Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung

Leitfaden

Zusammengestellt von Dr. Matthias Schmidl

(überarbeitet von Mag. Marek Gerhalter, LL.M.)

Stand: September 2022

Inhalt

Vorwort

Der vorliegende Leitfaden stellt eine zusammenfassende Information über die Datenschutz-Grundverordnung (DSGVO) dar, die die Arbeit mit der DSGVO erleichtern und Hilfestellung zu bestimmten Fragen bieten soll.

Es handelt sich **um keine abschließende Information**. Eine Beratung durch spezialisierte Einrichtungen oder eine anwaltliche Beratung kann durch den Leitfaden nicht ersetzt werden.

Der Leitfaden stellt **keine verbindliche Information** dar, die die Datenschutzbehörde in allfälligen Verfahren binden könnte, sondern spiegelt den Wissens- und Erfahrungsstand der Mitarbeiter und Mitarbeiterinnen zum derzeitigen Zeitpunkt wider.

Der Leitfaden wird regelmäßig einer Evaluierung und Aktualisierung unterzogen, um Neuerungen (v.a. auf europäischer Ebene) einbeziehen zu können.

In die vorliegende Aktualisierung wurden v.a. folgende Neuerungen einbezogen:

- neue Leitlinien und Empfehlungen des Europäischen Datenschutzausschusses
- neue Rechtsprechung des Europäischen Gerichtshofes und rezente Vorlagen zur Vorabentscheidung

Einleitung

Die DSGVO (vollständiger Titel: *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG*) wurde am 04.05.2016 im ABl. Nr. L119 S. 1 kundgemacht, trat am 20. Tag nach ihrer Veröffentlichung in Kraft und gilt seit dem 25.05.2018.

Sie hebt die Datenschutz-Richtlinie 95/46/EG (DSRL) auf und bildet seit 25. Mai 2018 das Rückgrat des allgemeinen Datenschutzes der EU.

Die Verordnung ist unmittelbar anwendbar und bedürfte grundsätzlich keines weiteren innerstaatlichen Umsetzungsaktes.

Die DSGVO enthält zahlreiche „Öffnungsklauseln“, die den nationalen Gesetzgeber verpflichten und/oder berechtigen, bestimmte Angelegenheiten gesetzlich näher zu regeln.

Es gibt daher neben der DSGVO in Österreich weiterhin ein nationales Datenschutzgesetz (siehe dazu näher Punkt 11 des Leitfadens).

Zielsetzungen der DSGVO sind

- ein einheitlicher Rechtsschutz für alle Betroffenen in der EU
- einheitliche Regeln für die Datenverarbeitung innerhalb der EU
- die Gewährleistung eines starken und einheitlichen Vollzuges

Die datenschutzrechtliche Terminologie ist in bestimmten Bereichen neu.

So wird bspw. der bisherige Auftraggeber zum „Verantwortlichen“ und der Dienstleister zum „Auftragsverarbeiter“ (wobei die Begriffe nicht immer deckungsgleich sind).

Im Folgenden werden einige wesentliche Aspekte beleuchtet.

1) Struktur der DSGVO

Die DSGVO umfasst 173 Erwägungsgründe und 99 Artikel.

Sie gliedert sich in 11 Kapitel:

- Kapitel I: Allgemeine Bestimmungen (Art. 1 bis 4)
- Kapitel II: Grundsätze (Art. 5 bis 11)
- Kapitel III: Rechte der betroffenen Person (Art. 12 bis 23)
- Kapitel IV: Verantwortlicher und Auftragsverarbeiter (Art. 24 bis 43)
- Kapitel V: Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen (Art. 44 bis 50)
- Kapitel VI: Unabhängige Aufsichtsbehörden (Art. 51 bis 59)
- Kapitel VII: Zusammenarbeit und Kohärenz (Art. 60 bis 76)
- Kapitel VIII: Rechtsbehelfe, Haftung und Sanktionen (Art. 77 bis 84)
- Kapitel IX: Vorschriften für besondere Verarbeitungssituationen (Art. 85 bis 91)
- Kapitel X: Delegierte Rechtsakte und Durchführungsrechtsakte (Art. 92 bis 93)
- Kapitel XI: Schlussbestimmungen (Art. 94 bis 99)

2) Kapitel I

Sachlicher Anwendungsbereich (Art. 2):

Die DSGVO findet Anwendung auf die **ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten** sowie für die **nichtautomatisierte Verarbeitung von personenbezogenen Daten**, die in einem **Dateisystem**[1] gespeichert sind oder gespeichert werden sollen.

Auf folgende Bereiche findet die DSGVO **keine** Anwendung:

- Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen
- Tätigkeiten im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik
- Datenverwendung im Rahmen ausschließlich persönlicher oder familiärer Tätigkeiten
- Tätigkeiten der zuständigen Behörden zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit[2]

Räumlicher Anwendungsbereich (Art. 3)[3]:

Wie bereits die Datenschutz-Richtlinie 95/46/EG (DSRL) knüpft die DSGVO primär an die Datenverwendung im Rahmen einer **Niederlassung** eines Verantwortlichen oder eines

[1] Zum Begriff eines „Dateisystems“ siehe auch das Urteil des EuGH vom 10.07.2018, C-25/17.
[2] Für diese Bereiche gilt die DSRL-PJ; die Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (Datenschutzrichtlinie-Polizei Justiz – DSRL-PJ) wurde am 04.05.2016 im Amtsblatt Nr. L119 S. 89 kundgemacht und trat am Tag nach ihrer Kundmachung in Kraft. Die nationale Umsetzung der DSRL-PJ erfolgt im Wesentlichen durch die Bestimmungen des 3. Hauptstückes im DSG.
[3] Siehe dazu die Leitlinien 3/2018 des EDSA zum räumlichen Anwendungsbereich, abrufbar in Deutsch unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_de.pdf.

Auftragsverarbeiters an[4]; liegt diese **Niederlassung im Unionsgebiet**, ist die DSGVO anwendbar.

Nach Art. 3 Abs. 2 findet die DSGVO auch Anwendung, wenn die Datenverarbeitung durch einen **nicht im Unionsgebiet niedergelassenen** Verantwortlichen oder Auftragsverarbeiter erfolgt und die Datenverarbeitung im Zusammenhang damit steht

- betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten (unabhängig von der Zahlung) oder
- das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

Die DSGVO findet auch dann Anwendung, wenn der Verantwortliche oder Auftragsverarbeiter zwar nicht im Unionsgebiet niedergelassen ist, jedoch an einem Ort, der aufgrund des Völkerrechts dem Recht eines Mitgliedstaats unterliegt.

Begriffsbestimmungen (Art. 4):

Die Begriffsbestimmungen der DSGVO (Art. 4) übernehmen vielfach die Begriffsbestimmungen der DSRL, enthalten aber auch neue Begriffe, wie bspw.

- Profiling (Art. 4 Z 4)
- Pseudonymisierung (Art. 4 Z 5)
- Verletzung des Schutzes personenbezogener Daten (Art. 4 Z 12; Data Breach)
- genetische und biometrische Daten sowie Gesundheitsdaten (Art. 4 Z 13 bis 15)
- Hauptniederlassung (Art. 4 Z 16)
- Vertreter, Unternehmen und Unternehmensgruppe (Art. 4 Z 17 bis 19)
- Aufsichtsbehörde und betroffene Aufsichtsbehörde (Art. 4 Z 21 und 22)
- grenzüberschreitende Verarbeitung (Art. 4 Z 23)
- maßgeblicher und begründeter Einspruch (Art. 4 Z 24)

[4] Vgl. zum Begriff der Niederlassung die Urteile des EuGH vom 01.10.2015, C-230/14, Weltimmo, und vom 28.07.2016, C-191/15, VKI; zum Begriff „im Rahmen der Tätigkeit einer Niederlassung“ vgl. das Urteil des EuGH vom 13.05.2014, C-131/12, Google.

- Dienst der Informationsgesellschaft (Art. 4 Z 25)
- internationale Organisation (Art. 4 Z 26)

3) Kapitel II

Die Grundsätze der Datenverarbeitung sind weitgehend ident mit jenen der DSRL.

Art. 6 – Rechtmäßigkeit der Verarbeitung – knüpft inhaltlich an Art. 7 der DSRL an. Demnach bleibt das Konzept aufrecht, dass die Verarbeitung von Daten unzulässig ist, außer es liegt ein Rechtfertigungsgrund vor (Verbot mit Ausnahmen).

Aufbauend auf die Judikatur des EuGH zu Art. 7 der DSRL[5] ist davon auszugehen, dass auch Art. 6 eine **abschließende Aufzählung zulässiger Eingriffe** enthält und die Mitgliedstaaten keine zusätzlichen Gründe für Eingriffe normieren können.

Der Zweckbindungsgrundsatz nach Art. 5 Abs. 1 lit. b wird durch Art. 6 Abs. 4 modifiziert. Demnach ist unter engen Voraussetzungen die Verwendung von Daten auch zu anderen Zwecken als jenen, für welche sie ursprünglich erhoben wurden, zulässig.[6]

Art. 7 legt die Bedingungen für die Einwilligung[7][8] fest (und zwar detaillierter als es bisher die DSRL tat)[9], Art. 8 nimmt ausdrücklich Bezug auf die Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft; damit wird dem Umstand der fortschreitenden Digitalisierung und der Nutzung sozialer Netzwerke auch durch Minderjährige Rechnung getragen.

---

[5] Vgl. dazu zuletzt das Urteil vom 19.10.2016, C-582/14, Breyer.

[6] Dieser Ansatz wurde im Zuge des Gesetzgebungsprozesses von Österreich kritisch gesehen; vgl. dazu *Fercher/Riedl*, DSGVO: Entstehungsgeschichte und Problemstellungen aus österreichischer Sicht in *Knyrim* (Hrsg.), Datenschutz-Grundverordnung [2016] S. 22 ff; vgl. dazu weiter *Kotschy*, Zweckbindungsprinzip und zulässige Weiterverarbeitung, Debattenbeitrag zur Datenschutz-Grundverordnung (Version 23.06.2016), abrufbar unter http://bim.lbg.ac.at/de/themen/datenschutz-grundverordnung.

[7] Siehe dazu näher die Leitlinien 5/2020 des EDSA zur Einwilligung, abrufbar in Englisch unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.

[8] Vgl. dazu auch den Bescheid der Datenschutzbehörde vom 31.07.2018, GZ DSB-D213.642/0002-DSB/2018.

[9] Vgl. dazu *Dürager/Kotschy*, Neuerungen zur Zustimmung (Einwilligung) nach der DS-GVO, Debattenbeitrag zur Datenschutz-Grundverordnung (Version 02.12.2016), sowie *Dürager/Kotschy*, Neuerungen zur Zustimmung: Besteht nach der DS-GVO ein generelles Koppelungsverbot?, Debattenbeitrag zur Datenschutz-Grundverordnung (Version 09.01.2017), beide abrufbar unter http://bim.lbg.ac.at/de/themen/datenschutz-grundverordnung.

Art. 9 enthält – ebenso wie bereits Art. 8 der DSRL – die Voraussetzungen für die Verwendung sensibler Daten (= besondere Kategorien personenbezogener Daten). Zu beachten ist, dass auch Informationen, welche indirekt Rückschlüsse auf die in Art. 9 DSGVO angeführten Eigenschaften einer betroffenen Person ermöglichen, als „sensible" personenbezogene Daten zu qualifizieren sind.[10]

Art. 10 legt fest, unter welchen Voraussetzungen personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten verarbeitet werden dürfen.[11] Der EuGH hat zum unionsrechtlich autonom auszulegenden Begriff der „Straftat" ausgesprochen, dass darunter nicht nur Straftaten im Sinne des Strafrechts (d.h. Zuwiderhandlungen, die im innerstaatlichen Recht als „strafrechtlich" eingestuft werden), sondern unter bestimmten Voraussetzungen auch Verwaltungsübertretungen (wie bspw. Übertretungen von Straßenverkehrsvorschriften) verstanden werden können.[12] Die Beurteilung ist anhand der vom EuGH aufgestellten Kriterien im Einzelfall vorzunehmen. Werden Daten über eine Verwaltungsübertretung als Daten iSd. Art. 10 DSGVO qualifiziert und erfolgt ihre Verarbeitung durch zuständige Behörden zur Aufklärung und Verfolgung von Straftaten, so wäre diesbezüglich der Anwendungsbereich der DSRL-PJ bzw. des 3. Hauptstückes des DSG eröffnet.

Art. 11 normiert abschließend den nicht unwesentlichen Umstand, dass Daten nicht bloß deshalb aufbewahrt werden müssen, um eine Person identifizieren zu können (bspw. um einem Auskunftsbegehren nachkommen zu können).

---

[10] Vgl. das Urteil des EuGH vom 1. August 2022, C-184/20, Rz. 123 ff.
[11] Diese „Strafdaten" gelten per definitionem nicht als sensible Daten. Sie unterlagen in Österreich aber bereits bisher einem speziellen Schutz; vgl. dazu § 8 Abs. 4 DSG 2000 sowie die Rechtsprechung des VwGH dazu (Erkenntnis vom 22.10.2012, Zl. 2009/03/0162).
[12] Urteil des EuGH vom 22. Juni 2021, C-439/19, Rz. 87 ff.

4) Kapitel III

Kapitel III regelt jene **Datenschutzrechte**, die einer betroffenen Person zukommen.

Die Betroffenenrechte, d.h. jene Rechte, die Betroffene aus der DSGVO bzw. dem DSG ableiten können, ergeben sich

- aus der Verfassungsbestimmung des § 1 DSG bzw.
- aus Art. 12 bis 22 DSGVO

Soweit es die DSGVO betrifft, ist **Art. 12 DSGVO** als **Horizontalbestimmung** für die Ausübung aller Betroffenenrechte heranzuziehen, weil dieser die Modalitäten der Ausübung festlegt.

Demnach gilt Folgendes:

Der Verantwortliche hat die Ausübung der Betroffenenrechte möglichst zu erleichtern, indem er

- Informationen und Mitteilungen in leicht verständlicher Sprache (v.a. für Kinder) zur Verfügung stellt;
- Informationen und Mitteilungen schriftlich, ggf. elektronisch, zur Verfügung stellt;
- Informationen und Mitteilungen auch mündlich zur Verfügung stellt, sofern die Identität der betroffenen Person in anderer Weise nachgewiesen wurde.

Maßnahmen, die aufgrund eines Auskunfts-, Richtigstellungs- oder Löschungsbegehrens, eines Widerspruchs oder eines Antrags auf Einschränkung der Verarbeitung oder auf Datenübertragbarkeit ergehen, müssen dem Betroffenen unverzüglich und jedenfalls **innerhalb eines Monats** mitgeteilt werden. Diese Frist kann in begründeten Fällen **um zwei weitere Monate erstreckt** werden, die betroffene Person ist vom Verantwortlichen innerhalb des ersten Monats unter Angabe der Gründe über die Fristerstreckung zu unterrichten. Wird ein Antrag einer betroffenen Person elektronisch gestellt, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nicht anderes angibt.

Wird dem Antrag eines Betroffenen nicht entsprochen, so ist der Betroffene **innerhalb eines Monats** unter Angabe der maßgeblichen Gründe schriftlich darüber zu unterrichten. Er ist auf die Möglichkeit, bei der Aufsichtsbehörde eine Beschwerde einzureichen, hinzuweisen.

Die Ausübung der Betroffenenrechte ist für die betroffene Person **kostenlos**. Bei **offenkundig unbegründeten** oder – insbesondere im Fall von häufiger Wiederholung – **exzessiven Anträgen** einer betroffenen Person kann der Verantwortliche

- entweder ein **angemessenes Entgelt** verlangen (unter Berücksichtigung der Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme) oder
- sich **weigern**, aufgrund des Antrages **tätig zu werden**.[13]

Die Nachweispflicht für das Vorliegen dieser Gründe trifft den Verantwortlichen.[14]

Hat der Verantwortliche **begründete Zweifel an der Identität** der betroffenen Person, kann er zusätzliche Informationen zur Bestätigung der Identität von der betroffenen Person anfordern. Die Identität des Auskunftswerbers wird regelmäßig in Form einer Kopie eines amtlichen Lichtbildausweises[15] nachgewiesen. Möglich ist aber auch der Nachweis in Form einer qualifizierten elektronischen Signatur.[16] Wird ein Auskunftsbegehren durch einen Rechtsanwalt für einen Mandanten eingebracht, ist dem Auskunftsbegehren die Vollmacht des Mandanten anzuschließen. Dies gilt nicht, wenn ein Rechtsanwalt gegenüber inländischen Behörden und Gerichten einschreitet, weil hier die bloße Berufung auf die erteilte Vollmacht ausreicht (§ 8 RAO).[17]

---

[13] Siehe dazu den Bescheid der Datenschutzbehörde vom 06.07.2018, GZ DSB-D123.051/0002-DSB/2018 (nicht rechtskräftig) oder auch das Erkenntnis des BVwG vom 02.03.2020, W214 2224106-1.

[14] Eine ähnliche Regelung sieht Art. 57 Abs. 4 DSGVO für das Beschwerdeverfahren vor der Datenschutzbehörde vor; vgl. hierzu etwa die Erkenntnisse des BVwG vom 29. April 2020, W274 2228071-1 und vom 3. November 2020, W214 2233563-1

[15] Der VwGH hat zum Nachweis der Identität ausgesprochen, dass diese in Form einer öffentlichen Urkunde nachgewiesen werden kann. Nach der Rsp des VwGH reicht aber bspw. die Vorlage einer Meldebestätigung nicht aus; Erkenntnis vom 04.07.2016, Zl. Ra 2016/04/0014.

[16] Art. 3 Z 12 eIDAS-VO (Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. Nr. L 257 vom 28.08.2014 S. 73, in der Fassung der Berichtigung ABl. Nr. L 257 vom 29.01.2015 S. 19); siehe auch das Erkenntnis des BVwG vom 27.05.2020, GZ W214 2228346-1.

[17] Siehe dazu nochmals das Erkenntnis des VwGH vom 04.07.2016.

Liegen hingegen genügend Anhaltspunkte vor, um die Identität des Auskunftswerbers zweifelsfrei zu bestätigen, darf der Verantwortliche keine weiteren Nachweise zur Identität (z.B. Lichtbildausweis) verlangen.[18]

Die Art. 13 und 14 – wie bereits schon Art. 10 und 11 der DSRL – legen die **Informationspflichten**[19] gegenüber Betroffenen fest. Demnach sind Betroffene darüber zu informieren, von wem, auf welcher Rechtsgrundlage und zu welchem Zweck ihre Daten verarbeitet und an wen sie übermittelt werden. Der EuGH misst diesen Informationspflichten großen Wert bei, weil diese die Voraussetzungen dafür schaffen, dass Betroffene ihre Rechte (Auskunft, Richtigstellung, Löschung, Widerspruch) ausüben können.[20]

Neben den schon bisher bekannten Rechten auf **Auskunft** (Art. 15), **Berichtigung** (Art. 16), **Löschung** (Art. 17; ausgeweitet zum „Recht auf Vergessenwerden“) werden neue Rechte eingeführt.

So sieht Art. 18 das **Recht auf Einschränkung der Verarbeitung** vor, wonach ein Betroffener vom Verantwortlichen die Einschränkung der Verarbeitung verlangen kann, wenn bspw. die Richtigkeit der Daten bestritten wird.

Art. 20 räumt einem Betroffenen das **Recht auf Datenübertragbarkeit** ein[21]. Damit soll sichergestellt werden, dass die von einem Betroffenen zur Verfügung gestellten personenbezogene Daten, die bei einem (privaten) Anbieter in einer bestimmten technischen Umgebung gespeichert werden, bei einem Anbieterwechsel in bestimmten Fällen[22] ohne technische Barrieren für die Betroffenen in eine neue technische Umgebung übertragen werden können.

---

[18] Siehe dazu den Bescheid der Datenschutzbehörde vom 31.07.2019, GZ DSB-D123.901/0002-DSB/2019.

[19] Siehe dazu näher die Leitlinien der Art. 29-Gruppe zur Transparenz, WP 260, abrufbar in Deutsch unter https://www.dsb.gv.at/dam/jcr:17cb6862-7bc0-4039-8c47-97bc09602214/Leitlinien%20f%C3%BCr%20Transparenz%20gem%C3%A4%C3%9F%20der%20Verordnung%202016-679.pdf. Diese Leitlinien wurden vom EDSA ausdrücklich übernommen: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

[20] Vgl. dazu das Urteil des EuGH vom 01.10.2015, C-201/14, Smaranda Bara u.a.

[21] Vgl. dazu WP 242 rev. 01, Leitlinie der Art. 29-Gruppe vom 13.12.2016 zur Datenübertragbarkeit, abrufbar unter https://www.dsb.gv.at/dam/jcr:01ff1101-f5bf-494b-a7d2-64392db10b78/Leitlinien%20zum%20Recht%20auf%20Daten%C3%BCbertragbarkeit,%20pdf.pdf. Diese Leitlinien wurden vom EDSA ausdrücklich übernommen: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

[22] Wesentlich ist u.a., dass die Datenverarbeitung auf einer Einwilligung beruht oder zur Vertragserfüllung vorgenommen wird und (kumulativ) mithilfe automatisierter Verfahren erfolgt.

Das Recht auf **Widerspruch** (Art. 21)[23] unterscheidet sich deutlich vom Widerspruchsrecht gemäß § 28 DSG 2000, und hat besondere Wirkung gegen Direktwerbung (Art. 21 Abs. 3).

Ebenfalls als Horizontalbestimmung regelt Art. 23 DSGVO, unter welchen Voraussetzungen Betroffenenrechte eingeschränkt werden können.[24]

Dies kann erforderlich sein aus Gründen

a) der nationalen Sicherheit;

b) der Landesverteidigung;

c) der öffentlichen Sicherheit;

d) der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;

e) des Schutzes sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit;

f) des Schutzes der Unabhängigkeit der Justiz und des Schutzes von Gerichtsverfahren;

g) der Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe;

h) der Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt verbunden sind;

i) des Schutzes der betroffenen Person oder der Rechte und Freiheiten anderer Personen;

j) der Durchsetzung zivilrechtlicher Ansprüche.

---

[23] Das Recht auf Widerspruch findet auch auf die Datenverwendung durch Behörden Anwendung; vgl. dazu das Urteil des EuGH vom 09.03.2017, C-398/15, Manni.

[24] Vgl. dazu EDSA, Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 1.0 vom 13. Oktober 2021, abrufbar in englischer Sprache unter https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf.

In Österreich wurde davon v.a. in den Materien-Datenschutz-Anpassungsgesetzen[25] Gebrauch gemacht.

Nach der Rsp des EuGH unterliegen solche Einschränkungen aber insofern der Kontrolle des EuGH, als auch Einschränkungen, die Mitgliedstaaten vornehmen können, in den Anwendungsbereich des Unionsrechtes fallen.[26]

[25] Vgl. dazu insbesondere das Materien-Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 32/2018, und das 2. Materien-Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 37/2018, wo von Einschränkungen iSd Art. 23 DSGVO Gebrauch gemacht wurde.
[26] Vgl. dazu das Urteil vom 21.12.2016, C-203/15, Tele 2 Sverige AB, und C-698/15, Watson.

5) Kapitel IV

Die DSGVO nimmt stärker als die DSRL und das DSG 2000 Verantwortliche und Auftragsverarbeiter in die Pflicht.

Art. 27 verpflichtet Verantwortliche und Auftragsverarbeiter, die **nicht im Unionsgebiet niedergelassen** sind, einen **Vertreter** in einem Mitgliedstaat zu benennen. Der Vertreter ist zusätzlich zum Verantwortlichen/Auftragsverarbeiter oder an dessen Stelle Anlaufpunkt für Betroffene und Aufsichtsbehörden.[27]

Das DVR-Meldeverfahren und das DVR selbst gibt es nicht mehr (**Entfall der DVR-Meldepflicht**). Stattdessen verpflichtet Art. 30 Verantwortliche und Auftragsverarbeiter ein **Verzeichnis von Verarbeitungstätigkeiten**[28] zu führen, das auf Anfrage der Aufsichtsbehörde vorzulegen ist. Diese Verpflichtung gilt nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn,

- die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen,
- die Verarbeitung erfolgt nicht nur gelegentlich oder
- es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 (sensible Daten) bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10.

Daneben werden Verantwortliche verpflichtet, vor Inbetriebnahme eines neuen Datenverarbeitungssystems, welches voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, eine **Datenschutz-Folgenabschätzung**[29] durchzuführen und ggf. mit der Aufsichtsbehörde im Rahmen eines

---

[27] Zur Verantwortung des Vertreters siehe nochmals die Leitlinien 3/2018 des EDSA zum räumlichen Anwendungsbereich, abrufbar in Deutsch unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_de.pdf, S. 19 ff.

[28] Siehe dazu näher *Horn*, Mögliche Erweiterungen des Verarbeitungsverzeichnisses nach Art. 30 DS-GVO zu einem umfassenden Compliance-Werkzeug, JusIT 5/2017 S. 183 ff.

[29] Vgl. dazu WP 248 rev.01, Leitlinien der Art. 29-Gruppe vom 04.04.2017 zur Datenschutz-Folgenabschätzung, abrufbar unter https://www.dsb.gv.at/dam/jcr:ba295358-cf65-41a6-911d-a88cae94ba20/Leitlinien%20zur%20Datenschutz-Folgenabschaetzung-wp248-rev-01_de.pdf.

Konsultationsverfahrens zusammenzuarbeiten (Art. 35 und 36). Die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung gilt unter bestimmten Voraussetzungen auch für das Gesetzgebungsverfahren selbst, wobei die Frage, inwiefern das Unterlassen einer verpflichtenden Risikofolgenabschätzung die Wirksamkeit einer Norm berührt, derzeit Gegenstand eines Vorabentscheidungsverfahrens vor dem EuGH ist.[30]

Verantwortliche werden verpflichtet, **Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde** zu erstatten (Art. 33) und ggf. **Betroffene** von der Verletzung zu **verständigen** (Art. 34).[31] Für Betreiber öffentlicher Kommunikationsdienste bestehen selbige Meldepflichten gemäß § 164 TKG 2021.[32]

Neu ist auch die verpflichtende **Bestellung eines Datenschutzbeauftragten** in bestimmten Bereichen (Art. 37 bis 39)[33], der seine Aufgaben als Datenschutzbeauftragter weisungsungebunden durchführt und unmittelbar der höchsten Managementebene berichtet. Ein iSd. DSGVO bestellter Datenschutzbeauftragter ist besonders geschützt und darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Mitgliedstaaten können dahingehend auch strengere Regelungen zum Kündigungsschutz von Datenschutzbeauftragten vorsehen, sofern diese die Verwirklichung der Ziele der DSGVO nicht beeinträchtigen.[34]

Folgende Verantwortliche/Auftragsverarbeiter haben zwingend einen Datenschutzbeauftragten zu bestellen:

---

[30] Rs C-61/22.

[31] Siehe EDSA, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, Version 2.0 vom 14. Dezember 2021, abrufbar in englischer Sprache unter https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf .

[32] Bundesgesetz, mit dem ein Telekommunikationsgesetz (Telekommunikationsgesetz 2021 – TKG 2021) erlassen wird, BGBl. I Nr. 190/2021; vgl. im Weiteren auch die Verordnung (EU) Nr. 611/2013, ABl. L 173/2013, S. 2.

[33] Vgl. dazu WP 243 rev. 01, Leitlinie der Art. 29-Gruppe vom 13.12.2016 zum Datenschutzbeauftragten, abrufbar unter https://www.dsb.gv.at/dam/jcr:a279307b-ce48-416e-9c28-5bae42e0038c/Leitlinien_in_Bezug_auf_Datenschutzbeauftragte.pdf.Diese Leitlinien wurden vom EDSA ausdrücklich übernommen: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

[34] Vgl. das Urteil des EuGH vom 22. Juni 2022, C-534/20, Rz. 34 ff; unzulässig wäre bspw. eine nationale Regelung, welche jede durch einen Verantwortlichen oder einen Auftragsverarbeiter ausgesprochene Kündigung eines Datenschutzbeauftragten, der nicht mehr die für die Erfüllung seiner Aufgaben erforderlichen beruflichen Eigenschaften besitzt oder seine Aufgaben nicht im Einklang mit der DSGVO erfüllt, verbietet.

- Behörden und öffentliche Stellen (mit Ausnahme von Gerichten, soweit es nicht die monokratische Justizverwaltung betrifft);
- wenn die Kerntätigkeit die regelmäßige und systematische Überwachung von Personen darstellt;
- wenn die Kerntätigkeit in der umfangreichen Verarbeitung von sensiblen Daten nach Art. 9 und Strafdaten nach Art. 10 besteht.

Zur Frage, ob eine bestimmte Funktion innerhalb der Organisation eines Verantwortlichen/Auftragsverarbeiters mit der Funktion eines Datenschutzbeauftragten vereinbar ist, ist derzeit ein Vorabentscheidungsverfahren vor dem EuGH anhängig.[35]

Die Art. 40 ff bauen das bereits in Art. 27 der DSRL vorgesehene System der **Verhaltensregeln** weiter aus. Demnach können Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, datenschutzrechtliche Verhaltensregeln erstellen und diese bei der Aufsichtsbehörde zur Genehmigung einreichen. Die Überwachung der Einhaltung von genehmigten Verhaltensregeln erfolgt durch eine dafür besonders **geeignete Stelle**, die von der Aufsichtsbehörde zu **akkreditieren** ist.[36]

Die Art. 42 und 43 legen fest, dass Verantwortliche und Auftragsverarbeiter bestimmte Verarbeitungsvorgänge zertifizieren lassen können, um nachzuweisen, dass die Verarbeitung in Übereinstimmung mit der DSGVO erfolgt (Datenschutzsiegel, -prüfzeichen). Die **Zertifizierung** erfolgt entweder durch die Aufsichtsbehörde selbst oder durch Zertifizierungsstellen, die von der Aufsichtsbehörde oder der nationalen Akkreditierungsstelle nach der VO (EG) Nr. 765/2008 hiezu eigens akkreditiert werden.[37] In Österreich erfolgt die Akkreditierung ausschließlich durch die Datenschutzbehörde (§ 21 Abs. 3 DSG).

---

[35] Rs C-453/21.

[36] Nähere Informationen werden unter https://www.dsb.gv.at/aufgaben-taetigkeiten/genehmigung-von-verhaltensregeln.html bereitgestellt.

[37] Vgl. dazu die Leitlinien 1/2018 des EDSA über Zertifizierungen und Zertifizierungskriterien nach Art. 42 und 43 DSGVO, abrufbar in Deutsch unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_de_0.pdf, und die Leitlinien 4/2018 über die Akkreditierung von Zertifizierungsstellen nach Art. 43 DSGVO, abrufbar in Deutsch unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_de.pdf.

Verhaltensregeln und Zertifizierungen können bei Vorliegen bestimmter zusätzlicher Voraussetzungen auch als Instrument zur Übermittlung personenbezogener Daten an Empfänger in Drittländern herangezogen werden (siehe nachfolgendes Kapitel V).

6) Kapitel V

Kapitel V regelt die näheren Voraussetzungen für den **Datenverkehr mit Empfängern in Drittstaaten[38] oder internationalen Organisationen[39]**.

Ein derartiger Datenfluss ist, neben der Einhaltung der allgemeinen Verarbeitungsgrundsätze, nur unter folgenden weiteren Bedingungen zulässig:

- Vorliegen eines Angemessenheitsbeschlusses der Europäischen Kommission (Art. 45)[40]
- Vorliegen geeigneter Garantien (Art. 46). Dazu gehören vor allem von der Europäischen Kommission erlassene Standarddatenschutzklauseln[41], von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. d) und verbindliche interne Datenschutzvorschriften (Binding Corporate Rules, BCRs[42] Art. 47), sowie neue Mechanismen wie Verhaltensregeln[43] (Art. Art. 40) und Zertifizierungen[44] (Art. 42).

[38] Als Drittstaaten gelten in diesem Sinne alle Länder außerhalb der EU bzw. des EWR-Raums.
[39] Darunter sind auf Grundlage eines völkerrechtlichen Vertrages bzw. einer entsprechenden Vereinbarung zweier oder mehrerer Völkerrechtssubjekte errichtete Organisationen zu verstehen, wie z.B. die Vereinten Nationen. Privatrechtliche Organisationen bzw. nichtstaatliche Verbände (NGOs) ohne völkerrechtliches Mandat fallen dagegen nicht unter diesen Begriff.
[40] Eine Liste der derzeit in Geltung stehenden Angemessenheitsbeschlüsse ist unter https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en abrufbar.
[41] Vgl. Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, ABl. L 199/2021, S. 31; Die unter der RL 95/46/EG erlassenen Klauselwerke können nur mehr bis zum 27. Dezember 2022 herangezogen werden.
[42] Vgl. dazu WP 256 und WP 257 der Art. 29 Gruppe, Arbeitsdokumente mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher interner Datenschutzvorschriften, abrufbar in deutscher Sprache unter https://ec.europa.eu/newsroom/article29/items/614109 und https://ec.europa.eu/newsroom/article29/items/614109. Diese wurden vom EDSA übernommen: https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf.
[43] Vgl. dazu EDSA, Guidelines 04/2021 on Codes of Conduct as tools for transfers, Version 2.0 vom 22. Februar 2022, abrufbar in englischer Sprache unter https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf.
[44] Vgl. dazu EDSA, Guidelines 07/2022 on certification as a tool for transfers, Version 1.0 vom 14. Juni 2022, abrufbar in englischer Sprache unter https://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202207_certificationfortransfers_en_1.pdf (diese befinden sich bis zum 30. September in öffentlicher Begutachtung).

Art. 49 sieht Ausnahmen für bestimmte Fälle vor, wobei eine restriktive Anwendung der dort vorgesehenen Ausnahmetatbestände geboten ist.[45]

Die Ratio hinter Kapitel V ist, dass die übermittelten Daten beim Empfänger im Drittstaat bzw. bei der internationalen Organisation einem der Sache nach gleichwertigen Schutzniveau wie in der EU unterliegen sollen. Die meisten Transfers sollen genehmigungsfrei sein.[46]

Hoheitlich tätige Verantwortliche im Bereich der öffentlichen Sicherheit müssen beachten, dass gemäß §§ 58 und 59 DSG **Sonderbestimmungen** für Übermittlungen an Empfänger in Drittländern oder in internationalen Organisationen im Rahmen der Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs bestehen.

Hinweis:

Der EuGH hat in der als „Schrems II“ bekannten Entscheidung vom 16.07.2020, C-311/18, den für einen Großteil der Datenübermittlungen in die USA maßgeblichen „Privacy-Shield-Beschluss“ (Durchführungsbeschluss (EU) 2016/1250 der Europäischen Kommission) für **ungültig** erklärt, da die U.S.-amerikanische Rechtsordnung derzeit kein der Sache nach gleichwertiges Schutzniveau normiert.[47] Seine Entscheidung begründete der EuGH insbesondere mit dem Bestehen von umfangreichen, nicht auf das zwingend erforderliche Maß beschränkten Eingriffs- und Zugriffsbefugnissen von U.S.-amerikanischen Behörden auf

[45] Vgl. dazu die Leitlinien des EDSA 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, abrufbar in Deutsch unter https://www.dsb.gv.at/dam/jcr:db22aec8-5c71-4ae4-9c30-b06d07f79335/Leitlinien2-2018%20zu%20den%20Ausnahmen%20nach%20Artikel49%20der%20Verordnung2016-679.pdf.

[46] Ausnahmen von der Genehmigungsfreiheit bestehen bspw. bei Bestimmungen in Verwaltungsvereinbarungen gemäß Art. 46 Abs. 3 lit. b DSGVO; siehe den Bescheid der DSB vom 16. Mai 2022, GZ 2022-0.296.352.

[47] Die Europäische Kommission und die USA haben dahingehend am 25. März 2022 eine gemeinsame Erklärung zur Schaffung eines neuen transatlantischen Datenschutzabkommens abgegeben, abrufbar in deutscher Sprache unter https://ec.europa.eu/commission/presscorner/detail/de/ip_22_2087; im US-Parlament wird derzeit der Entwurf eines American Data Privacy and Protection Acts diskutiert, mit welchem grundlegende Datenschutzrechte für Verbraucher samt wirksamen Aufsichts- und Durchsetzungsmechanismen verankert werden sollen, abrufbar in englischer Sprache unter https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

personenbezogenen Daten, welche aus dem Unionsgebiet in die USA übermittelt werden, sowie mit unzureichenden Rechtsschutzmöglichkeiten für Betroffene.[48] Gleichzeitig hat er ausgesprochen, dass die Standardvertragsklauseln gemäß dem Beschluss der Europäischen Kommission 2010/87/EU idF des Beschlusses 2016/2297 mit dem Unionsrecht vereinbar sind. In bestimmten Fällen müssen sie aber durch so genannte „Zusatzgarantien" ergänzt werden, d.h. dass Verantwortliche neben der Vereinbarung von Standarddatenschutzklauseln gegebenenfalls zusätzliche Maßnahmen ergreifen müssen, um die Einhaltung eines der Sache nach gleichwertigen Schutzniveaus zu gewährleisten.[49] Diese Überlegungen sind auf die „neuen" Standarddatenschutzklauseln gemäß Durchführungsbeschluss (EU) 2021/914 übertragbar.

Angemessenheitsbeschlüsse: Die Europäische Kommission hat im Jahr 2021 Angemessenheitsbeschlüsse für das Vereinigte Königreich Großbritannien und Nordirland sowie für die Republik Korea (Südkorea) erlassen.

[48] Für ausführliche Informationen hierzu siehe die FAQs des EDSA in Englisch unter https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf.

[49] Siehe dazu im Detail die Empfehlungen 01/2020 des EDSA zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, abrufbar in Deutsch unter https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en; vgl. auch die Zusammenfassung auf der Website der Datenschutzbehörde unter https://www.dsb.gv.at/aufgaben-taetigkeiten/internationaler-datenverkehr.html.

7) Kapitel VI[50]

Es gibt in jedem Mitgliedstaat zumindest eine unabhängige Aufsichtsbehörde. In Österreich hat die **Datenschutzbehörde** diese Funktion.

Die Aufgaben und Befugnisse werden durch die DSGVO erheblich erweitert (Art. 57 und 58).

Art. 58 normiert drei Arten von Befugnissen:

- Untersuchungsbefugnisse (einschließlich des Betretungsrechts bestimmter Räumlichkeiten)
- Abhilfebefugnisse (das sind Befugnisse, die es der Aufsichtsbehörde ermöglichen, ein rechtswidriges Verhalten abzustellen, bspw. durch konkrete Anordnungen oder die Verhängung von Geldbußen iHv bis zu 20 Millionen Euro oder 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres)
- Genehmigungs- und Beratungsbefugnisse.

Gerichte sind gemäß Art. 55 Abs. 3 DSGVO von der Aufsicht durch die Datenschutzbehörde ausgenommen, sofern sie im Rahmen ihrer justiziellen Tätigkeit handeln. In diesem Fall richtet sich der Rechtsschutz vordergründig nach den §§ 83 ff GOG.[51] Im Umkehrschluss unterliegen Organe der Gerichtsbarkeit aber dann der Aufsicht durch die Datenschutzbehörde, wenn sie im Rahmen der monokratischen Justizverwaltung tätig werden.[52] Ob eine justizielle Tätigkeit eines Gerichts vorliegt, ist im Einzelfall zu beurteilen.[53] Der EuGH hat dahingehend ausgesprochen, dass vom Begriff der „justiziellen Tätigkeit“ alle Verarbeitungsvorgänge erfasst sind, die von Gerichten vorgenommen werden, soweit deren

---

[50] Vgl. dazu im Detail *Schmidl*, Aufgaben und Befugnisse der Aufsichtsbehörden sowie Rechtsschutzmöglichkeiten nach der DSGVO, ÖBA 1/17 S. 27 ff; *Flendrovsky*, Die Aufsichtsbehörden, in *Knyrim* (Hrgs.) aaO S. 281 ff.

[51] Aufgrund von BGBl. I Nr. 22/2018 sind die Bestimmungen des GOG auch von den Verwaltungsgerichten, vom VwGH und vom VfGH sinngemäß anzuwenden. Selbiges wurde auch für Landesverwaltungsgerichte vorgesehen, vgl. bspw. § 40a Abs. 2 des NÖ Landesverwaltungsgerichtsgesetzes, LGBl. 0015-0 idgF.

[52] Vgl. dazu näher *Schmidl* in *Gantschacher/Jelinek/Schmidl/Spanberger*, Kommentar zu Datenschutz-Grundverordnung1[2017] Art. 55 Anm. 3; *Nguyen* in *Gola* (Hrsg.), Datenschutz-Grundverordnung [2017] Art. 55 Rz. 13.

[53] Vgl. dazu die Bescheide der Datenschutzbehörde vom 22.01.2019, GZ DSB-D123.848/0001-DSB/2019, und vom 04.02.2019, GZ DSB-D123.937/0001-DSB/2018.

Kontrolle durch eine Aufsichtsbehörde mittelbar oder unmittelbar die Unabhängigkeit der Mitglieder oder der Entscheidungen der Gerichte beeinflussen könnte.[54]

Ob **Organe der Gesetzgebung** (Nationalrat, Bundesrat, Volksanwaltschaft, Rechnungshof) der Aufsicht durch die Datenschutzbehörde unterliegen, ist derzeit Gegenstand eines Vorabentscheidungsverfahrens vor dem EuGH.[55] Zu unterscheiden ist hiervon die grundsätzliche Bindung von Gesetzgebungsorganen an die DSGVO, welche vom EuGH bejaht wurde.[56]

[54] Urteil des EuGH vom 24. März 2022, C-245/20 (X und Z gg. Autoriteit Persoonsgegevens), Rz. 34.
[55] Siehe C-33/22.
[56] Urteil des EuGH vom 9. Juli 2020, C-272/19 (VQ gg. Land Hessen), Rz. 63 ff.

8) Kapitel VII[57]

Da im digitalen Zeitalter **grenzüberschreitende Sachverhalte** die Norm sind, sieht die DSGVO auch eine verstärkte **Zusammenarbeit zwischen den einzelnen Aufsichtsbehörden** vor. Liegt ein grenzüberschreitender Sachverhalt vor, soll unter Einbindung aller betroffenen Aufsichtsbehörden eine abgestimmte Entscheidung getroffen werden, die dann dem Verantwortlichen oder Auftragsverarbeiter am Sitz seiner Hauptniederlassung zuzustellen ist. Sowohl die betroffene Person, als auch der Verantwortliche/Auftragsverarbeiter, sollen sich im Ergebnis mit nur einer Anlaufstelle konfrontiert sehen („One-Stop-Shop").[58]

Dabei fungiert die Aufsichtsbehörde am **Sitz der Hauptniederlassung** als **federführende Aufsichtsbehörde**[59], die die Einbindung der (sonst noch) betroffenen Aufsichtsbehörden koordiniert und einen Entscheidungsentwurf vorbereitet und mit den betroffenen Aufsichtsbehörden abstimmt.

Der Empfänger ist, sofern er die Entscheidung nicht bekämpft, verpflichtet, die Entscheidung in all seinen Niederlassungen in der EU umzusetzen.

Kapitel VII sieht auch noch die Verpflichtung zur wechselseitigen Amtshilfe (Art. 61) und die Möglichkeit zur Durchführung gemeinsamer Maßnahmen der Aufsichtsbehörden (Art. 62) vor.

---

[57] Siehe dazu im Detail *Leissler/Wolfbauer*, Der One Stop Shop in der DSGVO, in *Knyrim* (Hrsg.) aaO S. 291 ff; *Schmidl*, Kooperation der Aufsichtsbehörden bei grenzüberschreitenden Fällen, in *Knyrim* (Hrsg.) aaO S. 303 ff.

[58] Zur Zusammenarbeit der federführenden und betroffenen Aufsichtsbehörden vgl. EDSA, Guidelines 02/2022 on the application of Article 60 GDPR, Version 1.0 vom 14. März 2022, abrufbar in englischer Sprache unter https://edpb.europa.eu/system/files/2022-03/guidelines_202202_on_the_application_of_article_60_gdpr_en.pdf.

[59] Vgl. dazu WP 244, Leitlinie der Art. 29-Gruppe vom 13.12.2016 zur Feststellung der federführenden Aufsichtsbehörde, abrufbar unter https://www.dsb.gv.at/dam/jcr:59cd262c-c7b4-45ad-b127-ad58767cdc33/Leitlinien%20f%C3%BCr%20die%20Bestimmung%20der%20federf%C3%BChrenden%20Aufsichtsbeh%C3%B6rde%20eines%20Verantwortlichen.pdf. Diese Leitlinien wurden vom EDSA ausdrücklich übernommen: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

Das Verfahren zur Zusammenarbeit findet keine Anwendung, wenn es sich beim Verantwortlichen/Auftragsverarbeiter um eine Behörde oder einen beliehenen Rechtsträger handelt (Art. 55 Abs. 2).

Eine wesentliche Rolle spielt der nach Art. 68 eingerichtete **Europäische Datenschutzausschuss (EDSA)**[60], in welchem die Aufsichtsbehörden aller Mitgliedstaaten, der Europäische Datenschutzbeauftragte sowie die Europäische Kommission vertreten sind.

Der Ausschuss hat nach Art. 70 vielfältige Aufgaben, darunter die Verabschiedung von **Leitlinien** zu bestimmten Themen der DSGVO, aber auch die Abgabe von **Stellungnahmen** sowie die **Fassung verbindlicher Beschlüsse** (Art. 64 und 65).[61] Er wird dabei von einem Sekretariat unterstützt, das vom Europäischen Datenschutzbeauftragten bereitgestellt wird.

[60] Siehe auch https://edpb.europa.eu/.
[61] Die im Rahmen des sogenannten „Kohärenzverfahrens“ angenommenen Entscheidungen sind unter https://edpb.europa.eu/our-work-tools/consistency-findings_en abrufbar.

9) Kapitel VIII

Art. 77 normiert das **Recht auf eine Beschwerde** bei einer Aufsichtsbehörde.

Gegen verbindliche Entscheidungen der Aufsichtsbehörde bzw. gegen Untätigkeit der Aufsichtsbehörde steht der **Rechtsweg an ein Gericht** offen (Art. 78). Zuständig für solche Beschwerden sind die Gerichte jenes Mitgliedstaates, in welchem die Behörde ihren Sitz hat.

Das Verfahren vor der Aufsichtsbehörde ist für den Beschwerdeführer kostenfrei, außer die Beschwerdeführung erfolgt offensichtlich unbegründet oder – insbesondere aufgrund ihrer Häufung – exzessiv. In diesen Fällen kann sich die Aufsichtsbehörde weigern, tätig zu werden oder angemessene Kosten vorschreiben.

Art. 79 normiert das Recht auf einen wirksamen gerichtlichen Behelf gegen Verantwortliche oder Auftragsverarbeiter. Nach der Rechtsprechung des Obersten Gerichtshofes (OGH)[62] kann gegen Verantwortliche und Auftragsverarbeiter des privaten Bereiches (das sind im Wesentlichen Privatpersonen, Personengemeinschaften und juristische Personen des Privatrechts, wie Vereine, GmbH etc.) **Klage** vor dem zuständigen Zivilgericht erhoben werden.

Das bedeutet, dass ein **Wahlrecht beim Rechtsschutz** besteht: Beschwerde vor der Datenschutzbehörde oder Klage vor einem Zivilgericht. Zur Frage, welchem dieser beiden Rechtsbehelfe Vorrang zukommt und ob in derselben Sache gleichzeitig eine Beschwerde nach Art. 77 Abs. 1 DSGVO und eine gerichtliche Klage nach Art. 79 Abs. 1 leg. cit. erhoben werden kann, ist derzeit ein Vorabentscheidungsverfahren vor dem EuGH anhängig.[63]

Örtlich und sachlich zuständig ist in erster Instanz gemäß § 29 Abs. 2 DSG das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht, in dessen Sprengel der Kläger (oder wahlweise der Beklagte) seinen gewöhnlichen Aufenthalt oder Sitz hat. Der Oberste Gerichtshof hat ausgesprochen, dass die Bestimmung des § 29

[62] Siehe dazu die Entscheidungen vom 20.12.2018, GZ 6 Ob 131/18k, und vom 23.05.2019, GZ 6 Ob 91/19d.
[63] Rs C-132/21.

Abs. 2 DSG nicht nur auf Schadenersatzklagen im engeren Sinn, sondern erweiternd auch auf andere zivilrechtliche Ansprüche nach dem DSG bzw. der DSGVO anzuwenden ist.[64]

Bitte beachten Sie dabei, dass – im Gegensatz zu einem Beschwerdeverfahren vor der Datenschutzbehörde – eine zivilrechtliche Klage jedenfalls mit Kosten (Gerichtsgebühren) verbunden ist und Sie sich ab einem Streitwert von mehr als 4 000 Euro zwingend (und kostenpflichtig) von einem Rechtsanwalt vertreten lassen müssen.

Gegen Behörden, Ämter udgl. ist jedoch eine zivilrechtliche Klage nicht möglich. Hier besteht ausschließlich die Möglichkeit einer Beschwerde vor der Datenschutzbehörde.

Nach Art. 80 können sich betroffene Personen von **spezialisierten Einrichtungen,** Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht **vor der Aufsichtsbehörde vertreten** und **Schadenersatz gerichtlich einklagen** lassen. Die Mitgliedstaaten können auch vorsehen, dass diese Einrichtungen auch unabhängig von einer Bevollmächtigung Beschwerde bei der Aufsichtsbehörde einreichen können. Die Geltendmachung von Schadenersatzforderungen ist hingegen ohne Mandat nicht möglich.[65]

Bitte beachten Sie, dass in Österreich die genannten Einrichtungen keine Schadenersatzklagen und auch keine Beschwerde ohne Mandat erheben können (§ 28 DSG)![66]

Art. 82 normiert die Möglichkeit, für erlittenen materiellen und immateriellen Schaden **Schadenersatz[67]** vom Verantwortlichen oder Auftragsverarbeiter zu verlangen.[68] Sind an einer Verarbeitung mehrere Verantwortliche oder Auftragsverarbeiter beteiligt, so haftet jeder von ihnen für den Gesamtschaden (Art. 82 Abs. 4).

Art. 83 enthält Geldbußentatbestände sowie jene Gründe, die als erschwerend oder mildernd bei der Strafbemessung zu berücksichtigen sind. Der Europäische Datenschutzausschuss

---

[64] Vgl. den Beschluss des OGH vom 3. August 2021, 6 Nc 19/21b mwN.
[65] Siehe dazu EG 142. Damit sollen Sammelklagen verhindert werden.
[66] Siehe dazu auch OGH 26.11.2019, GZ 4 Ob 84/19k
[67] Zur Auslegung von Art. 82 DSGVO und insbesondere zur Frage, ob die Zuerkennung immateriellen Schadenersatzes eine Beeinträchtigung bestimmter Intensität verlangt, sind derzeit mehrere Vorabentscheidungsersuchen anhängig, siehe bspw. C-300/21..
[68] Siehe dazu auch *Tretzmüller*, Private Enforcement – Immaterieller Schadenersatz bei Datenschutzverletzungen, in: *Jahnel* (Hrsg.) Datenschutzrecht. Jahrbuch 17 (2017) S. 199 ff.

hat – rechtlich unverbindliche – Leitlinien mit Kriterien zur Berechnung der Höhe von Geldbußen erlassen.[69]

Die **Geldbußen**, bei welchen es sich um **Verwaltungsstrafen** handelt[70], reichen bis zu 20 Millionen Euro oder, im Falle eines Unternehmens, bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Betrag höher ist. Es bleibt den Mitgliedstaaten vorbehalten festzulegen, ob Geldbußen auch gegen Behörden und öffentliche Stellen verhängt werden können.[71]

Sieht die Rechtsordnung eines Mitgliedstaates keine Geldbußen vor, kann Art. 83 so angewendet werden, dass die Aufsichtsbehörde einen Strafantrag bei Gericht stellt und die Geldbuße von einem Gericht verhängt wird.

Art. 83 DSGVO ermöglicht auch die Verhängung von Geldbußen **direkt gegen juristische Personen** (GmbH, AG, Verein etc.). Ob es für die Zurechnung zur juristischen Person erforderlich ist, dass die Aufsichtsbehörde einer vertretungsbefugten Person (Geschäftsführer, Vorstandsmitglied, Obmann etc.) eine Verfehlung nachzuweisen hat, wird derzeit durch den EuGH geklärt.[72]

Art. 84 verpflichtet die Mitgliedstaaten, zusätzliche Sanktionen, vor allem gerichtlich strafbare Tatbestände, zu normieren.

---

[69] Vgl. EDSA, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 1.0 vom 12. Mai 2022, abrufbar in englischer Sprache unter https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf (die öffentliche Begutachtung endete am 27. Juni 2022).

[70] Dies ergibt sich eindeutig aus einem Vergleich der Sprachfassungen; die englische Sprachfassung spricht von „administrative fines“, die französische von „amendes administratives“. Bei Geldbußen handelt es sich folglich um Strafen und nicht um eine andere Sanktion (vgl. dazu zu Geldbußen im Bereich des Vergabewesens etwa das Erkenntnis des VwGH vom 16.12.2015, Zl. Ro 2014/04/0065).

[71] Für Österreich siehe zur Unzulässigkeit der Verhängung einer Verwaltungsstrafe gegen ein oberstes Organ VfSlg. 19.988/2015. Nach § 30 Abs. 5 DSG können gegen Behörden und öffentliche Stellen keine Geldbußen verhängt werden (siehe dazu Punkt 11 unten).

[72] C-807/21.

10) Kapitel IX bis XI

Kapitel IX legt besondere Verarbeitungssituationen (bspw. Freiheit der Meinungsäußerung, Zugang zu amtlichen Dokumenten, Beschäftigungskontext) fest. Die Mitgliedstaaten sind dazu angehalten, durch Rechtsvorschriften diese Verarbeitungssituationen näher zu determinieren, um sie in Einklang mit der DSGVO zu bringen.

Art. 85 Abs. 2 gibt Mitgliedstaaten die Möglichkeit, die Anwendung bestimmter Kapitel der DSGVO im Falle einer Verarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken auszuschließen. Davon hat der österreichische Gesetzgeber etwa in § 9 DSG Gebrauch gemacht. Zur Frage, ob die Bestimmung des § 9 Abs. 1 DSG verfassungswidrig ist, ist derzeit ein Normenkontrollverfahren nach Art. 140 Abs. 1 B-VG beim Verfassungsgerichtshof anhängig.[73]

Nach Art. 99 trat die Verordnung am zwanzigsten Tag nach ihrer Veröffentlichung im ABl. in Kraft (das war der 24.05.2016) und gilt seit dem 25.05.2018.

[73] VfGH, G 200/2022

11) Das österreichische Datenschutzgesetz

In Durchführung der DSGVO und Umsetzung der Datenschutzrichtlinie für den Bereich Polizei und Justiz (DSRL-PJ)[74] wurde vom österreichischen Gesetzgeber das Datenschutz-Anpassungsgesetz 2018[75] verabschiedet, das am 25. Mai 2018 in Kraft getreten ist. Es gab dazu im Jahr 2018 zwei Novellen (BGBl. I Nr. 23/2018 und BGBl. I Nr. 24/2018), mit BGBl. I Nr. 14/2019 wurde das DSG zuletzt novelliert und auch in Zukunft ist mit Änderungen zu rechnen.

Kernstück der neuen Regelung ist das Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG). Dabei wurde das früher geltende DSG 2000 der einfachgesetzlichen Bestimmungen entkleidet, die Verfassungsbestimmungen (insbes. das Grundrecht auf Datenschutz nach § 1) bleiben weitgehend bestehen bzw. wurden angepasst.

Das DSG gliedert sich in fünf Hauptstücke. Das 1. Hauptstück normiert die Durchführung der Datenschutz-Grundverordnung und ergänzende Regelungen, das 2. Hauptstück regelt die Organe (des Datenschutzes), das 3. Hauptstück die Umsetzung der DSRL-PJ, das 4. Hauptstück die besonderen Strafbestimmungen und das 5. Hauptstück die Schlussbestimmungen.

Für Verantwortliche und Auftragsverarbeiter relevant ist v.a. das **1. Hauptstück**, das sich in **drei Abschnitte** gliedert.

Der **1. Abschnitt** enthält **allgemeine Bestimmungen** (bspw. zum Datenschutzbeauftragten oder zum Datengeheimnis).

Der **2. Abschnitt** regelt die **Datenverarbeitungen zu spezifischen Zwecken** (wie bspw. für Zwecke der wissenschaftlichen Forschung und Statistik).

---

[74] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates – Datenschutzrichtlinie-Polizei Justiz (DSRL-PJ), ABl. Nr. L 119 vom 04.05.2016 S. 89.

[75] BGBl. I Nr. 120/2017.

Der **3. Abschnitt** regelt die **Bildverarbeitung** (vormals „Videoüberwachung“). Das Bundesverwaltungsgericht (BVwG) hat jedoch entschieden, dass diese Bestimmungen nicht anzuwenden sind.[76] Die Bildverarbeitung im privaten Bereich richtet sich daher nach den Art. 5 und 6 DSGVO.[77]

Weitere wesentliche Eckpunkte sind:

- Die **Datenschutzbehörde** wird als **Aufsichtsbehörde mit allen Befugnissen** (**einschließlich der Verhängung von Geldbußen**[78]) nach der DSGVO und der DSRL-PJ eingerichtet.
- **Geldbußen** können auch direkt **gegen juristische Personen** verhängt werden und nicht nur gegenüber dem verantwortlichen Beauftragten (§ 9 des Verwaltungsstrafgesetzes 1991 – VStG); gegen Behörden und öffentliche Stellen können keine Geldbußen verhängt werden.
- Die Datenschutzbehörde entscheidet über alle **Beschwerden** verbindlich (d.h. auch über solche, bei denen nach der früheren Rechtslage der Zivilrechtsweg gemäß § 32 DSG 2000 zu beschreiten war).
- Gegen verbindliche Entscheidungen der Datenschutzbehörde steht der Rechtszug an das **Bundesverwaltungsgericht** uneingeschränkt offen.
- **Betroffene** können sich von Einrichtungen, Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht, die im Bereich des Datenschutzes tätig sind, vor der Datenschutzbehörde und vor dem Bundesverwaltungsgericht **vertreten lassen**; ein **Einschreiten** der Einrichtungen, Organisationen oder Vereinigungen **ohne Mandat** (d.h. ohne Bevollmächtigung) ist **nicht vorgesehen**[79].
- Es werden – neben den Geldbußen nach der DSGVO – auch **Verwaltungsübertretungen** normiert, die von der Datenschutzbehörde mit Geldstrafe bis zu 50 000 Euro zu ahnden sind.

---

[76] Siehe dazu die Entscheidungen vom 20.11.2019, GZ W256 2214855-1, und vom 20.11.2019, GZ W211 2210458-1.

[77] Siehe dazu die Informationen unter https://www.dsb.gv.at/download-links/fragen-und-antworten.html#Videoueberwachung_durch_Private_einschlieszlich_der_Privatwirtschaftsverwaltung_der_oeffentlichen_Hand_.

[78] Zur Zulässigkeit der Verhängung von Geldstrafen in substantieller Höhe durch Verwaltungsbehörden vgl. das Erkenntnis des VfGH vom 13.12.2017, GZ G 408/2016 u.a..

[79] Siehe dazu OGH 4 Ob 84/19k.

- Die von der **Datenschutzbehörde** zu führenden **Listen** (Notwendigkeit der Durchführung einer Datenschutz-Folgeabschätzung, Anforderungen an Zertifizierungsstellen, Kriterien für die Akkreditierung einer Stelle) sind in Form einer **Verordnung** im BGBl. kundzumachen[80]

[80] Siehe dazu die Seite https://www.dsb.gv.at/verordnungen-in-osterreich. Bereits erlassen wurden die Datenschutz-Folgenabschätzung-Ausnahmenverordnung (DSFA-AV), BGBl. II Nr. 108/2018, sowie die Verordnung über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V), BGBl. II Nr. 278/2018, und die Verordnung über die Anforderungen an eine Überwachungsstelle für Verhaltensregeln (ÜStAkk-V), BGBl. II Nr. 264/2019.

12) Häufig gestellte Fragen

a) Allgemeines

Seit wann gilt die DSGVO?

Seit 25. Mai 2018.

Kann ich mich mit Fragen betreffend die DSGVO und das DSG an die Datenschutzbehörde wenden?

Die Datenschutzbehörde erteilt den Parteien inhaltliche Auskünfte zu ihren anhängigen Verfahren vor der Datenschutzbehörde.

Die Datenschutzbehörde ist gemäß Art. 57 Abs. 1 lit. e DSGVO verpflichtet, auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieser Verordnung zur Verfügung zu stellen. Diese Unterstützung ist aber nicht geeignet, einen Anwalt zu ersetzen und darf auch nicht das Ergebnis eines Verfahrens vorwegnehmen.

Es wird daher um Verständnis ersucht, dass im Rahmen einer schriftlichen Anfrage keine rechtlichen Beurteilungen zur Anwendung und Auslegung rechtlicher Bestimmungen und inhaltliche Beratungsleistungen vorgenommen werden können. Verbindliche Entscheidungen kann es immer nur am Ende eines konkreten Verfahrens geben.

Was ist eine „öffentliche Stelle“?

Die Datenschutzbehörde kann keine konkrete Einzelfallprüfung vor- bzw. vorwegnehmen, ob eine Stelle als öffentliche Stelle anzusehen ist oder nicht.

- Grundsätzlich obliegt es dem Verantwortlichen selbst, diese Einordnung entsprechend der gegebenen Rechtsgrundlagen vorzunehmen. Neben diversen deutschsprachigen Kommentaren (siehe dazu Punkt 13 dieses Leitfadens) sowie der Leitlinie der Art. 29-Gruppe zum Datenschutzbeauftragten[81], welche Anhaltspunkte für die Auslegung des Begriffs der öffentlichen Stelle liefern, ist insbesondere das

[81] Abrufbar unter https://www.dsb.gv.at/europa-internationales/europaeischer_datenschutzausschuss_edsa.html.

Datenschutzgesetz[82] heranzuziehen. Es findet sich in **§ 30 Abs. 5 DSG** eine Definition, welche herangezogen werden kann. Als „öffentliche Stellen" können demnach insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, die im gesetzlichen Auftrag handeln, und Körperschaften des öffentlichen Rechts, angesehen werden.

Sofern die genannten Merkmale vom jeweiligen Verantwortlichen nicht erfüllt werden, wird schwerlich eine Einordnung als öffentliche Stelle möglich sein.

Gibt es nach Inkrafttreten der DSGVO noch ein nationales Datenschutzrecht?

Ja. Das österreichische Parlament hat dazu das Datenschutz-Anpassungsgesetz erlassen (siehe dazu auch Punkt 11 des Leitfadens). Das Datenschutzgesetz (DSG) besteht weiter.

Gilt das Datenschutzrecht auch für juristische Personen?

Juristische Personen (bspw. ein Verein, eine GmbH, eine AG, eine Genossenschaft) werden durch die DSGVO verpflichtet, bestimmte Vorgaben einzuhalten.

Sie können sich im Regelfall aber nicht auf die **DSGVO** berufen, um Rechte (wie bspw. Auskunft, Löschung, Widerspruch etc.) geltend zu machen, weil die DSGVO nur natürliche Personen schützt. Der EuGH lässt eine Berufung auf die DSGVO nur zu, wenn in der Firma/Bezeichnung der juristischen Person der Name einer natürlichen Person vorkommt (z.B. Max Mustermann GmbH).[83]

§ 1 DSG schützt – anders als die DSGVO – in Österreich nach wie vor auch juristische Personen.[84]

---

[82] Abrufbar auf der Website des Parlaments unter www.parlament.gv.at.
[83] Vgl. das Urteil des EuGH vom 9. November 2010, verb. Rs C-92/09 und C-93/09 (Schecke und Eifert), Rz. 53 ff.
[84] Siehe hierzu auch den Bescheid der Datenschutzbehörde vom 25.05.2020 zur GZ: 2020-0.191.240.

Das heißt, dass juristische Personen in „Binnenfällen“ (d.h. Fällen ohne Auslandsbezug) folgende Rechte geltend machen können:

- Geheimhaltung
- Auskunft
- Richtigstellung
- Löschung

Wie kann ich die DSFA-AV von der DSFA-V abgrenzen?

Wenn sich die Frage stellt, ob (k)eine Datenschutz-Folgenabschätzung durchzuführen ist, sollten zuerst die beiden Verordnungen der DSB und die Erläuterungen dazu (abrufbar auf der Website der DSB) gelesen werden.

Nur dann, wenn eine Verarbeitungstätigkeit in der **DSFA-AV nicht** aufscheint, stellt sich die Frage einer Datenschutz-Folgenabschätzung.

Die **DSFA-V** räumt der DSFA-AV einen Vorrang ein (vgl. dazu § 2 DSFA-V, wo es heißt: „*Sofern […] keine Datenverarbeitung gemäß der [DSFA-AV] vorliegt, ist nach Maßgabe der folgenden Bestimmungen jedenfalls eine Datenschutz-Folgenabschätzung durchzuführen*“).

b) Ich bin Betroffene(r) – meine Rechte

Welche Rechte stehen mir zu (Betroffenenrechte) und wo kann ich sie geltend machen?

Die DSGVO bringt einen neuen Katalog von Rechten, die teilweise mit bisher gewohnten Rechten übereinstimmen. Beachten Sie, dass diese Rechte im Regelfall nur natürlichen Personen zustehen.

In fast allen Fällen muss der Verantwortliche aufgefordert werden, das Recht zu gewähren, bevor eine Beschwerde möglich ist. Die Datenschutzbehörde bietet auf ihrer Website unverbindlich dafür geeignete Formulare an[85].

[85] Abrufbar unter https://www.dsb.gv.at/dokumente.

1. Das **Recht auf Auskunft (Art. 15 DSGVO)**. Der Betroffene darf eine Bestätigung verlangen, ob ihn betreffende Daten verarbeitet werden, einschließlich einer Negativauskunft. Werden Daten verarbeitet, hat der Betroffene das Recht auf folgende Informationen:

    a. Verarbeitungszwecke;

    b. Datenkategorien;

    c. Kopie (z.B. Ausdruck) der verarbeiteten Dateninhalte;

    d. Datenempfänger oder Empfängerkategorien;[86]

    e. geplante Speicherdauer (oder Kriterien für deren Festlegung);

    f. Bestehen eines Berichtigungs-, Löschungs-, Einschränkungs- oder Widerspruchsrechts;

    g. Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

    h. verfügbare Informationen über die Datenherkunft;

    i. Bestehen einer automatisierten Entscheidungsfindung (Profiling eingeschlossen), Logik und Tragweite solcher Verfahren.[87]

    Die Frist zur Auskunftserteilung wird durch die DSGVO auf einen Monat verkürzt. U.U. ist eine Verlängerung auf drei Monate möglich.

    Das Recht auf Auskunft ist ein Recht auf Auskunft über eigene Daten des Betroffenen.[88] Eine Kopie der verarbeiteten Dateninhalte muss so gestaltet sein, dass die Datenschutzrechte anderer Personen nicht verletzt werden. Der Umfang des Auskunftsrechts nach Art. 15 Abs. 3 DSGVO ist derzeit Gegenstand eines Vorabentscheidungsverfahrens vor dem EuGH.[89]

---

[86] Beachte das derzeit anhängige Vorabentscheidungsverfahren vor dem EuGH in der Rs C-154/21.
[87] Beachte das zu Art. 22 derzeit anhängige Vorabentscheidungsverfahren vor dem EuGH in der Rs C-203/22.
[88] Vgl. die Bescheide der DSB vom 18. April 2019, GZ D122.913/0001-DSB/2019; sowie vom 12. November 2020, GZ 2020-0.697.744.
[89] Rs C-487/21.

2. Das **Recht auf Berichtigung (Art. 16 DSGVO)** bezieht sich auf Dateninhalte.[90] Neu in der DSGVO ist das Recht auf Vervollständigung von Daten – eventuell durch eine ergänzende Anmerkung. Die Frist zur Berichtigung wird durch die DSGVO auf einen Monat verkürzt. U.U. ist eine Verlängerung auf drei Monate möglich.

3. Das **Recht auf Löschung (Art. 17 DSGVO)** (einschließlich des „Rechts auf Vergessenwerden"). Das Löschungsrecht setzt voraus, dass einer der folgenden Umstände vorliegt oder eingetreten ist:

    a. Wegfall des Verarbeitungszwecks

    b. Widerruf der Einwilligung des Betroffenen

    c. wirksamer Widerspruch gegen die Datenverarbeitung

    d. anfängliche Unrechtmäßigkeit der Datenverarbeitung

    e. rechtliche Verpflichtung zur Löschung (z.B. Gesetz, Urteil, Bescheid)

    f. Fehlen einer Einwilligung der Erziehungsberechtigten eines Kindes

    Neu: Hat der Verantwortliche die Daten öffentlich gemacht (z.B. Im Internet), so muss er bei Löschung alle angemessenen Maßnahmen, auch technischer Art ergreifen, um verantwortliche Datenempfänger (insbesondere Suchmaschinenbetreiber) darüber zu informieren, dass der Betroffene die Löschung oder Entfernung von Links, Kopien oder Replikationen wünscht (= „Recht auf Vergessenwerden").

    Das Löschungsrecht kann durch das Recht auf Meinungsfreiheit, durch Rechtspflichten des Verantwortlichen, Interessen der Rechtsverteidigung sowie öffentliche Interessen (öffentliche Gesundheit, wissenschaftliche und Archivzwecke) beschränkt sein.

    Die Frist zur Löschung wird durch die DSGVO auf einen Monat verkürzt. U.U. ist eine Verlängerung auf drei Monate möglich.

[90] Die DSB vertritt die Ansicht, dass bloße orthografische (Schreib-)Fehler nicht vom Recht auf Berichtigung erfasst werden. Dies wurde vom BVwG im Erkenntnis vom 5. Februar 2021, W211 2226025-1 bestätigt und wird gegenwärtig vom Verwaltungsgerichtshof im Rahmen eines Revisionsverfahrens überprüft.

4. Neu: Das **Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)**. Es handelt sich um ein zeitlich beschränktes bzw. bedingtes Recht. Die Voraussetzungen sind:

    a. die Richtigkeit der Daten wird bestritten;

    b. die Rechtmäßigkeit der Datenverarbeitung wird bestritten, der Betroffene selbst lehnt aber die Löschung ab;

    c. der Betroffene benötigt die Daten, deren Verarbeitungszweck weggefallen ist, für die Geltendmachung von Rechtsansprüchen;

    d. der Betroffene hat Widerspruch gegen die Datenverarbeitung eingelegt.

    Daten, hinsichtlich derer das Recht auf Einschränkung der Verarbeitung ausgeübt worden ist, dürfen nur mehr mit Zustimmung des Betroffenen, zur Geltendmachung von Rechtsansprüchen, zum Schutz der Rechte anderer oder aus wichtigen öffentlichen Interessen verarbeitet werden.

    In den Fällen a. und d. ist die Einschränkung auf die Dauer der Prüfung des Hauptanspruchs (auf Löschung) beschränkt. Der Betroffene muss vor Aufhebung der Einschränkung informiert werden.

    Datenempfänger sind, wenn dies nicht unmöglich oder mit unverhältnismäßigem Aufwand verbunden ist, über Einschränkungen zu informieren. Der Betroffene kann verlangen, über die Empfänger der Daten informiert zu werden.

    Die Frist zur Einschränkung der Verarbeitung beträgt einen Monat. U.U. ist eine Verlängerung auf drei Monate möglich.

5. Neu: Das **Recht auf Datenübertragbarkeit (Art. 20 DSGVO)**. Es soll sicherstellen, dass der Betroffene eigene Daten, die er selbst einem (privaten) Verantwortlichen bekanntgegeben (sie „bereitgestellt“) hat, zurückerhalten oder einem neuen Verantwortlichen übergeben kann. Zu denken ist etwa an selbst erstellte Profile in sozialen Netzwerken. Die Verantwortlichen sollen nach Möglichkeit eine direkte, technische Übertragbarkeit sicherstellen, zwingend ist dies aber nicht vorgeschrieben. Die Daten anderer Personen als des Betroffenen unterliegen nicht diesem Recht. Es kann nur dann geltend gemacht werden, wenn Grundlage für die

Datenverarbeitung entweder die Einwilligung der betroffenen Person oder ein Vertrag ist.

6. Das **Recht auf Widerspruch (Art. 21 DSGVO)**. Durch die Ausübung dieses Rechts kann der Betroffene bei einer Datenverarbeitung, die ohne seine ausdrückliche oder implizite Einwilligung stattfindet (etwa auf Grund einer gesetzlichen Ermächtigung oder wegen vom Verantwortlichen behaupteter überwiegender berechtigter Interessen), eine Prüfung der von ihm vorgebrachten Gründe für eine Beendigung der Verarbeitung verlangen. Gegen die Datenverarbeitung für Zwecke der Direktwerbung und damit verbundenes Profiling (automatische Bewertung einer Person und ihres Verhaltens, z.B. Kaufkrafteinschätzung, Einordnung in eine Marketing-Zielgruppe) ist ein jederzeitiger Widerspruch ohne Angabe von Gründen möglich. Gegen die Zusendung elektronischer Post zu Werbezwecken (SMS, E-Mails, etc.) kann der Widerspruch auch mittels Eintragung in die sog. „ECG-Liste“ erfolgen.[91] Gegen die Zusendung postalischer Werbematerialien kann eine Eintragung in die sog. „Robinson-Liste“ erfolgen.[92] Ist der Widerspruch begründet, sind die Daten zu löschen.

   Die Frist zur Entscheidung über einen Widerspruch beträgt einen Monat. U.U. ist eine Verlängerung auf drei Monate möglich.

7. **Rechte betreffend automatisierte Einzelentscheidungen und Profiling (Art. 22 DSGVO)**. Die DSGVO verbietet solche Entscheidungen (z.B. bei Verhängung von Verwaltungsstrafen, Steuervorschreibungen, Entscheidung über Stellenbewerbungen, Kreditgewährung, Vertragsabschlüssen allgemein, Einordnung in eine Marketing-Zielgruppe) zunächst grundsätzlich, sieht aber einige Ausnahmen vor. Ausnahmegründe sind gesetzlich vorgeschriebene Anwendungsfälle, ausdrückliche und nachweisliche Einwilligung des Betroffenen und Sorgfaltspflichten anlässlich eines Vertragsabschlusses. Für die Anwendbarkeit der Bestimmung muss nicht der gesamte Entscheidungsprozess ausschließlich automatisiert ablaufen. Er darf sich nur unter besonderen Bedingungen und nie ausschließlich auf sensible Daten (besondere Datenkategorien gemäß Art. 9 Abs. 1 DSGVO) stützen. Der

[91] Vgl. § 174 Abs. 4 Z 4 TKG 2021 iVm. § 7 Abs. 2 E-Commerce-Gesetz; die „ECG-Liste“ wird von der Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) geführt.
[92] Die „Robinson-Liste“ wird von der WKO geführt.

Betroffene kann vor allem die Überprüfung der automatisierten Entscheidung durch einen Menschen verlangen und hat ein besonderes Auskunftsrecht hinsichtlich der Logik der automatisierten Entscheidungsfindung.

Die Frist zur Entscheidung über Rechte betreffend die automatisierte Entscheidungsfindung beträgt einen Monat. U.U. ist eine Verlängerung auf drei Monate möglich.

c) Ich bin Verantwortliche(r)/Auftragsverarbeiter(in) – meine Pflichten

Bin ich Verantwortliche(r) oder Auftragsverarbeiter(in)?

Die Definition der eigenen Rolle ist essentiell.

Verantwortliche(r) im Sinne der DSGVO ist, wer darüber bestimmt, welche Daten zu welchen Zwecken mit welchen Mitteln verarbeitet werden („Herr der Daten"). Verantwortlicher zu sein hängt nicht von der Organisations- oder Rechtsform ab, sondern von funktionalen Gesichtspunkten.[93] Der/Die Verantwortliche trifft auch die alleinige Entscheidung, ob Daten verändert, berichtigt oder gelöscht werden. Er/Sie ist Adressat von Betroffenenrechten und muss diesen nachkommen.

UU liegt eine **gemeinsame Verantwortung** vor (Art. 26 DSGVO), d.h. dass zwei oder mehr Verantwortliche die oben genannten Entscheidungen treffen.[94] Dabei ist es nicht erforderlich, dass die Aufgaben und Pflichten gleich verteilt sind; entscheidend ist aber, dass jeder Beteiligte zumindest – wenn auch nur minimal – Entscheidungen treffen kann (vgl. dazu v.a. die Urteile des EuGH vom 05.06.2018, C-210/16, und vom 10.07.2018, C-25/17).

---

[93] Siehe dazu auch das Erkenntnis des BVwG W258 2221952-1/3E vom 31.03.2020; vgl. im Weiteren EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, Version 2.0 vom 7. Juli 2021, abrufbar in deutscher Sprache unter https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_de.pdf.

[94] Vgl. etwa in Bezug auf gerichtlich beeidete Sachverständige die Erkenntnisse des Bundesverwaltungsgerichts vom 27.09.2018, GZ W214 2196366-2 und vom 23.01.2020, GZ W214 2196366-3.

Ein **Auftragsverarbeiter** hingegen verarbeitet Daten „im Auftrag“, d.h. auf **Weisung** und unter **Aufsicht** eines/einer Verantwortlichen. Eine Datenverarbeitung zu eigenen Zwecken ist nicht vorgesehen.

Folgende Personen/Stellen sind im Regelfall **keine Auftragsverarbeiter**:

- Angehörige freier Berufe (d.h. Rechtsanwälte, Ärzte, Steuerberater etc.) – diese unterliegen eigenen Standesregeln bzw. sehen die einschlägigen gesetzlichen Bestimmungen eine eigenverantwortliche Datenverarbeitung vor
- Telekom-Unternehmen – diese unterliegen den Vorschriften des TKG 2021, welches sie verpflichtet, Daten eigenverantwortlich zu verarbeiten
- Kreditauskunfteien – diese unterliegen der Gewerbeordnung und verarbeiten Daten eigenständig für Zwecke der Auskunft über die Kreditwürdigkeit einer Person
- Betreiber von Internet-Suchmaschinen – diese entscheiden im Rahmen der von Ihnen automatisch, kontinuierlich und systematisch durchgeführten „Durchforstung“ der im Internet veröffentlichten Informationen selbst über die Zwecke und Mittel der Verarbeitung und sind daher als Verantwortliche anzusehen

Ob jemand Verantwortlicher oder Auftragsverarbeiter ist, kann grundsätzlich nicht pauschal beantwortet werden und ist im Einzelfall zu beurteilen.[95]

Gilt die DSGVO nur für Großunternehmen?

Nein. Die DSGVO gilt für Klein- und Einpersonenunternehmen ebenso wie für Vereine und für Behörden und öffentliche Stellen. Punktuell sind Ausnahmen für Klein- und Einpersonunternehmen vorgesehen (z.B. in Art. 30 Abs. 5 DSGVO betreffend die Führung eines Verzeichnisses von Verarbeitungstätigkeiten).

Ich habe für eine Datenverarbeitung die Einwilligung von Betroffenen (z.B. Kunden) eingeholt. Ändert sich durch die DSGVO etwas daran?

Sofern eine eingeholte Einwilligung den Voraussetzungen von Art. 7 DSGVO entspricht, ändert sich nichts. Gegebenenfalls sind Einwilligungen erneut einzuholen.

---

[95] Bspw. kommt es bei Berufsdetektiven darauf an, ob der jeweilige Auftrag über einen solchen Detaillierungsgrad verfügt, dass die Letztentscheidung, insbesondere über den Zeitpunkt der Datenerhebung und die Mittel, vom Auftraggeber getroffen wird; vgl. das Erkenntnis des Bundesverwaltungsgerichts vom 25. Juni 2019, GZ W258 2188466-1.

Was ist von einer Einwilligung umfasst?

Die Einwilligung ist eine von mehreren Möglichkeiten, Daten rechtskonform zu verarbeiten (**Rechtsgrundlage für eine Datenverarbeitung**). Mit der Einwilligung stimmt der Betroffene zu, dass seine Daten zu einem bestimmten Zweck verarbeitet werden. Die Einwilligung kann jederzeit widerrufen werden.

Von einer Einwilligung sind hingegen nicht umfasst

- Abweichungen von notwendigen Datensicherheitsmaßnahmen (z.B. Einwilligung, dass Nachrichten auf eine bestimmte – unsichere – Weise übermittelt werden)
- Heranziehungen von Auftragsverarbeitern (diese Entscheidung obliegt alleine dem Verantwortlichen)

In Derartiges kann nicht rechtswirksam eingewilligt werden.

Zu beachten ist ferner, dass bei einigen Verarbeitungsvorgängen eine "normale" Einwilligung nicht ausreicht und die betroffene Person ihre Einwilligung ausdrücklich erteilen muss.[96]

Worüber muss ich Betroffene bei der Erhebung ihrer Daten informieren? Gibt es davon Ausnahmen?

Wenn Sie die Daten direkt bei den jeweiligen Betroffenen erheben, müssen Sie den Betroffenen sämtliche Informationen wie in Art. 13 DSGVO vorgesehen mitteilen. Eine Ausnahme von der Informationspflicht besteht nur dann, wenn die Betroffenen bereits über diese Informationen verfügen.

Wenn Sie Daten verarbeiten wollen, die Sie nicht bei den Betroffenen selbst erhoben haben, müssen Sie den Betroffenen sämtliche Informationen wie in Art. 14 DSGVO vorgesehen mitteilen. Dies kann unterbleiben, wenn die Betroffenen über die Informationen bereits verfügen, die Erteilung der Information unmöglich oder mit unverhältnismäßigem Aufwand verbunden ist, die Verarbeitung gesetzlich vorgesehen ist oder die Daten dem Berufsgeheimnis unterliegen (vgl. Art. 14 Abs. 5 DSGVO).

[96] Dies ist bspw. vorgesehen bei bestimmten Verarbeitungsvorgängen besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 2 lit. a DSGVO), bei automatisierten Entscheidungen im Einzelfall (Art. 22 Abs. 2 lit. c DSGVO), oder bei der Übermittlung personenbezogener Daten in ein unsicheres Drittland im Ausnahmefall (Art. 49 Abs. 1 lit. a DSGVO).

Beachten Sie dazu die Leitlinien des EDSA zur Transparenz (nähere Ausführungen dazu vorne zu Kapitel III).

Exkurs:

In diesem Zusammenhang ist darauf hinzuweisen, dass auch die Einwilligung zu Cookies „freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich" erfolgen muss. „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit" können keine Einwilligung im Sinne der DSGVO darstellen.[97]

Welche Pflichten gibt es für Verantwortliche und Auftragsverarbeiter?

Im Folgenden erhalten Sie einen kurzen Überblick über die wesentlichsten Pflichten, welche die Verantwortlichen bzw. die Auftragsverarbeiter durch die DSGVO treffen:

- ***Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)***

Verantwortliche müssen schriftlich ein Verzeichnis aller Verarbeitungstätigkeiten (= Datenanwendungen), die ihrer Zuständigkeit unterliegen, führen. Dieses Verzeichnis hat jedenfalls zu enthalten: den Namen und die Kontaktdaten des Verantwortlichen, Daten eines mit ihm gemeinsamen Verantwortlichen (falls vorhanden), Daten seines Vertreters (falls vorhanden), Daten des Datenschutzbeauftragten falls vorhanden), die Zwecke der Verarbeitung, die Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (= betroffene Personenkreise und Datenarten), Kategorien von Empfängern (einschließlich Empfänger in Drittländern oder internationale Organisationen); wenn möglich: Löschungsfristen, Beschreibung technischer und organisatorischer Maßnahmen.

Das Verzeichnis kann intern in jeder Sprache geführt werden. Kommt es jedoch zu einer Vorlage an die Datenschutzbehörde**, ist das Verzeichnis zwingend auf Deutsch vorzulegen**, da die Datenschutzbehörde fremdsprachige Dokumente in ihren Verfahren nicht berücksichtigen kann (Amtssprache Deutsch gemäß Art. 8 Abs. 1 Bundes-Verfassungsgesetz; siehe dazu auch das Erkenntnis des Verwaltungsgerichtshofes vom 17. Mai 2011, Zl. 2007/01/0389).

[97] Siehe hiezu die Entscheidung des EuGH vom 01.10.2019, C-673/17.

Auch Auftragsverarbeiter müssen schriftlich ein Verzeichnis aller Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten führen. Der Verantwortliche und sein Auftragsverarbeiter oder gegebenenfalls deren Vertreter haben der Datenschutzbehörde auf Anfrage das Verzeichnis zur Verfügung zu stellen.

Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, trifft die Pflicht zur Führung eines Verzeichnisses nicht, es sei denn, die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 DSGVO (Daten über rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung) bzw. eine Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO.

Zur Information:

Mit 25. Mai 2018 ist die Meldepflicht gemäß §§ 17 ff Datenschutzgesetz 2000 (DSG 2000) an das Datenverarbeitungsregister entfallen. DVR-Meldungen sind nicht mehr vorgesehen (siehe dazu auch die Information unter Punkt 11).

Da die Erstellung und Führung eines Verzeichnisses nach Art. 30 DSGVO ausschließliche Verantwortung von Verantwortlichen/Auftragsverarbeitern ist, bleibt es nach Ansicht der Datenschutzbehörde auch diesen überlassen, wie sie ihr Verzeichnis inhaltlich gestalten wollen. Seitens der Datenschutzbehörde gibt es dazu keine Vorgaben/kein Muster. Ehemalige DVR-Meldungen können als Vorlage für ein Verzeichnis herangezogen werden, zwingend ist dies jedoch nicht.

- ***Zusammenarbeit mit der Aufsichtsbehörde (Art. 31 DSGVO)***

Der Verantwortliche und der Auftragsverarbeiter, gegebenenfalls deren Vertreter, haben mit der Datenschutzbehörde auf deren Anfrage zusammenzuarbeiten. Die Nichtbefolgung dieser Pflicht ist mit Geldbuße bis zu 10 Millionen Euro bedroht.

- ***Sicherheit der Verarbeitung (Art. 32 DSGVO)***

Der Verantwortliche und sein Auftragsverarbeiter müssen durch geeignete technische und organisatorische Maßnahmen ein angemessenes Schutzniveau gewährleisten, dies kann u.a. nachgewiesen werden durch genehmigte Verhaltensregeln (Art. 40 DSGVO) oder aufgrund genehmigter Zertifizierungsverfahrens (Art. 42 DSGVO).

- ***Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33 DSGVO)***

Ein Verantwortlicher hat eine Meldung im Falle einer Verletzung des Schutzes personenbezogener Daten an die Datenschutzbehörde zu erstatten, wenn dadurch ein Risiko für die Rechte und Freiheiten der Betroffenen besteht; dies unverzüglich und möglichst binnen 72 Stunden nachdem ihm die Verletzung bekannt wurde. Darüber hinaus sind die notwendigen Informationen (Beschreibung der Verletzung, Anzahl der Betroffenen bzw. der Datensätze, Maßnahmen, wahrscheinliche Folgen, Dokumentation etc.) der Datenschutzbehörde zu übermitteln. Die Datenschutzbehörde stellt auf ihrer Website ein Musterformular für Meldungen bereit[98].

- ***Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person (Art. 34 DSGVO)***

Ein Verantwortlicher hat Betroffene über die von ihm verursachten Datenschutzverletzungen zu benachrichtigen, wenn ein hohes Risiko für Rechte und Freiheiten der Betroffenen besteht; dies ohne ungebührliche Verzögerung (Ausnahmen sind hier möglich).

- ***Datenschutz-Folgenabschätzung (Art. 35 DSGVO)***

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen.

Eine Datenschutz-Folgenabschätzung ist insbesondere in folgenden Fällen erforderlich:

[98] Abrufbar unter https://www.dsb.gv.at/dokumente

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO oder
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Die Datenschutzbehörde hat eine Liste der Verarbeitungsvorgänge zu erstellen und zu veröffentlichen, für die eine Datenschutz-Folgenabschätzung jedenfalls durchzuführen ist (siehe dazu die Datenschutz-Folgenabschätzungs-Verordnung – DSFA-V, BGBl. II Nr. 278/2018). Sie hat auch eine Liste der Verarbeitungsvorgänge, bei denen keine Datenschutz-Folgenabschätzung durchzuführen ist, veröffentlicht (die Datenschutz-Folgenabschätzung-Ausnahmenverordnung - DSFA-AV, BGBl. II Nr. 108/2018[99]). Auch Rechtsvorschriften können eine verpflichtende Datenschutz-Folgenabschätzung vorsehen.

Die Datenschutz-Folgenabschätzung hat zumindest zu enthalten:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass

[99] Abrufbar unter https://www.dsb.gv.at/verordnungen-in-osterreich.

diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Datenschutz-Folgenabschätzung vorgenommen werden.

Hinweis:

- In den Leitlinien der Art. 29-Gruppe zur Datenschutz-Folgenabschätzung[100] werden neun Kriterien angeführt, die für die Durchführung einer Datenschutz-Folgenabschätzung ausschlaggebend sein können.
- In der genannten Leitlinie finden sich Hinweise auf bereits etablierte Verfahren für Datenschutz-Folgenabschätzungen.
- Für bereits existierende Verarbeitungsvorgänge (Datenanwendungen) ist grundsätzlich keine Datenschutz-Folgenabschätzung durchzuführen, wenn diese Verarbeitungsvorgänge durch die Datenschutzbehörde bereits zu einem früheren Zeitpunkt im Zuge einer DVR-Registrierung im Rahmen eines Vorabkontrollverfahrens gemäß § 18 Datenschutzgesetz 2000 (DSG 2000) genehmigt wurden. Bei der automatischen Registrierung über DVR-Online oder in Fällen, in denen die Datenschutzbehörde eine Datenanwendung registriert hat, jedoch tatsächlich kein Fall der Vorabkontrolle vorgelegen ist (das betrifft nichtvorabkontrollpflichtige Meldungen vor dem 1. September 2012 oder Meldungen, bei denen der Auftraggeber irrtümlicherweise das Vorhandensein der Vorabkontrolle angekreuzt hat), kommt dies hingegen nicht in Betracht.
- Kommt es zu einer Änderung bestehender Verarbeitungsvorgänge, ist jedoch sehr wohl eine Datenschutz-Folgenabschätzung durchzuführen, wenn die Voraussetzungen des Art. 35 Abs. 1 DSGVO zutreffen. Generell wird empfohlen, bereits existierende Datenverarbeitungsvorgänge einer regelmäßigen Evaluierung zu unterziehen, ob sich Voraussetzungen geändert haben. Bejahendenfalls wäre - bei Vorliegen aller Voraussetzungen - eine Datenschutz-Folgenabschätzung

[100] Abrufbar unter https://www.dsb.gv.at/dam/jcr:ba295358-cf65-41a6-911d-a88cae94ba20/Leitlinien%20zur%20Datenschutz-Folgenabschaetzung-wp248-rev-01_de.pdf.
Diese Leitlinien wurden vom EDSA ausdrücklich übernommen:
https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

durchzuführen. Überdies wird empfohlen, auch zu dokumentieren, aus welchen Gründen keine Datenschutz-Folgenabschätzung durchgeführt wurde.

- Die Datenschutz-Folgenabschätzung kann in jeder Sprache durchgeführt und intern schriftlich festgehalten werden. Kommt es jedoch zu einer Vorlage an die Datenschutzbehörde (bspw. bei einem Konsultationsverfahren), ist die Datenschutz-Folgenabschätzung zwingend in Deutsch vorzulegen, da die Datenschutzbehörde fremdsprachige Dokumente in ihren Verfahren nicht berücksichtigen kann.

- ***Vorherige Konsultation (Art. 36 DSGVO)***

Der Verantwortliche hat vor Beginn der Verarbeitung die Datenschutzbehörde zu konsultieren, wenn aus einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

Sollte die Datenschutzbehörde zur Auffassung gelangen, dass die geplante Verarbeitung nicht im Einklang mit der DSGVO stünde, insbesondere, weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, unterbreitet sie dem Verantwortlichen (und gegebenenfalls dem Auftragsverarbeiter) entsprechende schriftliche Empfehlungen und kann ihre in Art. 58 DSGVO genannten Befugnisse ausüben.

Der Verantwortliche hat der Datenschutzbehörde im Rahmen einer Konsultation folgende Informationen zur Verfügung zu stellen:

- gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen;
- die Zwecke und die Mittel der beabsichtigten Verarbeitung;
- die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß der DSGVO vorgesehenen Maßnahmen und Garantien;
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
- die Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und
- alle sonstigen von der Aufsichtsbehörde angeforderten Informationen.

Darüber hinaus können Verantwortliche durch Rechtsvorschriften verpflichtet werden, bei der Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, einschließlich der Verarbeitung zu Zwecken der sozialen Sicherheit und der öffentlichen Gesundheit, die Aufsichtsbehörde zu konsultieren und deren vorherige Genehmigung einzuholen.

- ***Benennung eines Datenschutzbeauftragten (Art. 37 DSGVO)***

Der Verantwortliche und der Auftragsverarbeiter haben einen Datenschutzbeauftragten zu benennen, wenn:

- die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln;
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO besteht.

Andere Verantwortliche oder Auftragsverarbeiter können einen Datenschutzbeauftragten auf freiwilliger Basis bestellen. Eine Gruppe von Unternehmen bzw. öffentlichen Einrichtungen kann einen gemeinsamen Datenschutzbeauftragten benennen. Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen und der Datenschutzbehörde mitzuteilen.

Brauche ich einen Datenschutzbeauftragten?

Ob Sie einen Datenschutzbeauftragten „brauchen“, müssen Sie zunächst selbst entscheiden. Für die Mehrheit der Unternehmen wird die Bestellung grundsätzlich optional sein. Zwingend aufgrund der DSGVO zu bestellen ist ein Datenschutzbeauftragter nur von Behörden bzw. öffentlichen Stellen (mit Ausnahme von Gerichten, sofern sie nicht im Rahmen der Justizverwaltung handeln) und bei Unternehmen, die schwerpunktmäßig in einem spezifischen Geschäftsbereich tätig sind. Die entsprechenden Regelungen finden Sie in Art. 37 DSGVO.

Wann ist ein Datenschutzbeauftragter verpflichtend (in meinem Unternehmen) zu bestellen?

Der Verantwortliche bzw. Auftragsverarbeiter muss einen Datenschutzbeauftragten bestellen, wenn

a. die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder

b. die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten (gemäß Art. 9 DSGVO) oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (gemäß Art. 10 DSGVO) besteht.

Welche Stellung[101] hat der Datenschutzbeauftragte und muss dieser zwingend ein Arbeitnehmer sein?

Die Stellung des Datenschutzbeauftragten ist in Art. 38 DSGVO näher geregelt. Demnach erhält der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen und darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene. Ferner müssen der Verantwortliche und der Auftragsverarbeiter den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben unterstützen und ihm die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen zur Verfügung stellen.

Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen (Art. 37 Abs. 6 DSGVO).

Für **Bundesministerien und diesen nachgeordneten Dienststellen bzw. Einrichtungen** sieht § 5 DSG vor, dass der Datenschutzbeauftragte dem Dienststand des jeweiligen Ministeriums bzw. der Dienststelle oder Einrichtung anzugehören hat.

---

[101] Siehe dazu auch die Leitlinien in Bezug auf Datenschutzbeauftrage, abrufbar unter https://www.dsb.gv.at/dam/jcr:a279307b-ce48-416e-9c28-5bae42e0038c/Leitlinien_in_Bezug_auf_Datenschutzbeauftragte.pdf. Diese Leitlinien wurden vom EDSA ausdrücklich übernommen: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

Sozialversicherungsträger bzw. Selbstverwaltungskörper, bei denen lediglich ein Aufsichtsrecht des Bundes besteht, fallen nicht unter § 5 DSG.

Kann ein Datenschutzbeauftragter verantwortlicher Beauftragter nach § 9 VStG sein?

Der **Datenschutzbeauftragte** hat nach Ansicht der Datenschutzbehörde **beratende Funktion**. Verbindliche Anordnungen sind von der Managementebene zu treffen. Deshalb ist die Datenschutzbehörde der Ansicht, dass ein Datenschutzbeauftragter **nicht** als verantwortlicher Beauftragter bestellt werden kann.

Braucht der Datenschutzbeauftragte eine bestimmte (akademische) Ausbildung?

Nein. Gemäß Art. 37 Abs. 5 DSGVO wird der Datenschutzbeauftragte auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf Grundlage seiner Fähigkeit zur Erfüllung der Aufgaben des Datenschutzbeauftragten gemäß Art. 39 DSGVO.

Brauchen politische Parteien und Gewerkschaften einen Datenschutzbeauftragten?

Ja. Politische Parteien und Gewerkschaften fallen zwar nicht unter den Begriff der „öffentlichen Stelle“, jedoch besteht deren Kerntätigkeit in der umfangreichen Verarbeitung sensibler Daten nach Art. 9 DSGVO (hier: politische Meinung und Gewerkschaftszugehörigkeit, eventuell auch religiöse oder weltanschauliche Überzeugungen).

Braucht ein einzelner Arzt oder ein einzelner Rechtsanwalt einen Datenschutzbeauftragten?

Nein. Eine umfangreiche Verarbeitung sensibler Daten oder von Strafdaten an sich wäre zwar Voraussetzung für die Notwendigkeit der Bestellung eines Datenschutzbeauftragten, die DSGVO sieht in diesem Punkt jedoch Erleichterungen für den einzelnen Arzt oder Rechtsanwalt vor. Nach Erwägungsgrund 91 sollte die Verarbeitung personenbezogener Daten **nicht als umfangreich** gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt.

Was sind Verhaltensregeln?

Gemäß Art. 40 DSGVO legen Verhaltensregeln die Rechtslage inhaltsspezifisch näher aus, indem sie die Anwendung der DSGVO in gewissen Bereichen präzisieren. Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, können solche Verhaltensregeln ausarbeiten und der Aufsichtsbehörde zur Genehmigung vorlegen. Mit der Überwachung der Einhaltung von genehmigten Verhaltensregeln ist eine von der Aufsichtsbehörde dafür akkreditierte Stelle zu betrauen. Die Einhaltung der Verhaltensregeln gemäß Art. 40 DSGVO kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen oder Auftragsverarbeiters nachzuweisen.

Die Datenschutzbehörde hat bereits Verhaltensregeln genehmigt und stellt allgemeine Hinweise für Verhaltensregeln auf ihrer Website bereit.[102]

Was ist eine Zertifizierung und wer führt sie durch?

Datenschutzspezifische Zertifizierungsverfahren, Datenschutzsiegel und Datenschutzprüfzeichen dienen dem Nachweis der faktischen Einhaltung von Vorgaben der DSGVO bei bestimmten Verarbeitungsvorgängen. Eine Zertifizierung wird durch die Datenschutzbehörde oder von ihr eigens dazu akkreditierten Stellen auf Grundlage der Zertifizierungskriterien eines genehmigten Zertifizierungsverfahrens erteilt. Die maximale Gültigkeit einer Zertifizierung beträgt drei Jahre, eine (mehrfache) Verlängerung um je maximal drei Jahre ist möglich.

Was bedeutet die DSGVO für die Inanspruchnahme von Cloud-Services?

Die meisten Cloud-Dienste (insb. Speicherung) sind eine Form von Auftragsverarbeitung. Es ist zu beachten, dass durch die Inanspruchnahme von Cloud-Services ggf. eine Datenübermittlung in ein Drittland stattfindet, für die es eine gesonderte Rechtsgrundlage braucht (bspw. Standarddatenschutzklauseln). Wird ein Cloud-Diensteanbieter in Anspruch genommen, so muss eine sichere Datenverarbeitung durch diesen gewährleistet sein. Kommt es zu einer Verletzung des Schutzes personenbezogener Daten in der Cloud (bspw. durch einen Hackerangriff o.ä.) trägt die datenschutzrechtliche Verantwortung (einschließlich

[102] Siehe dazu https://www.dsb.gv.at/aufgaben-taetigkeiten/genehmigung-von-verhaltensregeln.html.

schadenersatzrechtlicher Ansprüche) nach außen hin der Verantwortliche (d.h. jene Person/jene Einrichtung, die Cloud-Services in Anspruch nimmt).

Wofür muss ich haften?

Jede (natürliche) Person, der durch einen Verstoß gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Dabei haftet jeder Verantwortliche der an der Verarbeitung beteiligt war zur Gänze. Der Auftragsverarbeiter haftet, sofern er seine speziellen Pflichten nicht erfüllt oder die Anweisungen des Verantwortlichen nicht (zur Gänze) befolgt hat. Im Innenverhältnis kann sich der Beanspruchte im Verhältnis der Verantwortlichkeit an anderen Beteiligten regressieren.

Damit soll ein wirksamer Rechtsschutz gewährleistet werden.

Keine Haftung tritt ein, wenn weder der Verantwortlicher noch der Auftraggeber für den Umstand durch welchen der Schaden eingetreten ist, verantwortlich ist.

Wie ist die Rechtslage bei Vereinen?

Die DSGVO nimmt auf bestimmte Rechts- und Organisationsformen wenig Bezug. Vereine, die personenbezogene Daten verarbeiten, sind Verantwortliche.

Die Datenschutz-Folgenabschätzung-Ausnahmenverordnung (DSFA-AV), BGBl. II Nr. 108/2018, nimmt die Mitgliederverwaltung von Vereinen und Personengemeinschaften (DSFA-A03 Mitgliederverwaltung) aus. Diese Ausnahme ist aber auf die Führung von Mitgliederverzeichnissen, Evidenz der Mitglieds- und Förderungsbeiträge und den Verkehr mit Mitgliedern oder Förderern begrenzt.

Bei Vereinen mit religiösem, ethnischem oder sonst weltanschaulichem Hintergrund können besondere Kategorien personenbezogener Daten verarbeitet werden. Gemäß Art. 9 Abs. 2 lit. d DSGVO dürfen solche Daten durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht verarbeitet werden:

- auf der Grundlage geeigneter Garantien;
- im Rahmen ihrer rechtmäßigen Tätigkeiten;

- unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und
- die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden.

Die sonstigen Bestimmungen der DSGVO gelten auch für Vereine uneingeschränkt (v.a. die Pflicht zur Information von Betroffenen nach Art. 13 DSGVO sowie die Führung eines Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 DSGVO).

Wie lange darf ich Daten speichern?

In einigen Fällen gibt es gesetzliche Fristen, innerhalb derer Daten aufzubewahren sind (z.B. 7 Jahre gemäß § 132 der Bundesabgabenordnung – BAO).

Ist keine gesetzliche Frist vorgesehen, obliegt es dem/der Verantwortlichen **eigenständig** festzulegen, wie lange Daten gespeichert werden (siehe dazu bspw. § 51 Abs. 3 Ärztegesetz).

Dabei können folgende Faktoren ausschlaggebend sein:

- anhängige oder konkret drohende Rechtsstreitigkeit (die bloße Annahme, es könnte zu Klagen kommen, reicht nicht)
- Zeit, die seit der Datenermittlung verstrichen ist (je älter die Daten desto weniger Relevanz haben sie)
- Daten sind zur Erfüllung eines Vertrags (nicht mehr) erforderlich (z.B. Versicherungsvertrag)

Unzulässig ist eine **pauschale** (d.h. nicht näher begründete) Aufbewahrungsdauer für zumindest 30 Jahre (allgemeine Verjährungsfrist nach dem Allgemeinen bürgerlichen Gesetzbuch – ABGB zur Geltendmachung bestimmter Rechte).

Darf ich Nachrichten/Dokumente nur mehr verschlüsselt elektronisch versenden?

Die DSGVO sieht nicht vor, dass Nachrichten/Dokumente jedenfalls nur in verschlüsselter Form elektronisch versendet werden dürfen (bspw. durch verschlüsselte Mails).

Ein verschlüsselter Versand kann aber – abhängig von den jeweiligen Umständen (Datenart, Verarbeitungszwecke, Verlässlichkeit des Systems) – empfehlenswert sein.

Wichtig: Von Betroffenen kann mittels Einwilligungserklärung nicht rechtswirksam verlangt werden, dass sie bestimmten Übermittlungsarten zustimmen (bspw. Übermittlung via Messengerdiensten oder E-Mail).

Darf ich eine Videoüberwachung/Bildverarbeitung betreiben?

Nähere Informationen dazu finden Sie unter https://www.dsb.gv.at/fragen-und-antworten > Videoüberwachung durch Private (einschließlich der Privatwirtschaftsverwaltung durch die öffentliche Hand).

d) Internationaler Datentransfer an Empfänger in einem Drittstaat oder in einer internationalen Organisation

Was ist bei Übermittlungen von Daten an Empfänger in einem Drittstaat oder in einer internationalen Organisation zu beachten? Was passiert mit bisherigen Genehmigungen?

Durch die DSGVO erfolgt eine weitreichende Genehmigungsfreiheit im internationalen Datenverkehr (Art. 44-50 DSGVO). Es ist darauf zu achten, dass alle Verarbeitungsvorgänge zuerst im Inland zulässig sind, bevor ein Datenexport zulässig ist (sog. „Zwei-Stufen-Prüfung“).

Die bereits unter der RL 95/46/EG bekannten rechtlichen Instrumente für den Datenexport sind erhalten geblieben und werden durch zum Teil neue Möglichkeiten ergänzt:

Personenbezogene Daten dürfen an Empfänger in einem Drittland oder in einer internationalen Organisation übermittelt werden, wenn dort ein angemessenes Schutzniveau festgestellt wurde (Art. 45 DSGVO). Die Feststellung erfolgt durch die Europäische Kommission, ihre Angemessenheitsbeschlüsse werden veröffentlicht.[103]

[103] Eine Übersicht samt weiteren Informationen zu den Angemessenheitsbeschlüssen nach Art 45 DSGVO findet sich in Englisch unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Weiters ist die Übermittlung zulässig, wenn zwischen dem Datenexporteur und dem Datenimporteur eine vertragliche Vereinbarung unter Verwendung von Standarddatenschutzklauseln abgeschlossen wurde oder verbindliche interne Datenschutzvorschriften (Binding Corporate Rules, BCRs) bestehen. Diese Instrumente gab es schon unter der RL 95/46/EG, wenngleich die verbindlichen internen Datenschutzvorschriften erst mit der DSGVO ausdrücklich kodifiziert sind. Zu den neuen rechtlichen Instrumenten gehören Verhaltensregeln (Art. 40 DSGVO) und Zertifizierungsmechanismen (Art. 42 DSGVO). Art. 46 Abs. 3 DSGVO enthält die Möglichkeit, für weitere Instrumente (z.B. individuelle Vertragsklauseln) eine Genehmigung durch die Aufsichtsbehörde einzuholen, wobei hierbei zu beachten ist, dass für solche Fälle im Grundsatz das Kohärenzverfahren gemäß Art. 63 DSGVO (d.h. insbesondere die Einbindung der Europäischen Kommission und des Europäischen Datenschutzausschusses) anzuwenden ist.

Art. 49 DSGVO enthält einige Ausnahmentatbestände für Sonderfälle, von denen einige mit den Regeln im vorherigen § 12 DSG 2000 übereinstimmen (Zustimmung, Vertragserfüllung, öffentliches Interesse, Verteidigung von Rechtsansprüchen, lebenswichtige Interessen) und einige, die neu dazugekommen sind (Übermittlung eines Auszugs aus einem öffentlichen Register). Bei all diesen Ausnahmen ist jedoch eine restriktive Anwendung geboten.

ACHTUNG: Es gibt Leitlinien des EDSA zu Art. 49 DSGVO![104]

Die DSGVO bringt weniger Behördenwege und mehr Verantwortung für den datenschutzrechtlich Verantwortlichen. Es ist insbesondere erforderlich, die eigenen Datenverarbeitungen sowie deren Zwecke zu kennen und (sofern für das betreffende Drittland kein Angemessenheitsbeschluss der Europäischen Kommission besteht) selbst zu entscheiden, welche rechtlichen Instrumente bzw. geeigneten Garantien (samt allfälligen zusätzlichen Maßnahmen) für einen Datentransfer an Empfänger in einem Drittstaat oder in einer internationalen Organisation geboten sind.[105]

---

[104] abrufbar in Deutsch unter https://www.dsb.gv.at/dam/jcr:db22aec8-5c71-4ae4-9c30-b06d07f79335/Leitlinien2-2018%20zu%20den%20Ausnahmen%20nach%20Artikel49%20der%20Verordnung2016-679.pdf.

[105] Vgl. dazu EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0

Es bestehen auch Informationspflichten an Betroffene, wenn Daten in einen Drittstaat oder in eine internationale Organisation übermittelt werden sollen (Art. 13 Abs. 1 lit. f und 14 Abs. 1 lit. f DSGVO).

Bereits erteilte Genehmigungen bleiben grundsätzlich gültig (Art. 46 Abs. 5 erster Satz DSGVO).

ACHTUNG: Der sog. „Privacy-Shield-Beschluss“ wurde durch die Entscheidung des EuGH vom 16.07.2020, C-311/18 für **ungültig** erklärt. Der EuGH begründete seine Entscheidung im Wesentlichen damit, dass durch die U.S.-amerikanische Rechtsordnung kein der Sache nach gleichwertiges Schutzniveau normiert wird.[106]

HINWEIS ZU STANDARDDATENSCHUTZKLAUSELN: Die Europäische Kommission hat mit dem Durchführungsbeschluss (EU) 2021/914 „neue“ Standarddatenschutzklauseln erlassen. Die von der Europäischen Kommission unter der DSRL erlassenen Klauselwerke können nur mehr bis zum 27. Dezember 2022 herangezogen werden und verlieren danach ihre Gültigkeit.

Gilt die DSGVO auch für internationale Organisationen wie bspw. die UNO, die OSZE u.a.?

Es hängt in erster Linie vom Abkommen ab, dass die internationale Organisation mit dem jeweiligen (europäischen) Sitzstaat abschließt (Sitzstaatsabkommen = völkerrechtlicher Vertrag). In den meisten Fällen verpflichten sich die internationalen Organisationen die Gesetze des Sitzlandes – und damit auch die DSGVO – zu beachten. Allerdings enthalten die Abkommen in der Regel Bestimmungen über Privilegien und Immunitäten von internationalen Organisationen und deren Bediensteten, wie insbesondere die Unverletzlichkeit des Amtssitzes, die Immunität vor staatlicher Verfolgung (d.h. auch vor Verfahrenshandlungen der Datenschutz-Aufsichtsbehörden), etc..

---

vom 18. Juni 2021, abrufbar in deutscher Sprache unter https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_de.pdf.

[106] Für ausführliche Informationen hierzu siehe die FAQs des EDSA in Englisch unter https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf.

e) Brexit

Welche Auswirkungen hat der sog. „Brexit“ auf die Übermittlung personenbezogener Daten an Empfänger im Vereinigten Königreich?

Das Vereinigte Königreich stimmte am 23. Juni 2016 im Rahmen eines Referendums für den **Austritt aus der Europäischen Union** und verließ diese mit Ablauf des 31. Jänners 2020. Zuvor wurde ein **Austrittsabkommen**[107] unterzeichnet, welches mit 1. Februar 2020 in Kraft getreten ist und wesentliche Aspekte des Austritts des Vereinigten Königreichs aus der Europäischen Union und der Europäischen Atomgemeinschaft regelt.

Das Austrittsabkommen sah bis zum 31. Dezember 2020 einen Übergangszeitraum („transition period“) vor, in welchem das Unionsrecht (und folglich auch die DSGVO) für das Vereinigte Königreich sowie im Vereinigten Königreich grundsätzlich weitergalt. In diesem Zeitraum ergaben sich daher noch keine unmittelbaren Folgen für den Datentransfer.

Kurz vor Ende des Übergangszeitraums wurde zwischen der Europäischen Union und dem Vereinigten Königreich ein **Handels- und Kooperationsabkommen**[108] ausverhandelt, welches seit dem 1. Jänner 2021 vorläufig angewendet und am 1. Mai 2021 endgültig in Kraft getreten ist.

In Bezug auf das Datenschutzrecht enthält das Handels- und Kooperationsabkommen eine weitere **Überbrückungslösung**, gemäß welcher die Übermittlung personenbezogener Daten aus der Europäischen Union an Empfänger im Vereinigten Königreich in einem **Zeitraum von maximal sechs Monaten nach seinem Inkrafttreten nicht als Übermittlung an ein Drittland im Sinne des Unionsrechts gilt**. Bedingung hierfür ist, dass sich das derzeit im Vereinigten Königreich geltende Datenschutzrecht in jenem Zeitraum nicht ändert und das Vereinigte Königreich in diesem Zeitraum keine seiner neuen Befugnisse in diesem Bereich ausübt.

Die **Überbrückungslösung endete mit Ablauf des 30. Juni 2021**.

---

[107] Abkommen über den Austritt des Vereinigten Königreichs Großbritannien und Nordirland aus der Europäischen Union und der Europäischen Atomgemeinschaft, ABl. L 2020/29, S. 7 idF. L 2020/443, S. 3.

[108] Handels- und Kooperationsabkommen zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits, ABl. L 2020/444, S. 14.

Die Europäische Kommission hat zuvor jedoch **zwei Angemessenheitsbeschlüsse** (jeweils einen für den Bereich DSGVO und einen für den Bereich DSRL-PJ) für das Vereinigte Königreich erlassen, welche **am 28. Juni 2021 in Kraft getreten** sind. Die Europäische Kommission hat dem Vereinigten Königreich im Grundsatz ein dem Wesen nach **gleichwertiges Schutzniveau** wie in der Europäischen Union **bescheinigt**. Personenbezogene Daten können somit auf Grundlage dieser beiden Angemessenheitsbeschlüsse **ungehindert** aus der Europäischen Union an Empfänger im Vereinigten Königreich übermittelt werden.

Zu beachten ist jedoch, dass Datenübermittlungen, welche zu Zwecken der vom Vereinigten Königreich praktizierten Einwanderungskontrolle erfolgen, derzeit vom sachlichen Geltungsbereich des Angemessenheitsbeschlusses für den Bereich DSGVO ausgenommen sind!

Beide Angemessenheitsbeschlüsse sind zudem zeitlich befristet und laufen vier Jahre nach ihrem Inkrafttreten aus. Die Europäische Kommission wird während der Vierjahresperiode die Rechtslage im Vereinigten Königreich überwachen und kann im Falle von Veränderungen betreffend das Schutzniveau im Vereinigten Königreich jederzeit eingreifen und die Angemessenheitsbeschlüsse im Bedarfsfall aussetzen, ändern, oder aufheben. Die Geltungsdauer der beiden Angemessenheitsbeschlüsse kann von der Europäischen Kommission auch verlängert werden.

f) Verfahren vor der Datenschutzbehörde

In welcher Sprache kann ich Dokumente an die Datenschutzbehörde vorlegen bzw. in welcher Sprache werden Verfahren geführt?

Alle Unterlagen, die der Verantwortliche/der Auftragsverarbeiter oder der Beschwerdeführer der Datenschutzbehörde im Rahmen eines Verfahrens vorzulegen hat, müssen **in deutscher Sprache** (Amtssprache gemäß Art. 8 Abs. 1 Bundes-Verfassungsgesetz; siehe dazu auch das Erkenntnis des Verwaltungsgerichtshofes vom 17. Mai 2011, Zl. 2007/01/0389) abgefasst sein. Ist dies nicht der Fall, ist die Datenschutzbehörde nicht verpflichtet, diese Dokumente zu akzeptieren. Beschwerden, die in einer anderen als der deutschen Sprache eingebracht werden, werden nach erfolgloser Mangelbehebung zurückgewiesen (vgl. dazu den Bescheid vom 21.09.2018, GZ DSB-D130.092/0002-DSB/2018).

Die Verpflichtung zur Vorlage deutschsprachiger Dokumente gilt **jedenfalls** für die **Datenschutz-Folgenabschätzung** gem. Art. 35 DSGVO, die der Datenschutzbehörde etwa im Rahmen der „Konsultation“ gem. Art. 36 DSGVO vorgelegt werden muss, sowie für das **Verzeichnis von Verarbeitungstätigkeiten** gem. Art. 30 DSGVO, das in der Regel die Basis für die Datenschutz-Folgenabschätzung sein wird.

Welche Geldbußen kann die Aufsichtsbehörde verhängen und wofür?

Die DSGVO sieht Geldbußen vor. Die Geldbußen sind von der Datenschutzbehörde als Verwaltungsstrafen gegen Unternehmen (Unternehmensträger) oder Einzelpersonen zu verhängen, die jeweils als für eine Datenverarbeitung Verantwortlicher oder Auftragsverarbeiter agieren. Die Zahl der strafbaren Verhaltensweisen (Verstöße) wurde ausgedehnt. Auch Fahrlässigkeit ist strafbar.

Die in der DSGVO vorgesehenen hohen Geldbußen sollen eine Möglichkeit schaffen, auch sehr umsatzstarke Akteure in die Schranken zu weisen. Die Datenschutzbehörde wird ihre Sanktionsmöglichkeiten nach dem Gebot der Verhältnismäßigkeit einsetzen.

In bestimmten Fällen kann die Datenschutzbehörde an Stelle der Verhängung einer Geldbuße auch eine förmliche Verwarnung aussprechen. Dies erfolgt allerdings nur in jenen Fällen, in denen die Rechtsverletzung nicht als besonders schwerwiegend zu werten ist.

ACHTUNG: Es gibt kein Recht darauf, dass die Datenschutzbehörde bei einem erstmaligen Verstoß nur verwarnt!

Für weniger schwere Verstöße gegen Bestimmungen der DSGVO droht eine Geldbuße in Höhe bis zu 10 Millionen Euro (keine Mindeststrafe) oder bei Unternehmen bis zu 2 Prozent des weltweiten Jahresumsatzes des letzten Geschäftsjahrs. Es gilt der höhere Betrag.

Für schwerwiegende Verstöße gegen Bestimmungen der DSGVO droht eine Geldbuße in Höhe bis zu 20 Millionen Euro (keine Mindeststrafe) oder bei Unternehmen bis zu 4 Prozent des weltweiten Jahresumsatzes des letzten Geschäftsjahrs. Es gilt der höhere Betrag.

Einige Beispiele:

Verstoß/Übertretung	Höchstbuße	bisher (max. Geldstrafe)

Missachtung Bescheid d. DSB	€ 20.000.000,-- oder 4 % v.Ums.	€ 25.000,--
Verletzung des Auskunftsrechts	€ 20.000.000,-- oder 4 % v.Ums.	€ 500,--
Verletzung der Löschungsrechts	€ 20.000.000,-- oder 4 % v.Ums.	€ 500,--
unrechtmäßige Datenspeicherung	€ 20.000.000,-- oder 4 % v.Ums.	nicht strafbar
unzulässige Auslandsübermittlung	€ 20.000.000,-- oder 4 % v.Ums.	€ 10.000,--
fehlender Datenschutzbeauftragter	€ 10.000.000,-- oder 2 % v.Ums.	nicht strafbar
Nichtvornahme DSFA/DPIA	€ 10.000.000,-- oder 2 % v.Ums.	nicht strafbar
mangelhafte Datensicherheit	€ 10.000.000,-- oder 2 % v.Ums.	€ 10.000,--
kein Verarbeitungsverzeichnis	€ 10.000.000,-- oder 2 % v.Ums.	€ 10.000,-- (Meldepflicht)
fehlende Elternzustimmung	€ 10.000.000,-- oder 2 % v.Ums.	nicht strafbar
Nicht-Kooperation mit DSB	€ 10.000.000,-- oder 2 % v.Ums.	nicht strafbar

Gegen die Verhängung einer Geldbuße kann Beschwerde an das Bundesverwaltungsgericht erhoben werden.

Habe ich als Kleinunternehmen mit einer Geldbuße von 20 Millionen Euro zu rechnen?

Nein. Grundlage für die Festsetzung der Höhe der Geldbuße ist der konkrete Verstoß sowie die wirtschaftliche Leistungsfähigkeit des Verantwortlichen. Jede Strafe muss wirksam, **verhältnismäßig** und abschreckend sein.

Welche Befugnisse hat die Datenschutzbehörde?

Die Aufsichtsbehörde hat drei Arten von Befugnissen:

- Untersuchungsbefugnisse (einschließlich des Betretungsrechts bestimmter Räumlichkeiten nach Vorankündigung)
- Abhilfebefugnisse (das sind Befugnisse, die es der Aufsichtsbehörde ermöglichen, ein rechtswidriges Verhalten abzustellen, bspw. durch konkrete Anordnungen oder die Verhängung von Geldbußen iHv bis zu 20 Millionen Euro oder 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres)
- Genehmigungs- und Beratungsbefugnisse

Ist die DSB für das Parlament (Nationalrat, Bundesrat, Landtage) zuständig?

Im Regelfall ist keine Zuständigkeit gegeben. Aufgrund der Gewaltentrennung kann es keine Aufsicht einer Verwaltungsbehörde über die Gesetzgebung geben.

In **Ausnahmefällen**, v.a. wenn die Organe des Parlaments als Verwaltungsorgane handeln (z.B. bei der Verwaltung der eigenen Bediensteten), kann eine Zuständigkeit der DSB vorliegen.

13) Weiterführende Literatur

Stand: September 2022 (alphabetische, nicht vollständige Aufzählung)

DSGVO:

- *Ehmann/Selmayr* (Hrsg.), Datenschutz-Grundverordnung: DS-GVO[2] (Kommentar)
- *Feiler/Forgó*, EU-Datenschutz-Grundverordnung (Kommentar)
- *Gantschacher/Jelinek/Schmidl/Spanberger* (Hrsg.), Kommentar zur Datenschutz-Grundverordnung
- *Gola* (Hrsg.), Datenschutz-Grundverordnung[2] (Kommentar)
- *Jahnel* (Hrsg.), Datenschutz-Grundverordnung (Kommentar)
- *Kühling/Buchner* (Hrsg.), Datenschutz-Grundverordnung[3] (Kommentar)
- *Knyrim* (Hrsg.), Praxishandbuch Datenschutzrecht[4] (Praxishandbuch)
- *Knyrim* (Hrsg.), Datenschutz-Grundverordnung (Praxishandbuch)
- *Paal/Pauly* (Hrsg.), Datenschutz-Grundverordnung[3] (Kommentar)
- *Pollirer/Weiss/Knyrim/Haidinger*, DSGVO (Textausgabe)
- *Simitis/Hornung/Spieker* (Hrsg.), Datenschutzrecht (Großkommentar)
- *Sydow* (Hrsg.), Europäische Datenschutzgrundverordnung[2] (Kommentar)

DSG:

- *Bergauer/Jahnel*, DSGVO und DSG[3] (Textausgabe)
- *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, DSG (Kommentar)
- *Jelinek/Schmidl/Spanberger*, Datenschutzgesetz (Kommentar)
- *Pollirer/Weiss/Knyrim/Haidinger*, DSG[4] (Textausgabe mit Erläuterungen)
- *Thiele/Wagner*, DSG (Kommentar)