz 21; *Haidinger/Illibauer* in Praxishandbuch Datenschutzrecht 235.
[202] *Haidinger/Illibauer* in Praxishandbuch Datenschutzrecht 235.

betroffene Person in ähnlicher Weise erheblich beeinträchtigt.[203] Über den RSV werden Daten abgefragt und übermittelt. Diese Daten können als Grundlage für automatisierte Entscheidungen herangezogen werden, der RSV selbst trifft jedoch keine Entscheidungen. Das Recht auf Intervention bei einer automatisierten Entscheidung kann daher unabhängig von der Verarbeitung durch den RSV bei der Behörde, der die Entscheidung zugerechnet wird, geltend gemacht werden.

### *4.3. Beschränkungen der Betroffenenrechte*

Art 23 DSGVO eröffnet den mitgliedstaatlichen Gesetzgebern die Möglichkeit, für die Verarbeitung personenbezogener Daten durch öffentliche Stellen von den in den Art 12 bis 22 DSGVO gewährten Betroffenenrechten abzuweichen. Die Anforderungen an mitgliedstaatliche Gesetze, die die zum Grundrecht gehörenden Betroffenenrechte einschränken, sind sehr hoch.[204] Diese Gesetze müssen „den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme“[205] darstellen, die den Schutz wichtiger Ziele sicherstellt. In der Liste dieser Ziele in Art 23 Abs 1 DSGVO finden sich Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats wie zB die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit, aber auch den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats. Für eine Einschränkung der Betroffenenrechte für die Datenverarbeitung durch den RSV ist die Bestimmung des Art 23 Abs 1 lit e DSGVO näher zu betrachten, die „eine Art Generalklausel“[206] zur Verfolgung sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses darstellt. Einige derartige Ziele des allgemeinen öffentlichen Interesses werden in der Bestimmung selbst genannt, insbesondere wirtschaftliche oder finanzielle Interessen der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit.[207] In Erwägungsgrund 73 Satz 1 wird auch das Führen öffentlicher Register aus Gründen des allgemeinen öffentlichen

---

[203] *Haidinger/Illibauer* in Praxishandbuch Datenschutzrecht 237.
[204] *Sommer*, Betroffenenrechte in *Lühr/Jabkowski/Smentek*, Handbuch Digitale Verwaltung 240.
[205] Art 23 DSGVO.
[206] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 23 DSGVO (Stand 1.12.2020, rdb.at) Rz 7.
[207] Art 23 Abs 1 lit e DSGVO.

Interesses erwähnt.[208] Der unbestimmte Rechtsbegriff der „sonstigen wichtigen Ziele des allgemeinen öffentlichen Interesses“ bewirkt, dass die an sich taxative Aufzählung hinsichtlich der öffentlichen Ziele nicht abschließend ist, sondern im interpretativen Weg erweitert werden kann,[209] was Überlegungen zulässt, ob darunter auch die Tätigkeit des Register- und Systemverbunds zählt. Die Verarbeitungstätigkeit auf Grundlage des RSV umfasst das Abfragen bzw den Austausch von Daten aus Registern, jedoch kein Führen von Registern selbst. Diese Tätigkeit unterscheidet sich grundlegend vom Führen eines Registers, da der RSV als Datendrehscheibe lediglich für den Austausch und die Übermittlung von Daten herangezogen wird und gerade nicht selbstständig ein Register führt. Dieser Grund für eine Beschränkung der Betroffenenrechte wird daher für die Verarbeitung des RSV eher nicht in Frage kommen.

Art 23 Abs 2 DSGVO macht es zusätzlich zur Voraussetzung von mitgliedstaatlichen Gesetzgebungsmaßnahmen, die die Betroffenenrechte beschränken, dass sie spezifische Vorschriften enthalten.[210] Dabei handelt es sich um eine demonstrative Aufzählung, die einerseits Angaben zu Gegenstand und Reichweite der Beschränkung und andererseits Angaben zu Schutzmaßnahmen für betroffene Personen vorsieht.[211]

Im Rahmen des Datenschutzgesetzes wurde von der Beschränkungsmöglichkeit des Art 23 DSGVO in § 4 Abs 5 und 6 DSG in Hinblick auf das Recht auf Auskunft gemäß Art 15 DSGVO Gebrauch gemacht.[212] Während § 4 Abs 6 DSG das Auskunftsrecht ausschließt, wenn durch die Erteilung der Auskunft ein Geschäfts- oder Betriebsgeheimnis des Verantwortlichen oder Dritter gefährdet würde,[213] sieht § 4 Abs 5

---

[208] *Haidinger* in *Knyrim*, DatKomm Art 23 DSGVO (Stand 1.12.2022, rdb.at) Rz 17; *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 23 DSGVO (Stand 1.12.2020, rdb.at) Rz 10.
[209] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 23 DSGVO (Stand 1.12.2020, rdb.at) Rz 11.
[210] *Sommer*, Betroffenenrechte in *Lühr/Jabkowski/Smentek*, Handbuch Digitale Verwaltung 240.
[211] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 23 DSGVO (Stand 1.12.2020, rdb.at) Rz 24.
[212] *Haidinger* in *Knyrim*, DatKomm Art 23 DSGVO (Stand 1.12.2022, rdb.at) Rz 4; *Jahnel/Pallwein-Prettner*, Datenschutzrecht 111. Weitere Beschränkungen finden sich beispielsweise in Gesundheitsgesetzen (zB § 3b Abs 2 Ärztegesetz 1998 idF BGBl I 2022/65, § 9a Abs 2 Krankenanstalten- und Kuranstaltengesetz idF BGBl I 2022/79 oder § 6a Abs 3 Apothekengesetz idF BGBl I 2022/65), in Berufsgesetzen (zB § 9 Abs 4 Rechtsanwaltsordnung idF BGBl I 2022/224 oder § 37 Abs 4 Notariatsordnung idF BGBl I 2022/147) oder in Rechtsgrundlagen für den öffentlichen Bereich (zB § 77c Salzburger Raumordnungsgesetz idF LGBl 2022/103); Vgl dazu *Haidinger* in *Knyrim*, DatKomm Art 23 DSGVO (Stand 1.12.2022, rdb.at) sowie *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 23 DSGVO (Stand 1.12.2020, rdb.at).
[213] *Jahnel/Pallwein-Prettner*, Datenschutzrecht 111.

DSG ein Ablehnungsrecht für hoheitlich tätige Verantwortliche vor.[214] Demnach besteht das Recht auf Auskunft gemäß Art 15 DSGVO gegenüber einem hoheitlich tätigen Verantwortlichen nicht, wenn durch die Erteilung der Auskunft die Erfüllung einer dem Verantwortlichen gesetzlich übertragenen Aufgabe gefährdet würde.[215] Diese Bestimmung kann hoheitlich tätige Verantwortliche zur Ablehnung bzw auch Teilablehnung einer Auskunft berechtigen.[216]

Unter der Annahme, dass der Datenverarbeitungstätigkeit des RSV im Zuge der Errichtung der Once-Only-Plattform eine gesetzlich übertragene Aufgabe als Datendrehschreibe zur Umsetzung des Once-Only-Prinzips zugeschrieben wird, wird wohl nicht davon auszugehen sein, dass eine Auskunftserteilung eine solche Aufgabe iSd § 4 Abs 5 DSG gefährden würde, da sich eine Auskunftserteilung iSd Art 15 DSGVO nur auf einzelne Betroffene beziehen und nicht die Tätigkeit des RSV als Datendrehscheibe insgesamt gefährden würde.

## *4.4. Fazit*

Für die Erfüllung der Informationspflichten des bzw der Verantwortlichen empfiehlt sich grundsätzlich die Veröffentlichung einer Datenschutzerklärung, die die erforderlichen Informationen, etwa die Zwecke und Rechtsgrundlagen der Verarbeitung, Informationen über die Ausübung der Betroffenenrechte oder Kontaktdaten des Verantwortlichen enthält. Neben Informationen über das Bestehen von Betroffenenrechten sollten auch Informationen bereitgestellt werden, wie Betroffenenrechte – insbesondere das Auskunftsrecht – ausgeübt werden können und an wen sich Betroffene wenden können. Um dem Auskunftsrecht gerecht werden zu können, ist es notwendig, dass gewisse Informationen bei einem Datenaustausch entsprechend protokolliert werden, um in weiterer Folge von den Verantwortlichen beauskunftet werden zu können.

Für eine konkrete Ausgestaltung der datenschutzrechtlichen Transparenzanforderungen bei Datenverarbeitungen durch öffentliche Stellen können internationale Beispiele betrachtet werden. In Deutschland wurde im März 2021 das

[214] *Haidinger/Illibauer* in Praxishandbuch Datenschutzrecht 223.
[215] § 4 Abs 5 DSG idF BGBl I 2021/148.
[216] *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG) § 4 Rz 83.

Registermodernisierungsgesetz beschlossen.[217] Dieses sieht als Grundlage für die Digitalisierung der Verwaltung eine einheitliche Identifikationsnummer vor. Den datenschutzrechtlichen Transparenzanforderungen soll durch eine umfassende Protokollierung der Datenübermittlungen durch ein sogenanntes Datencockpit nachgekommen werden.[218] Beim Datencockpit handelt es sich um „eine IT-Komponente im Portalverbund, mit der sich natürliche Personen Auskünfte zu Datenübermittlungen zwischen öffentlichen Stellen anzeigen lassen können."[219] Im Datencockpit sollen ausschließlich Protokolldaten angezeigt werden, womit ex post die Kontrollierbarkeit der Datenzugriffe und Datenübermittlungen sichergestellt werden soll. Bürger:innen sollen sich für ein Datencockpit registrieren und festlegen können, in welchem Umfang das Datencockpit Protokolldaten einschließlich der übermittelten Inhaltsdaten erheben und anzeigen darf. Das Datencockpit soll von einer öffentlichen Stelle errichtet und betrieben werden.[220] In Estland haben Bürger:innen über die X-Road-Plattform einen transparenten Überblick über gespeicherte Daten und können so Zugriffe auf diese Daten nachvollziehen.[221]

[217] https://www.bva.bund.de/SharedDocs/Downloads/DE/Behoerden/Verwaltungsdienstleistungen/Register-modernisierung/registermodernisierungsgesetz.html (abgefragt am 01.12.2022).
[218] *Peuker*, Registermodernisierung und Datenschutz, NVwZ 2021, 1172.
[219] Dies wird mit § 10 Onlinezugangsgesetz (OZG) vorgehen, ist aber derzeit noch nicht in Kraft. Vgl Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz – RegMoG) vom 28. März 2021.
[220] *Parycek/Huber/Hunt/Novak/Thapa*, Analyse der rechtlich-technischen Gesamtarchitektur des Entwurfs des Registermodernisierungsgesetzes, Kompetenzzentrum Öffentliche IT 2021, 19.
[221] *Döring/Noack*, Standardisierter Datenaustausch in *Klenk/Nullmeier/Wewer*, Handbuch Digitalisierung in Staat und Verwaltung (2020) 5.

# 5. Sicherheit der Datenverarbeitung

## *5.1. Einleitung*

Neben den datenschutzrechtlichen Anforderungen nehmen auch die Anforderungen an die Datensicherheit stetig zu. Während das Ziel des Datenschutzes ist, personenbezogene Daten zu schützen, verfolgt die Informationssicherheit das Ziel, geeignete Maßnahmen zu treffen, um eine sichere Verarbeitung der Daten zu gewährleisten. In der DSGVO finden sich an mehreren Stellen Regelungen zur Datensicherheit. Die Pflicht, geeignete technische und organisatorische Maßnahmen zu treffen, wurde mit der DSGVO in Art 5 Abs 1 lit f als einer der sechs Grundsätze für die Verarbeitung personenbezogener Daten aufgenommen. Die zentrale Vorschrift zur Sicherheit der Verarbeitung enthält Art 32, die sowohl vom für die Verarbeitung Verantwortlichen als auch vom Auftragsverarbeiter zu beachten ist. Art 24 richtet sich hingegen nur an den Verantwortlichen und fordert von diesem allgemein die Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um die Rechtmäßigkeit der Verarbeitung sicherzustellen. Die Verantwortung des Auftragsverarbeiters ist gemäß Art 28 Abs 3 lit c in einer verpflichtend zwischen dem Verantwortlichen und dem Auftragsverarbeiter abzuschließenden Vereinbarung festzuhalten. Es besteht also eine doppelte Verantwortlichkeit für die Einhaltung der Informationssicherheit, die durchaus sinnvoll ist, da der für die Verarbeitung Verantwortliche idR kaum in der Lage sein wird, zu prüfen, ob die vom Auftragsverarbeiter implementierten Maßnahmen für die übertragene Verarbeitung ausreichen.[222]

Mit § 6 Abs 3 USPG wird festgehalten, dass der Bundesrechenzentrum GmbH im Rahmen des Once-Only-Systems die Rolle der datenschutzrechtlichen Auftragsverarbeiterin zukommt. Die BRZ GmbH hat im Rahmen ihrer Tätigkeit die datenschutzrechtlichen Pflichten gemäß Art 28 Abs 3 lit a bis h DSGVO wahrzunehmen und darf allenfalls weitere Auftragsverarbeiter in Anspruch nehmen.[223] Die BRZ GmbH hat als Auftragsverarbeiterin die Aufgabe, Maßnahmen zur Sicherstellung eines ordnungsgemäßen Betriebs vorzunehmen. Sollten während der Auftragsverarbeitung

[222] *Pollirer* in *Knyrim*, DatKomm Art 32 DSGVO (Stand 1.5.2022, rdb.at) Rz 19.
[223] § 6 Abs 3 USPG idF BGBl 2021/142 sowie Vorblatt und WFA zur Regierungsvorlage: 944 BlgNR XXVII. GP 3.

durch die zugrundeliegenden Daten Fehler auftreten, hat die BRZ GmbH die Problemanalyse bzw die Wiederherstellung eines verarbeitbaren Zustands über die dafür vorgesehenen betrieblichen Standardprozesse zu veranlassen.[224] Den für die Datenverarbeitung Verantwortlichen trifft insbesondere die Pflicht, Maßnahmen für die Erreichung eines dem Risiko angemessenen Schutzniveaus zu treffen.[225]

## *5.2. Kriterien für die Erreichung eines angemessenen Schutzniveaus*

### *5.2.1. Stand der Technik*

Für die Erreichung eines dem Risiko angemessenen Schutzniveaus fordert Art 32 Abs 1 DSGVO zunächst die Berücksichtigung des „Stands der Technik". Dieser Begriff ist schwer zu definieren, ebenso wie die mit dieser Bezeichnung vergleichbaren Begriffe „allgemein anerkannte Regeln der Technik" und „Stand von Wissenschaft und Technik".[226] Im deutschen Sprachraum hat sich die sog Drei-Stufen-Theorie etabliert: Die „allgemein anerkannten Regeln der Technik" bezeichnen Aufgabenstellungen mit vergleichsweise geringem Gefährdungspotential, die Generalklausel „Stand von Wissenschaft und Technik" umfasst das höchste Anforderungsniveau und die Generalklausel „Stand der Technik" liegt dazwischen und bezieht sich auf Regeln, die nach herrschender Auffassung das Erreichen eines vereinbarten oder vorgegebenen Ziels als gesichert erscheinen lässt.[227] Aufgrund der Formulierung „Stand der Technik" in Art 32 Abs 1 DSGVO kann abgeleitet werden, dass der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter die von ihnen getroffenen organisatorischen und technischen Maßnahmen im Bereich der Informationssicherheit stetig anpassen müssen.[228] Bei der Beurteilung des jeweiligen Stands der Technik hinsichtlich der zu treffenden Maßnahmen hat sich der Verantwortliche jedenfalls auch an europäischen Vorgaben und Empfehlungen zu orientieren.[229]

---

[224] Vorblatt und WFA zur Regierungsvorlage: 944 BlgNR XXVII. GP 3.
[225] Art 32 Abs 1 DSGVO.
[226] *Pollirer* in *Knyrim*, DatKomm Art 32 DSGVO (Stand 1.5.2022, rdb.at) Rz 20.
[227] *Pollirer* in *Knyrim*, DatKomm Art 32 DSGVO (Stand 1.5.2022, rdb.at) Rz 20.
[228] *Pollirer* in *Knyrim*, DatKomm Art 32 DSGVO (Stand 1.5.2022, rdb.at) Rz 20.
[229] *Probst*, Datensicherheit nach der DS-GVO (2019) 51.

### *5.2.2. Implementierungskosten*

Die Berücksichtigung der Implementierungskosten soll bewirken, dass der zeitliche und finanzielle Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht: Je höher das Risiko der Datenverarbeitung eingestuft wird, desto höhere Implementierungskosten sind dem Verpflichteten wirtschaftlich zumutbar.[230]

### *5.2.3. Art, Umfang, Umstände und Zweck der Datenverarbeitung*

Mit dem nächsten Kriterium sollen nach Art 32 Abs 1 DSGVO Art, Umfang, Umstände und Zweck der Datenverarbeitung berücksichtigt werden. Mit „Art" werden einerseits die Datenverarbeitungsvorgänge bezeichnet, also zB das Erheben, Erfassen, Übermitteln, Ordnen, Auslesen oder Offenlegen.[231] Andererseits können unter „Art der Verarbeitung" auch die Kategorien personenbezogener Daten, die Kategorien betroffener Personen oder die verwendete Verarbeitungstechnik erfasst werden.[232] „Umfang" bezieht sich auf die Quantität, wobei die DSGVO diesbezüglich keine Definition trifft. Nach Erwägungsgrund 91 liegen umfangreiche Verarbeitungsvorgänge dann vor, wenn „große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene" verarbeitet werden, die eine große Anzahl von Personen treffen könnten.[233] Die „Umstände" der Datenverarbeitung beziehen sich nicht nur darauf, ob die Datenverarbeitung im eigenen Rechenzentrum oder in einer Cloud-Umgebung betrieben wird, sondern auch, auf welche Art und Weise die personenbezogenen Daten erhoben werden (etwa direkt oder aus öffentlichen Quellen), welche Rechtsgrundlagen für die Datenverarbeitung herangezogen werden sowie welche einzelnen Verarbeitungsschritte durchgeführt werden.[234] Die „Zwecke" der Datenverarbeitung sind ebenso zu berücksichtigen. Diese werden gemäß Art 4 Z 7 iVm Art 5 Abs 1 lit b DSGVO vom Verantwortlichen selbst festgelegt. Der Verantwortliche und der Auftragsverarbeiter müssen genau analysieren, wie hoch der Schutzbedarf für jede einzelne Verarbeitung anzusetzen ist, und aufgrund des Ergebnisses die entsprechenden technischen und organisatorischen Maßnahmen implementieren.[235]

---

[230] *Pollirer* in *Knyrim*, DatKomm Art 32 DSGVO (Stand 1.5.2022, rdb.at) Rz 21.
[231] Vgl Art 4 Z 2 DSGVO; *Probst*, Datensicherheit 36.
[232] *Probst*, Datensicherheit 37.
[233] *Probst*, Datensicherheit 37.
[234] *Pollirer* in *Knyrim*, DatKomm Art 32 DSGVO (Stand 1.5.2022, rdb.at) Rz 24.
[235] *Pollirer* in *Knyrim*, DatKomm Art 32 DSGVO (Stand 1.5.2022, rdb.at) Rz 25.

#### *5.2.4. Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen*

Die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ist sowohl vom für die Verarbeitung Verantwortlichen als auch vom Auftragsverarbeiter zu beachten. Dieses Kriterium vollendet den risikobasierten Ansatz der DSGVO, dh die Ausrichtung der erforderlichen technischen und organisatorischen Maßnahmen auf die mit der Verarbeitung verbundenen Risiken.[236]

### *5.3. Umsetzung der Kriterien nach Art 32 DSGVO*

#### *5.3.1. Aufbau eines Informationssicherheits-Managementsystems*

Zur Umsetzung der Forderungen nach Art 32 DSGVO kann der Aufbau eines Informationssicherheits-Managementsystems (ISMS) und eine Orientierung an den internationalen Vorgaben der ISO/IEC 27000 Normenreihe, insb ISO/IEC 27001 und ISO/IEC 27002 zielführend sein.[237] Das Österreichische Informationssicherheitshandbuch[238] bietet einen guten Überblick zum Thema Informationssicherheit und orientiert sich sowohl am IT-Grundschutz-Kompendium des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) als auch an den Normen ISO/IEC 27001 und ISO/IEC 27002. Die BRZ GmbH besitzt eine ISO 27001-Zertifizierung für die von ihr betriebenen Systeme, womit ein strategischer Aufbau und eine kontinuierliche Verbesserung des Informationssicherheits-Managementsystems ermöglicht wird. [239]

Der Aufbau und Betrieb eines ISMS kann in die Abschnitte Entwicklung, Realisierung und Betrieb eingeteilt werden. Für die Entwicklung ist zunächst die Festlegung der

---

[236] *Pollirer* in *Knyrim*, DatKomm Art 32 DSGVO (Stand 1.5.2022, rdb.at) Rz 26.

[237] *Pollirer* in *Knyrim*, DatKomm Art 32 DSGVO (Stand 1.5.2022, rdb.at) Rz 28. Die ISO/IEC 27000-Reihe ist eine Reihe von Standards zur Informationssicherheit von der Internationalen Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC). Die Norm ISO/IEC 27001 gibt einen Überblick über Informationssicherheits-Managementsysteme, definiert Begriffe und gibt einen Überblick über die ISO/IEC 27000-Reihe. In der Norm ISO/IEC 27001 sind Regelungen zum Aufbau und Betrieb eines Informationssicherheits-Managementsystems enthalten. Die Norm ISO/IEC 27002 konkretisiert die Maßnahmen zum Aufbau und Betrieb eines Informationssicherheits-Managementsystems und die Norm ISO/IEC 27005 behandelt das Risikomanagementsystem für den Bereich der Informationssicherheit. Vgl *Mierowski*, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten – Eine kompakte Praxishilfe zur Maßnahmenauswahl: Prozess ZAWAS (2021) 6.

[238] Österreichisches Informationssicherheitshandbuch (Version 4.3.2 vom 11.11.2022), www.sicherheitshandbuch.gv.at (abgefragt am 01.12.2022).

[239] https://www.brz.gv.at/was-wir-tun/zertifizierungen.html (abgefragt am 01.12.2022).

relevanten Sicherheitsziele und -strategien in Form einer für alle verbindlichen Informationssicherheits-Politik (Information Security Policy), sowie die Ermittlung und Bewertung bestehender Sicherheitsrisiken (Information Security Risk Management) erforderlich. Für die Erstellung eines Sicherheitskonzepts sind sodann geeignete organisatorische, baulich-infrastrukturelle, personelle und technische Sicherheitsmaßnahmen auszuwählen. Für die Umsetzung bedarf es der Schulung und Sensibilisierung der Mitarbeiter:innen. Zudem soll ein Audit-Programm erstellt werden, um im Betrieb Sicherheitsüberprüfungen durchführen zu können. Für den Betrieb ist darüber hinaus die Prüfung und Behandlung von Sicherheitsvorfällen (Information Security Incident Handling) sicherzustellen.[240]

Entsprechend der ISO/IEC 27001 ist Informationssicherheit als kontinuierlicher Verbesserungsprozess zu verstehen, der nach dem sogenannten PDCA-Zyklus (Plan-Do-Check-Act) erfolgt.[241] In der ersten Phase („Plan“) soll der Geltungsbereich des Informationssicherheits-Managementsystems festgelegt, und relevante Sicherheitsziele und -strategien ermittelt werden. In der nächsten Phase („Do“) soll das ISMS umgesetzt und betrieben, also Sicherheitsmaßnahmen realisiert werden. Die Sicherheitsmaßnahmen sollen in der darauffolgenden Phase („Check“) hinsichtlich ihrer Wirksamkeit überwacht und überprüft werden. Die nächste Phase („Act“) verfolgt das Ziel des Instandhaltens und Verbesserns des ISMS, also Reagieren auf erkannte Fehler, Schwachstellen und veränderte Umfeldbedingungen und Beseitigen von Ursachen für Gefährdungen.[242] Dies bedingt in weiterer Folge die erneute Planung, womit wieder die erste Phase („Plan“) eingeleitet wird und sich der Kreislauf schließt.[243]

### *5.3.2. Prozess zur Auswahl angemessener Sicherheitsmaßnahmen (Prozess ZAWAS)*

Mit der Festlegung geeigneter technischer und organisatorischer Maßnahmen sollen die in Art 32 Abs 1 lit b und c DSGVO angeführten Ziele erreicht werden: Das Ziel der Vertraulichkeit bezeichnet den Schutz vor unbefugter Preisgabe von Informationen,[244] Integrität umfasst die Datenintegrität, also eine Korrektheit der Daten, und die

---

[240] *Pollirer* in *Knyrim*, DatKomm Art 32 DSGVO (Stand 1.5.2022, rdb.at) Rz 30.
[241] *Pollirer* in *Knyrim*, Datenschutzrecht[4] Kap 10 (Stand 1.4.2020, rdb.at) Rz 10.14.
[242] Österreichisches Informationssicherheitshandbuch (Version 4.3.2 vom 11.11.2022), https://www.sicherheitshandbuch.gv.at/siha.php#155 (abgefragt am 01.12.2022).
[243] *Pollirer* in *Knyrim*, DatKomm Art 32 DSGVO (Stand 1.5.2022, rdb.at) Rz 31.
[244] *Pollirer* in *Knyrim*, DatKomm Art 32 DSGVO (Stand 1.5.2022, rdb.at) Rz 38.

Systemintegrität, dh die korrekte Funktionsweise des Systems[245] und Verfügbarkeit bezeichnet die Anforderung, dass die Systeme abhängig von den Anforderungen der Nutzer:innen betriebsbereit sein müssen und die Verarbeitung auch korrekt erfolgt.[246] Die Verfügbarkeit wird üblicherweise in einem Service-Level-Agreement als Prozentsatz festgelegt und mit der Formel „Verfügbarkeit = (Gesamtlaufzeit–Gesamtausfallzeit)/Gesamtzeit" berechnet.[247]

In der DSGVO sind zwar, wie bereits dargestellt, zahlreiche Anforderungen an die technischen und organisatorischen Maßnahmen formuliert, allerdings bleibt offen, wie die konkrete Auswahl der Maßnahmen tatsächlich getroffen werden kann.[248] Mit dem Prozess ZAWAS (Prozess zur Auswahl angemessener Sicherheitsmaßnahmen) wird von dem Landesbeauftragten für den Datenschutz Niedersachsen *Stefan Mierowski* in 8 Schritten eine Methode und Handlungsempfehlung erstellt, mit der die Anforderungen der DSGVO zur Ermittlung geeigneter technischer und organisatorischer Maßnahmen umgesetzt werden können.[249]

*1) Verarbeitungstätigkeit beschreiben*

Der erste Schritt des Prozesses zur Auswahl angemessener Sicherheitsmaßnahmen besteht in einer Beschreibung der Verarbeitungstätigkeit sowie der Zwecke der Verarbeitung.[250] Dafür kann das gemäß Art 30 DSGVO zu führende Verarbeitungsverzeichnis herangezogen werden.[251]

*2) Rechtliche Grundlagen prüfen*

Im zweiten Schritt muss die Rechtmäßigkeit der Verarbeitung geprüft werden, wobei neben dem Grundsatz der Rechtmäßigkeit (Art 6 DSGVO) auch der Grundsatz der Zweckbindung (Art 5 Abs 1 lit b DSGVO) und der Grundsatz der Datenminimierung (Art 5 Abs 1 lit c DSVGO) sichergestellt werden müssen ebenso wie die Wahrung der Betroffenenrechte (Art 12 ff DSGVO).[252] Für die Wahrung der Betroffenenrechte ist

---

[245] *Pollirer* in *Knyrim*, DatKomm Art 32 DSGVO (Stand 1.5.2022, rdb.at) Rz 39.
[246] *Pollirer* in *Knyrim*, DatKomm Art 32 DSGVO (Stand 1.5.2022, rdb.at) Rz 40.
[247] *Pollirer* in *Knyrim*, DatKomm Art 32 DSGVO (Stand 1.5.2022, rdb.at) Rz 40.
[248] *Mierowski*, Datenschutz nach DS-GOV und Informationssicherheit gewährleisten 9.
[249] *Pollirer*, DSGVO und Informationssicherheit in Praxishandbuch Datenschutzrecht 294.
[250] *Mierowski*, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten 13.
[251] *Pollirer*, DSGVO und Informationssicherheit in Praxishandbuch Datenschutzrecht 294.
[252] *Mierowski*, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten 15 ff.

frühzeitig zu bestimmen, welche Rechte diesen zustehen und welche Informationen zu erteilen sind.[253] Darüber hinaus ist die Erforderlichkeit einer Datenschutz-Folgenabschätzung (DSFA) zu prüfen.[254]

*3) Strukturanalyse durchführen*

Ausgangspunkt der Strukturanalyse ist die konkrete Verarbeitungstätigkeit mit Betrachtung der zu verarbeitenden personenbezogenen Daten und beteiligten Systeme.[255] Mit der Strukturanalyse sollen die einzelnen Objekte der Verarbeitungstätigkeit dargestellt werden (etwa die Anwendungssoftware und IT-Systeme für die Verarbeitung, die Geräte, auf denen die Anwendungssoftware läuft und die Gebäude, in denen die Systeme betrieben werden).[256]

*4) Risikoanalyse vornehmen*

Die Risikoanalyse erfolgt in vier Schritten: der Risikoidentifizierung, der Einschätzung der Schadensschwere, der Bewertung der Eintrittswahrscheinlichkeit und der Ermittlung des Risikowerts.[257] Der Risikowert ergibt sich aus der Eintrittswahrscheinlichkeit und der Schwere des möglichen Schadens und wird im Sinne eines Ausgangsrisikos bewertet, dh bevor technische und organisatorische Maßnahmen ergriffen werden.[258]

*5) Maßnahmen auswählen*

Der nächste Schritt besteht in der konkreten Auswahl von technischen und organisatorischen Maßnahmen. Neben dem Risikowert sind für die Auswahl der Maßnahmen auch der Stand der Technik und die Implementierungskosten zu berücksichtigen.[259] Die spezifischen Maßnahmen können aus unterschiedlichen Quellen abgeleitet werden.[260]

---

[253] *Mierowski*, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten 16.
[254] *Mierowski*, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten 16 f.
[255] *Mierowski*, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten 19.
[256] *Mierowski*, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten 19 f.
[257] *Pollirer*, DSGVO und Informationssicherheit in Praxishandbuch Datenschutzrecht 295 f.
[258] *Mierowski*, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten 25, 30.
[259] *Mierowski*, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten 31.
[260] Die DSGVO sieht beispielsweise in Art 32 Abs 1 die Verschlüsselung und Pseudonymisierung vor. Weitere zweckdienliche Quellen für technische und organisatorische Maßnahmen sind etwa das BSI IT-Grundschutz-Kompendium, das Standard-Datenschutzmodell (SDM) oder Maßnahmen der ISO/IEC 27001.

*6) Restrisiko bewerten*

Das Restrisiko bezeichnet das durch technische und organisatorische Maßnahmen verminderte Ausgangsrisiko. Konnte das Ausgangsrisiko durch entsprechende Maßnahmen reduziert werden, kann der Prozess fortgesetzt werden. Bestehen noch zu hohe Risiken, sind weitere Maßnahmen auszuwählen, bis eine angemessene Risikoreduzierung erfolgt ist.[261] Teil dieses Schritts ist die Erstellung eines Fazits zur Durchführbarkeit oder Nichtdurchführbarkeit des geplanten Verfahrens aus datenschutzrechtlicher Sicht.[262]

*7) Maßnahmen konsolidieren*

Um zu prüfen, ob ausgewählte Maßnahmen überflüssig sind, sollen diese konsolidiert und auch unter Berücksichtigung des erforderlichen finanziellen und personellen Aufwands überprüft werden.[263]

*8) Maßnahmen realisieren*

Im letzten Schritt des Prozess ZAWAS sollen die Maßnahmen umgesetzt werden. Dies umfasst die Zuweisung von Aufgaben und Verantwortlichkeiten, die Erstellung einer Zeitplanung, die Priorisierung von Aufgaben, die Dokumentation der Umsetzung, das Erstellen eines Testkonzepts und in weiterer Folge die Protokollierung der Testfälle und gegebenenfalls das Nachsteuern von Maßnahmen.[264] Nach der Auswahl der Maßnahmen ist gemäß Art 32 Abs 1 lit d DSGVO ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der ausgewählten Maßnahmen zu etablieren.[265]

### *5.3.3. Sicherheitsmaßnahmen für die Datenverarbeitung durch den RSV*

Ein Austausch von Informationen über die Once-Only-Plattform soll grundsätzlich zertifikatsgeschützt erfolgen.[266] Zertifikate und Mechanismen zur Authentifizierung sollen aus den Umsetzungen im Portalverbund übernommen werden.[267] Aus dem Vorblatt zum USPG geht hervor, dass für den Register- und Systemverbund ein

---

[261] *Mierowski*, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten 35.
[262] *Mierowski*, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten 35.
[263] *Pollirer*, DSGVO und Informationssicherheit in Praxishandbuch Datenschutzrecht 297.
[264] *Mierowski*, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten 36.
[265] *Mierowski*, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten 36.
[266] ErlRV 944 BlgNR XXVII. GP 2.
[267] ErlRV 944 BlgNR XXVII. GP 2.

Sicherheitskonzept erstellt wurde, das ein Informationssicherheits- und Datenschutzkonzept enthält.[268] Darin sind Maßnahmen, technisch-organisatorische Spezifikationen und Kontrollmechanismen enthalten. Zudem wird festgehalten, dass eine Datenschutz-Folgenabschätzung nach Art 35 DSGVO nicht erforderlich sei.[269] Aus einer Stellungnahme des Datenschutzrates geht hervor, dass die Ausführungen zur Datenschutz-Folgenabschätzung im Vorblatt nicht ausreichend sind, da nicht klar hervorgeht, welche Daten über die Once-Only-Plattform übermittelt werden sollen. Entsprechend der sogenannten „Whitelist"[270] ist die Verarbeitung personenbezogener Daten im Rahmen von durch Unions-, Bundes- oder Landesrecht eingerichteten Registern, Evidenzen oder Büchern ausgenommen. (DSFA-A06).[271] Hierfür dürfen jedoch keine personenbezogenen Daten im Sinne von Art 9 und 10 DSGVO verarbeitet werden. Wenngleich dies aus dem USPG bzw den Materialien nicht eindeutig hervorgeht, könnte beispielsweise durch eine Anbindung des Strafregisters eine Verarbeitung von Daten im Sinne von Art 10 DSGVO erfolgen, die von der Ausnahme der Whitelist nicht erfasst ist und daher eine Datenschutz-Folgenabschätzung erforderlich machen könnte.[272]

[268] Vorblatt und WFA zur Regierungsvorlage: 944 BlgNR XXVII. GP 3.
[269] Vorblatt und WFA zur Regierungsvorlage: 944 BlgNR XXVII. GP 3.
[270] Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), BGBl II 2018/108.
[271] Laut DSFA-A06; Vgl dazu auch *Jahnel*, „Whitelist" und „Blacklist" zur Datenschutz-Folgenabschätzung, jusIT 2019/12, 36.
[272] *Thiele/Wagner*, Praxiskommentar zum DSG, A06 Rz 3.

# 6. Zusammenfassung und Ausblick

Der Register- und Systemverbund als Datendrehscheibe steht aufgrund der datenschutzrechtlichen Relevanz im Fokus der Betrachtungen dieser Arbeit. Dennoch wird auch die Entwicklung der Informationsverpflichtungsdatenbank spannend zu beobachten sein, da diese durchaus viele Nutzungspotenziale aufweist. Durch die IVDB und den Überblick über Informationsverpflichtungen können Optimierungspotenziale dargestellt und Maßnahmen abgeleitet werden, um die Informationsverpflichtungen entsprechend zu reduzieren. Der über die Einrichtung der IVDB ermöglichte Überblick über bestehende Informationsverpflichtungen führt allerdings noch nicht zu einer Entlastung der Unternehmen bzw Behörden. Es liegt dann an den zuständigen Ressorts, doppelt bzw mehrfach bestehende Informationsverpflichtungen auch tatsächlich zu beseitigen. Neben der Erhebung bestehender Informationsverpflichtungen ist für die Aktualität der Übersicht ein fortlaufendes Monitoring erforderlich, was durch eine Ausweitung des Formulars zur Eintragung in die IVDB und/oder über eine wiederholbare Erhebung erfolgen könnte. Die Aktualität spielt einerseits bei der Erlassung von neuen IVP eine Rolle, da somit gemäß § 7 USPG bei neuen rechtsetzenden Maßnahmen, die eine IVP enthalten, anlassbezogen abgefragt werden kann, ob eine diesbezügliche IVP bereits besteht. Andererseits könnte durch ein fortlaufendes Monitoring, etwa auf Basis periodisch durchgeführter Erhebungen, ein Gesamtüberblick geschaffen werden, was die Transparenz über bestehende Informationsverpflichtungen erhöht.

Für einen rechtmäßigen Datenaustausch zwischen Registern müsste das Ziel die Schaffung von registerübergreifenden legistischen Grundlagen sein. Eine gesetzliche Grundlage für den Datenaustausch ist für den Erlaubnistatbestand nach Art 6 Abs 1 lit e DSGVO Voraussetzung und erscheint aufgrund der Vielzahl von Anwendungsfällen, für die der RSV eingesetzt werden soll, am zweckmäßigsten. Die Alternative der Einwilligung bedürfe einer Betrachtung der Umstände des Einzelfalls und ist daher für eine breite Anwendung kaum bzw nur schwer praxistauglich. Mit der Schaffung einer gesetzlichen Grundlage könnten Behörden nicht nur berechtigt, sondern auch verpflichtet werden, einer anderen Behörde – unter Vorliegen der jeweiligen Berechtigungen – die Daten zu übermitteln.

Für die Einhaltung der Transparenzanforderungen und Sicherstellung der Betroffenenrechte ist einerseits dafür zu sorgen, dass die Daten entsprechend protokolliert

und Auskünfte erteilt werden können und für die Betroffenen klar ist, an wen sie sich zur Ausübung ihrer Rechte wenden können.

Bereits getroffene Maßnahmen für die Sicherheit der Datenverarbeitung können mit einer Orientierung am Prozess ZAWAS systematisch überprüft und gegebenenfalls ergänzt werden. Dem PDCA-Zyklus folgend sollte eine stetige Anpassung der technischen und organisatorischen Maßnahmen durchgeführt werden. Vor allem da die datenschutzrechtliche Verantwortlichkeit bei den abfragenden und auskunftserteilenden Behörden und damit bei mehreren Stellen liegen soll, kann es hilfreich sein, den Prozess ZAWAS als Methode für die Auswahl der entsprechenden Maßnahmen heranzuziehen und somit einen einheitlichen Auswahlprozess für die technischen und organisatorischen Maßnahmen zu etablieren.

Die Eckpunkte für die Errichtung der Once-Only-Plattform sind bereits definiert, für die Umsetzung bedarf es noch einiger Schritte und der Klärung offener Fragestellungen. Mit der Once-Only-Plattform soll eine E-Government-Infrastruktur geschaffen werden, die von den Ressorts, Ländern und Gemeinden genutzt werden kann.[273] Sollen beispielsweise Behörden der Länder auf Bundesregister zugreifen können, bräuchte es für die Zulässigkeit der Übermittlung von personenbezogenen Daten eine bundesgesetzliche Regelung mit einer entsprechenden Öffnungsklausel. Nach der technischen Anbindung der in Österreich verfügbaren Register an den RSV soll in weiterer Folge auch dafür gesorgt werden, dass der RSV entsprechend der mit der Once-Only-Plattform verfolgten Ziele auch für den grenzüberschreitenden Datenaustausch eingesetzt werden kann.

[273] Aus dem Ministerratsvortrag, BMDW 2020-0.644.727

# 7. Abstract

Bei der Datenverarbeitung durch Verwaltungsbehörden sollen gemäß dem Grundsatz „Once Only" zuerst alle zur Verfügung stehenden Daten genutzt werden, bevor sie von Bürger:innen und Unternehmen erneut abgefragt werden. Für die Umsetzung des Once-Only-Prinzips soll in Österreich unter anderem mit § 6 USPG eine „Once-Only-Plattform" eingerichtet werden. Dabei handelt es sich um eine Infrastruktur bestehend aus einem „Register- und Systemverbund" zum behördenübergreifenden Datenaustausch sowie einer „Informationsverpflichtungsdatenbank", die nicht personenbezogene Beschreibungen zu Informationsverpflichtungen für Bürger:innen oder Unternehmen enthält und der Erfassung und Administration von Informationsverpflichtungen dient.

Mit dem Register- und Systemverbund soll die Kommunikation zwischen einzelnen Datenbanken und Registern technisch ermöglicht werden. Da über den RSV personenbezogene Daten übermittelt werden sollen, stellen sich für die Umsetzung und Nutzung des RSV zahlreiche datenschutzrechtliche Fragestellungen. Als Rechtsgrundlage für die Datenübermittlung kommt insbesondere Art 6 Abs 1 lit e DSGVO in Frage. Voraussetzung hierfür ist, dass eine spezifische gesetzliche Grundlage geschaffen wird. Darüber hinaus sind Vorkehrungen zu treffen, etwa eine entsprechende Protokollierung des Datenaustauschs, um dem Auskunftsrecht von Betroffenen nachkommen zu können. Für eine sichere Datenverarbeitung ist die Auswahl geeigneter technischer und organisatorischer Maßnahmen erforderlich, wofür das Vorgehensmodell nach dem Prozess ZAWAS herangezogen werden kann.

# 8. Literaturverzeichnis

*Bergauer/Jahnel* (Hrsg), DSGVO und DSG – Das neue Datenschutzrecht[3] (2018)

*Böllhoff/Botta*: Das datenschutzrechtliche Verantwortlichkeitsprinzip als Herausforderung für die Verwaltungsdigitalisierung, NVwZ 2021, 425 ff

*Braun Binder*, Künstliche Intelligenz und automatisierte Entscheidungen in der öffentlichen Verwaltung, SJZ/RSJ 15/2019

*Döring/Noack*, Standardisierter Datenaustausch in *Klenk/Nullmeier/Wewer*, Handbuch Digitalisierung in Staat und Verwaltung (2020)

*Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung in *Raschauer*, Forschungen aus Staat und Recht 174 (2014)

*Feiler/Forgó*, EU-DSGVO Kurzkommentar (2017)

*Guckelberger*, Öffentliche Verwaltung im Zeitalter der Digitalisierung (Nomos 2019)

*Heberlein* in *Ehmann/Selmayr* (Hrsg), DS-GVO[2] (2018)

*Heine/Wessel*, E-Government und Datensouveränität – Einblicke und Lösungsansätze, HMD 2021 58, 1081-1091

*Jahnel*, „Whitelist" und „Blacklist" zur Datenschutz-Folgenabschätzung, jusIT 2019/12, 36

*Jahnel*, Kommentar zur Datenschutz-Grundverordnung (Stand 1.12.2020, rdb.at)

*Jahnel*, Verfassungsrechtliche Fragen der elektronischen Gesundheitsakte in FS Stolzlechner 2014, 309

*Jahnel/Mader/Staudegger* (Hrsg), IT-Recht[4] (2020)

*Jahnel/Pallwein-Prettner*, Datenschutzrecht[3] (2021)

*Knyrim* (Hrsg), Praxishandbuch Datenschutzrecht[4] (2020)

*Knyrim*, DatKomm - Praxiskommentar zum Datenschutzrecht (rdb.at)

*Krimmer/Margraf*, Empfehlungen zur digitalen Transformation der Verwaltung Deutschlands in Bertelsmann Stiftung (Hrsg), Digitale Transformation der Verwaltung 2017

*Kühling/Buchne*r (Hrsg), DS-GVO – BDSG[2] (2018)

*Lachmayer*, Die DSGVO im öffentlichen Bereich – Europarechtliche Vorgaben im öffentlichen Bereich, ÖJZ 2018/03

*Lehner/Lachmayer*, Datenschutz im Verfassungsrecht in *Bauer/Reimer* (Hrsg), Handbuch Datenschutzrecht (2009)

*Lühr/Jabkowski/Smentek*, Handbuch Digitale Verwaltung (2019)

*Martini/Wenzel*, „Once only" versus „only once": Das Prinzip einmaliger Erfassung zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit, DVBl 2017, 749-758

*Mierowski*, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten – Eine kompakte Praxishilfe zur Maßnahmenauswahl: Prozess ZAWAS (2021)

*Mierowski*, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten (2021)

*Mohabbat Kar/Thapa/Hunt/Parycek*, Recht Digital: Maschinenverständlich und automatisierbar – Impuls zur digitalen Vollzugstauglichkeit von Gesetzen, Kompetenzzentrum Öffentliche IT 2019

*Parycek* in *Mayrhofer/Parycek*, Digitalisierung des Rechts – Herausforderungen und Voraussetzungen, 21. ÖJT Band IV/1 (2022)

*Parycek/Huber/Hunt/Novak/Thapa*, Analyse der rechtlich-technischen Gesamtarchitektur des Entwurfs des Registermodernisierungsgesetzes, Kompetenzzentrum Öffentliche IT 2021

*Peuker*, Registermodernisierung und Datenschutz, NVwZ 2021, 1167

*Probst*, Datensicherheit nach der DS-GVO (2019)

*Raschauer*, Allgemeines Verwaltungsrecht[6] (2021)

*Reimer*, Verwaltungsdatenschutzrecht – Das neue Recht für die behördliche Praxis (2019)

*Schafferer/Horn/Schönbauer*, The Austrian Approach Concerning the European Data Retention Directive's Translation into National Law and its Technical Implementation, in Proceedings of the 12th European Conference on e-Government (ECEG 2012)

*Stember* et al (Hrsg), Handbuch E-Government (2019)

*Stocksmeier*, Potenziale der digitalen Transformation für die deutsche Verwaltung in Bertelsmann Stiftung (Hrsg), Digitale Transformation der Verwaltung (2017)

*Stocksmeier/Wimmer/Führer/Essmeyer*, Once-Only in Deutschland und Europa: Eine Roadmap grenzüberschreitender Vernetzung im Bereich Steuern in *Räckers* et al (Hrsg),

Digitalisierung von Staat und Verwaltung, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2019

*Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz[2] (DSG) (2022)

*Veil*, Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis, NJW 2018, 3337

*Von Lucke*, Hochleistungsportale für die öffentliche Verwaltung (2008)

*Zankl* (Hrsg), Rechtshandbuch der Digitalisierung (2021)