Republik Österreich
Datenschutz
behörde

Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung

Leitfaden

Zusammengestellt von Dr. Matthias Schmidl

Stand: Juli 2017

Inhalt

Vorwort 3
Einleitung 4
1) Struktur der DSGVO 5
2) Kapitel I 6
3) Kapitel II 8
4) Kapitel III 10
5) Kapitel IV 11
6) Kapitel V 13
7) Kapitel VI 14
8) Kapitel VII 15
9) Kapitel VIII 16
10) Kapitel IX bis XI 18
11) Das österreichische Datenschutz-Anpassungsgesetz 2018 19
12) Häufig gestellte Fragen 22
13) Weiterführende Literatur 38

Vorwort

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

Es handelt sich **um keine abschließende Information**. Eine Beratung durch spezialisierte Einrichtungen 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 MA zum derzeitigen Zeitpunkt wieder.

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

Einleitung

Die DSGVO (Verordnung (EU) 2016/679) wurde am 04.05.2016 im ABl. Nr. L119 S. 1 kundgemacht, trat am 20. Tag nach ihrer Veröffentlichung in Kraft und gilt ab dem 25.05.2018.

Sie hebt die DSRL auf und wird ab Mai 2018 das Rückgrat des allgemeinen Datenschutzes der EU bilden.

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 wird daher neben der DSGVO in Österreich weiterhin ein nationales Datenschutzgesetz geben.

Zielsetzungen der DSGVO sind

- einheitlicher Rechtsschutz für alle Betroffenen in der EU
- einheitliche Regeln für die Datenverarbeitung innerhalb der EU
- 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“.

Im Folgenden wurden 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** 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[1]

Räumlicher Anwendungsbereich (Art. 3):

Wie bereits die Datenschutz-Richtlinie – (DSRL) knüpft die DSGVO primär an die Datenverwendung im Rahmen einer **Niederlassung** eines Verantwortlichen oder eines Auftragsverarbeiters an[2]; 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

[1] 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. Sie ist bis zum 06.05.2018 in nationales Recht umzusetzen.

[2] 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.

- 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)
- 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[3] 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.[4]

Art. 7 legt die Bedingungen für die Einwilligung fest (und zwar detaillierter als es bisher die DSRL tat)[5], 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.

Art. 9 enthält – ebenso wie bereits Art. 8 der DSRL – die Voraussetzungen für die Verwendung sensibler Daten.

Art. 10 legt fest, unter welchen Voraussetzungen personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten verarbeitet werden dürfen.[6]

---

[3] Vgl. dazu zuletzt das Urteil vom 19.10.2016, C-582/14, Breyer.
[4] 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.
[5] 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.
[6] Diese „Strafdaten" gelten per definitionem nicht als sensible Daten. Sie unterliegen in Österreich aber bereits jetzt einem speziellen Schutz; vgl. dazu § 8 Abs. 4 DSG 2000 sowie die Rsp des VwGH dazu (Erkenntnis vom 22.10.2012, Zl. 2009/03/0162).

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).

4) Kapitel III

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

Die Art. 13 und 14 – wie bereits schon Art. 10 und 11 der DSRL – legen die Informationspflichten 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.[7]

Neben den schon bisher bekannten Rechten auf **Auskunft** (Art. 15), **Berichtigung** (Art. 16), **Löschung** (Art. 17; ausweitet zum „Recht auf Vergessenwerden“) und **Widerspruch** (Art. 21)[8] 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[9]. 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 ohne technische Barrieren für die Betroffenen in eine neue technische Umgebung übertragen werden können.

Art. 23 ermächtigt die Union und die Mitgliedstaaten, die in den Art. 12 bis 22 und Art. 34 und 5 normierten Rechte und Pflichten unter bestimmten Voraussetzungen einzuschränken. 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.[10]

[7] Vgl. dazu das Urteil des EuGH vom 01.10.2015, C-201/14, Smaranda Bara u.a.
[8] 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.
[9] Vgl. dazu WP 242rev.01, Leitlinie der Art. 29-Gruppe vom 13.12.2016 zur Datenübertragbarkeit, abrufbar in Englisch unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.
[10] 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.

Das bisherige DVR-Meldeverfahren und das DVR selbst wird es nicht mehr geben (**Entfall der DVR-Meldepflicht**). Stattdessen verpflichtet Art. 30 Verantwortliche und Auftragsverarbeiter ein **Verzeichnis von Verarbeitungstätigkeiten** zu führen, das auf Anfrage der Aufsichtsbehörde vorzulegen ist. Diese Verpflichtung gilt nicht für Unternehmen oder Einrichtungen, die weniger als 250 Bedienstete beschäftigen, sofern

- die Verarbeitung nicht ein Risiko für die Rechte und Freiheiten betroffener Personen birgt,
- nicht nur gelegentlich erfolgt oder
- nicht die Verarbeitung von sensiblen Daten nach Art. 9 und Strafdaten nach Art. 10 einschließt.

Daneben werden Verantwortliche verpflichtet, vor Inbetriebnahme eines neuen Datenverarbeitungssystems eine **Datenschutz-Folgeabschätzung**[11] durchzuführen und ggf. mit der Aufsichtsbehörde im Rahmen eines **Konsultationsverfahrens** zusammenzuarbeiten (Art. 35 und 36).

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).

Neu ist auch die verpflichtende **Bestellung eines Datenschutzbeauftragten** in bestimmten Bereichen (Art. 37 bis 39)[12], der die DSB Aufgaben weisungsungebunden durchführt und unmittelbar der höchsten Managementebene berichtet.

[11] Vgl. dazu WP 248, Leitlinie der Art. 29-Gruppe vom 04.04.2017 zur Datenschutz-Folgeabschätzung, abrufbar in Englisch unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.
[12] Vgl. dazu WP 243rev.01, Leitlinie der Art. 29-Gruppe vom 13.12.2016 zum Datenschutzbeauftragten, abrufbar in Englisch unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Folgende Verantwortliche/Auftragsverarbeiter haben zwingend einen Datenschutzbeauftragten zu bestellen:

- Behörden und öffentliche Stellen (mit Ausnahme von Gerichten soweit es nicht die 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.

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 obliegt der Aufsichtsbehörde; sie kann aber auch eine dafür besonders **geeignete Stelle akkreditieren**.

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.

6) Kapitel V

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

Ein derartiger Datenfluss ist nur unter folgenden Bedingungen zulässig:

- Vorliegen eines Angemessenheitsbeschlusses der Europäischen Kommission (Art. 45)
- Vorliegen geeigneter Garantien (Art. 46)
- Vorliegen verbindlicher unternehmensinterner Vorschriften (Art. 47)

Art. 49 sieht Ausnahmen für bestimmte Fälle vor.

Die Ratio hinter Kapitel V ist, dass die übermittelten Daten beim Empfänger im Drittstaat demselben Schutzregime wie in der EU unterliegen sollen.

7) Kapitel VI[13]

Wie derzeit wird es in jedem Mitgliedstaat zumindest eine unabhängige Aufsichtsbehörde geben.

Die Aufgaben und Befugnisse werden 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 von der Aufsicht ausgenommen, sofern sie im Rahmen ihrer justiziellen Tätigkeit handeln. Im Umkehrschluss unterliegen Organe der Gerichtsbarkeit daher der Aufsicht, wenn sie im Rahmen der Justizverwaltung tätig werden.

[13] 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.

8) Kapitel VII[14]

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.

Dabei fungiert die Aufsichtsbehörde am **Sitz der Hauptniederlassung** als **federführende Aufsichtsbehörde**[15], 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.

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 wird der nach Art. 68 einzurichtende **Europäische Datenschutzausschuss** spielen, 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 **Fällung verbindlicher Beschlüsse** (Art. 64 und 65). Er wird dabei von einem Sekretariat unterstützt, das vom Europäischen Datenschutzbeauftragten bereitgestellt wird.

---

[14] 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.

[15] Vgl. dazu WP 244, Leitlinie der Art. 29-Gruppe vom 13.12.2016 zur Feststellung der federführenden Aufsichtsbehörde, abrufbar in Englisch unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

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.

Art. 79 normiert das Recht auf einen wirksamen gerichtlichen Behelf gegen Verantwortliche oder Auftragsverarbeiter.

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.[16]

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

Art. 83 enthält Gelbußentatbestände sowie jene Gründe, die als erschwerend oder mildernd bei der Strafbemessung zu berücksichtigen sind.

Die **Geldbußen**, bei welchen es sich um **Verwaltungsstrafen** handelt[17], reichen bis zu 20 Millionen Euro oder, im Falle eines Unternehmens[18], 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.[19]

---

[16] Siehe dazu EG 142. Damit sollen Sammelklagen verhindert werden.
[17] 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).
[18] Da dem österreichischen Verwaltungsstrafrecht die Strafbarkeit juristischer Personen fremd ist, müsste innerstaatlich dafür eine Rechtsgrundlage geschaffen werden (vgl. dazu bspw. § 35 FM-GWG).
[19] Für Österreich siehe zur Unzulässigkeit der Verhängung einer Verwaltungsstrafe gegen ein oberstes Organ VfSlg. 19.988/2015.

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.[20]

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

[20] *Flendrovsky* argumentiert auf Basis der Rsp des VfGH, dass derart hohe Geldstrafen in Österreich zwingend von einem Gericht zu verhängen wären und nicht von einer Verwaltungsbehörde; vgl. dazu *Flendrovsky*, Die Aufsichtsbehörden, in *Knyrim* (Hrgs.) aaO S. 287.

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.

Nach Art. 99 trat die Verordnung am zwanzigsten Tag nach ihrer Veröffentlichung im ABl. in Kraft (das war der 25.05.2016) und gilt ab dem 25.05.2018.

11) Das österreichische Datenschutz-Anpassungsgesetz 2018

In Durchführung der DSGVO und Umsetzung der Datenschutzrichtlinie für den Bereich Polizei und Justiz (DSRL-PJ)[21] wurde vom österreichischen Gesetzgeber das Datenschutz-Anpassungsgesetz 2018[22] verabschiedet, das am 25. Mai 2018 in Kraft treten soll.

Kernstück des Datenschutz-Anpassungsgesetzes 2018 ist das Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG). Dabei wurde das bestehende DSG 2000 der einfachgesetzlichen Bestimmungen entkleidet, die Verfassungsbestimmungen (insbes. das Grundrecht auf Datenschutz nach § 1) bleiben bestehen.

Das (neue) DSG gliedert sich in 5 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 oder für die Verwendung im Beschäftigungskontext).

Der **3. Abschnitt** regelt die **Bildverarbeitung** (vormals „Videoüberwachung“).

Weitere wesentliche Eckpunkte sind:

- Die **Datenschutzbehörde** wird als **Aufsichtsbehörde mit allen Befugnissen** (**einschließlich der Verhängung von Geldbußen**) nach der DSGVO und der DSRL-PJ eingerichtet.

[21] 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.
[22] BGBl. I Nr. 120/2017.

- **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 derzeitiger Rechtslage der Zivilrechtsweg zu beschreiten ist; vgl. dazu § 32 DSG 2000).

- 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**; diese Einrichtungen, Organisationen oder Vereinigungen können für Betroffene auch das Recht auf **Schadenersatz** gerichtlich geltend machen; ein **Einschreiten** der Einrichtungen, Organisationen oder Vereinigungen **ohne Mandat** (d.h. ohne Bevollmächtigung) ist **nicht vorgesehen**.

- 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.

- 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 und können bereits vor dem 25. Mai 2018 kundgemacht werden (sie treten jedoch nicht vor diesem Datum in Kraft).

Die **Übergangsbestimmungen** (§ 69 DSG) regeln folgende wesentliche Sachverhalte:

- Das **DVR** bleibt zu **Archivzwecken** bis Ende 2019 bestehen, es dürfen jedoch keine inhaltlichen Änderungen vorgenommen werden[23]; eine öffentliche Einsicht bleibt bis zu diesem Zeitpunkt weiter möglich.

[23] Die Datenschutzbehörde stellt eine technische Schnittstelle zur Verfügung, über welche registrierte Datenanwendungen in einem technisch üblichen Format heruntergeladen und weiterbearbeitet werden können.

- **Registrierungen** im DVR werden **gegenstandslos**, am 25. Mai 2018 anhängige **Registrierungsverfahren** nach §§ 17 ff DSG 2000 gelten mit diesem Tag als **eingestellt.**

- **Verfahren nach den §§ 13, 46 und 47 DSG 2000** sind **fortzuführen**, sofern die Genehmigung nach dem DSG oder der DSGVO erforderlich ist; anderenfalls gelten sie als **eingestellt.**

- Zum Zeitpunkt des Inkrafttretens des DSG bei der Datenschutzbehörde oder bei den ordentlichen Gerichten zum DSG 2000 **anhängige Verfahren** sind **nach den Bestimmungen des DSG und der DSGVO fortzuführen**, mit der Maßgabe, dass die Zuständigkeit der ordentlichen Gerichte aufrecht bleibt.

Die auf Basis des DSG 2000 erlassenen **Verordnungen** (Standard- und Muster-Verordnung 2004 – StMV 2004, Datenverarbeitungsregister-Verordnung 2012 – DVRV 2012 und die Datenschutzangemessenheits-Verordnung – DSAV, BGBl. II Nr. 521/1999) **treten** mit Ablauf des 24. Mai 2018 **außer Kraft**.

12) Häufig gestellte Fragen

Ab wann gilt die DSGVO?

25. Mai 2018.

Gilt die DSGVO nur für Großunternehmen?

Nein. Die DSGVO gilt auch für Klein- und Einpersonunternehmen unter bestimmten Voraussetzungen sowie 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).

Gibt es eine Übergangsfrist?

Die DSGVO normiert, dass bestehende Datenverarbeitungen innerhalb von zwei Jahren ab Inkrafttreten der DSGVO (das war der 25. Mai 2016) mit ihr in Einklang zu bringen sind. D.h., dass bestehende Datenverarbeitungen ab dem 25. Mai 2018 „DSGVO-konform" zu sein haben.

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.

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 Artikel 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 Artikel 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. Artikel 14. Abs. 5 DSGVO).

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

1. Das **Recht auf Auskunft (Art. 15 DSGVO)**. Der Betroffene muss eine Bestätigung erhalten, 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;

    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 Datenherkunft;

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

    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. Eine Kopie der verarbeiteten Dateninhalte muss so gestaltet sein, dass die Datenschutzrechte anderer Personen nicht verletzt werden.

2. Das **Recht auf Berichtigung (Art. 16 DSGVO)**. Es bezieht sich auf Dateninhalte. 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.

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 nicht unmöglich oder mit unverhältnismäßigem Aufwand verbunden, 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 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.

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 von ihm vorgebrachter Gründe für eine Beendigung der Verarbeitung verlangen. Gegen 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. 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. Nicht der gesamte Entscheidungsprozess muss ausschließlich automatisiert ablaufen. Er darf sich nie ausschließlich (und nur unter besonderen Bedingungen) auf sensible Daten (besondere Datenkategorien, Art. 9 Abs. 1 DSGVO) stützen. Der 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 automatisierte Entscheidungsfindung beträgt einen Monat. U.U. ist eine Verlängerung auf drei Monate möglich.

Welche neuen Pflichten gibt es für Verantwortliche und Auftragsverarbeiter?

Im Folgenden erhalten Sie einen kurzen Überblick über die wesentlichsten Pflichten, welche auf die Verantwortlichen bzw. auf die Auftragsverarbeiter im Zuge der DSGVO zukommen werden:

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

Verantwortliche müssen schriftlich ein Verzeichnis aller Verarbeitungstätigkeiten (= Datenanwendungen), die ihrer Zuständigkeit unterliegen, führen. Dieses Verzeichnis hat jedenfalls zu enthalten: seinen Namen und seine Kontaktdaten, 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 internationalen Organisationen); wenn möglich: Löschungsfristen, Beschreibung technischer und organisatorischer Maßnahmen.

Auch Auftragsverarbeiter müssen schriftlich ein Verzeichnis aller Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten führen.

Der Verantwortliche, sein Auftragsverarbeiter oder gegebenenfalls deren Vertreter haben der Datenschutzbehörde auf deren Anfrage das Verzeichnis zur Verfügung zu stellen.

Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, trifft die Pflicht zur Führung eines Verzeichnisses nicht, außer eine Verarbeitung birgt ein Risiko für Rechte und Freiheiten der Betroffenen oder sie erfolgt nicht nur gelegentlich oder umfasst 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 (Art. 9 Abs. 1) oder Daten über strafrechtliche Verurteilungen bzw. über Straftaten (Art. 10).

Zur Information:

- **Mit 25. Mai 2018 entfällt die Meldepflicht gemäß §§ 17 ff Datenschutzgesetz 2000 (DSG 2000) an das Datenverarbeitungsregister. DVR-Meldungen sind ab diesem Zeitpunkt 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 wird es dazu keine Vorgaben/kein Muster geben. DVR-Meldungen können als Vorlage für ein Verzeichnis herangezogen werden, zwingend ist dies jedoch nicht. Voraussichtlich ab August/September 2017 wird eine Schnittstelle zur Verfügung stehen, sodass bestehende DVR-Meldungen in ein Verzeichnis nach Art. 30 DSGVO übertragen werden können.**

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

Der Verantwortliche und der Auftragsverarbeiter, gegebenenfalls deren Vertreter, haben mit der Datenschutzbehörde auf deren Anfrage zusammenzuarbeiten.

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

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) oder aufgrund genehmigter Zertifizierungsverfahrens (Art. 42).

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

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.

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

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-Folgeabschätzung (Art. 35)***

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:

- 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 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 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. Sie kann eine Liste der Verarbeitungsvorgänge, bei denen keine Datenschutz-Folgenabschätzung durchzuführen ist, veröffentlichen. 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 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.

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

Der Verantwortliche hat vor Beginn der Verarbeitung die Datenschutzbehörde zu konsultieren, wenn aus einer Datenschutz-Folgenabschätzung gemäß Art. 35 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 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 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)***

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 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 besteht.

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

Brauche ich einen Datenschutz-Beauftragten?

Ob Sie einen Datenschutzbeauftragten „brauchen", müssen Sie zunächst 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.

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[24], welche Anhaltspunkte für die Auslegung des Begriffs der öffentlichen Stelle liefern, ist insbesondere das **Datenschutzanpassungsgesetz 2018**[25] heranzuziehen. Darin findet sich in § 26 Abs. 1 DSG eine Definition für den **Verantwortlichen des öffentlichen Bereichs**. Darunter fallen alle Verantwortliche,

- die in Formen des öffentlichen Rechts eingerichtet sind oder
- zwar in Form des Privatrechts eingerichtet sind, jedoch in Vollziehung der Gesetze tätig werden (so genannte „beliehene Rechtsträger" sowie Fälle der schlichten Hoheitsverwaltung).

Nach derzeitiger Ansicht der Datenschutzbehörde kann diese Definition als Beurteilungskriterium herangezogen werden. Sie entspricht auch weitgehend jener

[24] Abrufbar in Englisch (Guidelines on Data Protection Officers; Annex) unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.
[25] Abrufbar auf der Website des Parlaments unter www.parlament.gv.at.

Definition, die das deutsche Bundesdatenschutzgesetz vorsieht, welches den Begriff der „öffentlichen Stelle“ schon jetzt kennt.[26]

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

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) oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (gemäß Art. 10) besteht.

Welche Stellung 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).

Kann ein Datenschutzbeauftragter verantwortlicher Beauftragter nach § 9 VStG sein?

[26] Für weitere Ausführungen siehe *König/Leiter* in *Gantschacher/Jelinek/Schmidl/Spanberger*, Kommentar zur Datenschutz-Grundverordnung[1] [2017] Art. 37 Anm. 3.

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.

Was sind Verhaltensregeln?

Gem. 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 die Aufsichtsbehörde beauftragt, wobei diese auch eine von ihr dafür besonders geeignete Stelle akkreditieren kann.

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 Aufsichtsbehörde 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 ist bei Übermittlungen von Daten ins Nicht-EU-Ausland zu beachten? Was passiert mit bisherigen Genehmigungen?

Durch die DSGVO erfolgt eine weitreichende Genehmigungsfreiheit im internationalen Datenverkehr (Art. 44-50 DSGVO). Es ist – wie bisher auch – darauf zu achten, dass alle Verarbeitungsvorgänge zuerst im Inland zulässig sind, bevor ein Datenexport möglich ist.

Die bereits bekannten rechtlichen Instrumente für den Datenexport bleiben erhalten und werden ergänzt:

Daten dürfen an ein Drittland oder eine internationale Organisation übermittelt werden, wenn dort ein angemessenes Schutzniveau besteht (Art. 45 DSGVO). Die Feststellung erfolgt wie bisher durch die Kommission der EU. Die bestehende Liste bleibt gültig.

Weiters ist die Übermittlung zulässig, wenn eine vertragliche Vereinbarung mit Standarddatenschutzklauseln abgeschlossen wurde oder verbindliche interne Datenschutzvorschriften (Binding Corporate Rules, BCRs) bestehen. Diese Instrumente gab es schon bisher. Zu den neuen rechtlichen Instrumenten gehören Verhaltensregeln (Art. 40 DSGVO) und Zertifizierungsmechanismen (Art. 42 DSGVO). Art. 46 Abs. 3 DSGVO enthält die Möglichkeit, in Sonderfällen eine Genehmigung durch die Aufsichtsbehörde einzuholen.

Art. 49 DSGVO enthält einige Sonderfälle, von denen einige mit den Regeln im bestehenden § 12 DSG 2000 übereinstimmen (Zustimmung, Vertragserfüllung, öffentliches Interesse, Verteidigung von Rechtsansprüchen, lebenswichtige Interessen) und einige neu dazugekommen sind (Übermittlung eines Auszugs aus einem öffentlichen Register).

Die DSGVO bringt weniger Behördenwege, und mehr Verantwortung. Es ist insbesondre erforderlich, die eigenen Zwecke und Datenbanken zu kennen und selbst zu entscheiden, welche rechtlichen Instrumente geboten sind.

Es bestehen auch Informationspflichten an Betroffene, wenn Daten ins Nicht-EU-Ausland übermittelt werden sollen (Art. 13 Abs. 1 lit. f und 14 Abs. 1 lit. f DSGVO).

Bereits erteilte Genehmigungen bleiben grundsätzlich gültig (Art. 6 Abs. 5 DSGVO).

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

Hier tritt kein wesentlicher Unterschied zur Rechtslage nach dem DSG 2000 ein. 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. Standardvertragsklauseln). 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 Could (bspw. durch einen Hackerangriff o.ä.) trägt die datenschutzrechtliche Verantwortung (einschließlich schadenersatzrechtlicher Ansprüche) nach außen hin der Verantwortliche (d.h. jene Person/jene Einrichtung, die Cloud-Services in Anspruch nimmt).

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.

In bestimmten Fällen kann die Datenschutzbehörde an Stelle der Verhängung einer Geldbuße auch eine förmliche Verwarnung aussprechen.

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.

Wird es eine Frist nach dem 25.05.2018 geben, während derer keine Geldbußen verhängt werden?

Die DSGVO sieht keine Übergangsfrist vor. Es wird jeder Fall einzeln beurteilt und das Erfordernis der Verhängung einer Geldbuße durch die Datenschutzbehörde geprüft werden.

Welche Befugnisse hat die Datenschutzbehörde?

Die Aufsichtsbehörde hat 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

Wofür muss ich haften?

Jeder (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 Verantwortlicher noch Auftraggeber für den Umstand durch welchen der Schaden eintrat, verantwortlich ist.

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).

13) Weiterführende Literatur

Stand: Juli 2017 (alphabetische, nicht vollständige Aufzählung)

- *Feiler/Forgó*, EU-Datenschutz-Grundverordnung (Kommentar)
- *Gantschacher/Jelinek/Schmidl/Spanberger* (Hrsg.), Kommentar zur Datenschutz-Grundverordnung
- *Gola* (Hrsg.), Datenschutz-Grundverordnung (Kommentar)
- *Kühling/Buchner* (Hrsg.), Datenschutz-Grundverordnung (Kommentar)
- *Knyrim* (Hrsg.), Datenschutz-Grundverordnung (Praxishandbuch)
- *Paal/Pauly* (Hrsg.), Datenschutz-Grundverordnung (Kommentar)
- *Pollirer/Weiss/Knyrim/Haidinger*, DSGVO (Textausgabe)
- *Sydow* (Hrsg.), Europäische Datenschutzgrundverordnung (Kommentar)