

Zeitschrift für

VERBRAUCHER-**VbR** RECHT

Wichtiges
zur DSGVO

Chefredakteurin **Petra Leupold**
Redaktion **Wilma Dehn, Alexander Klauser,**
Paul Oberhammer, Alexander Schopper

Mai 2018

03

81 – 124

Datenschutz NEU

Betroffenenrechte nach der DSGVO

Georg Fellner ➤ 84

Rechtsdurchsetzung nach der DSGVO

Alexander Klauser ➤ 89

Beiträge

Zur Regelung der Bankomatgebühren durch die VZKG-Novelle 2017

Thomas Haghofer ➤ 95

Kryptowährungen als volatile Waren gemäß § 18 Abs 1 Z 2 FAGG?

Arthur Stadler und Andreas Pfeil ➤ 101

Rechtsprechung

Erklärungsfiktionsklauseln nächster Generation

Beate Gelbmann ➤ 104

VKrG: Überziehung vs Überschreitung

Stephan Foglar-Deinhardstein ➤ 113

Abschöpfungsverfahren: Übergang zum IRÄG 2017

Birgit Schneider ➤ 115

Anlegerschaden in der Insolvenz des Beraters

Wolfgang Fichtinger ➤ 117

Ausgleichszahlung bei „wildem Streik“ ➤ 118

Lebensversicherung: Spätücktritt und Rückabwicklung ➤ 119

Forum

Digitalisierung und das ABGB – Einige Vorbemerkungen aus Anlass des 20. Österreichischen Juristentags *Nikolaus Forgó* ➤ 122

Betroffenenrechte nach der DSGVO

Ab 25. 5. 2018 gilt die EU-DSGVO und schafft einen neuen Rechtsrahmen im Bereich des Datenschutzes. Großes Ziel ist die Stärkung der Rechte der betroffenen Personen. Dieser Beitrag gibt einen Überblick über die aus Konsumentensicht wesentlichen materiell-rechtlichen Neuerungen.

Von Georg Fellner

VbR 2018/47

A. Hintergrund

Die DSGVO¹⁾ wird vielfach als neuer Meilenstein im Datenschutzbereich beschrieben. Ohne Zweifel bedeutet sie die größte Änderung im Datenschutzrecht seit mehr als 20 Jahren. Die DSGVO löst die bisherige DatenschutzRL²⁾ aus 1995 ab. Neue technologische Entwicklungen haben den Datenschutz seither vor große Herausforderungen gestellt. Die Themen Cloud, Big Data, Social Media, Internet der Dinge, Industrie 4.0 waren 1995 noch weitgehend unbekannt. Diese technologischen Entwicklungen haben dazu geführt, dass generell immer mehr und mehr Daten weltweit verarbeitet werden. Wie die aktuellen Medienberichte über Facebook und Cambridge Analytica wieder zeigen, birgt dies auch die große Gefahr, dass Daten missbräuchlich verwendet werden. Die DSGVO hat sich das ambitionierte Ziel gesetzt, die Rechte der Bürger zu stärken und ihnen die Kontrolle über ihre persönlichen Daten zurückzugeben. Unternehmen und Organisationen trifft künftig eine erhöhte Selbstverantwortung bei der Verarbeitung von personenbezogenen Daten. Es gelten erweiterte Dokumentationspflichten sowie strengere Vorgaben für Datensicherheit. Einer der Kernpunkte der Reform sind zudem die strengen Sanktionen, welche dem Datenschutz mehr Beachtung schenken sollen. Künftig drohen bei Datenschutzverletzungen Geldstrafen bis zu 20 Mio Euro oder bis zu 4% des konzernweit erzielten Jahresumsatzes.

B. Anwendungsbereich

1. Sachlicher Anwendungsbereich

Die DSGVO gilt für die Verarbeitung **personenbezogener Daten**, dh jeglicher Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Bei der Frage, ob es sich um eine identifizierbare Person handelt, ist nicht nur auf das Wissen und die rechtlichen und tatsächlichen Möglichkeiten des jeweiligen Verantwortlichen abzustellen, der die Daten konkret verarbeitet. Für den Personenbezug genügt bereits die Identifikationsmöglichkeit durch einen Dritten.³⁾ Eine IP-Adresse eines Nutzers ist daher für einen Websitebetreiber auch dann personenbezogen, wenn nur der Internet Access Provider den Nutzer anhand der IP-Adresse identifizieren kann.⁴⁾ Die in Ö bislang geltenden Erleichterungen bei der Verarbeitung von lediglich indirekt personenbezogenen Daten, die vom jeweiligen Verarbeiter nicht einer bestimmten Person zugeordnet werden können, fallen mit der DSGVO künftig weg.⁵⁾ **Anonyme Daten**, die von nie-

mandem auf eine bestimmte Person rückgeführt werden können, sind datenschutzrechtlich nicht relevant. Nach der DSGVO künftig nicht mehr geschützt sind Daten über juristische Personen.⁶⁾

Die DSGVO gilt für die ganz oder teilweise **automatisierte** Verarbeitung von Daten. Sie gilt darüber hinaus – ähnlich wie bisher das DSG 2000 – auch für die **manuelle Verarbeitung** von Daten, die nach bestimmten Kriterien strukturiert in Form eines Dateisystems gespeichert werden.⁷⁾ Nach der bisherigen Rsp zum DSG 2000 sind darunter Karteien und Listen zu verstehen, nicht aber **Papierakten** und Aktenkonvolute.⁸⁾

- 1) VO (EU) 679/2016 vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).
- 2) RL 95/46/EG vom 24. 10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 281 vom 23. 11. 1995, S 31.
- 3) Vgl ErwGr 26 Satz 3 DSGVO, wonach alle Mittel zu berücksichtigen sind, die von dem Verantwortlichen oder einem Dritten nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die betroffene Person direkt oder indirekt zu identifizieren.
- 4) *Feiler/Forgo*, EU-DSGVO (2017) 4.
- 5) Bei der Verarbeitung von indirekt personenbezogenen Daten galten schutzwürdige Geheimhaltungsinteressen nach § 8 Abs 2 DSG 2000 und selbst für sensible Daten nach § 9 Z 2 DSG 2000 als nicht verletzt.
- 6) Im Datenschutz-Deregulierungs-Gesetz 2018 (98 BlgNR 26. GP) wird in § 4 DSG nunmehr klargestellt, dass das DSG nur für die Verarbeitung personenbezogener Daten natürlicher Personen gilt. Die Verfassungsbestimmung in § 1 DSG, die auch juristische Personen umfasst, blieb mangels Verfassungsmehrheit unverändert. Vgl zur Kontroverse über den Schutz juristischer Personen *Anderl/Hörlsberger/Müller*, Kein einfachgesetzlicher Schutz für Daten juristischer Personen, ÖJZ 2018/3.
- 7) Der Begriff des Dateisystems in Art 2 und Art 4 Z 6 DSGVO entspricht dem bisher in der RL 95/46/EG und dem DSG 2000 verwendeten Begriff der „Datei“. Darunter ist „jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind“, zu verstehen. In ErwGr 15 DSGVO wird klargestellt, dass „Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind“, nicht in den Anwendungsbereich der DSGVO fallen.
- 8) Nach stRsp der Datenschutzbehörde, des OGH, VwGH und VfGH zum geltenden DSG 2000 sind **Papierakten** (insb Behörden- und Gerichtsakten) keine Datei und besteht daher hinsichtlich der darin enthaltenen Daten kein Recht auf Löschung (zuletzt VfGH 12. 12. 2017, E 3249/2016). Nach der Rsp ist eine strukturierte Sammlung personenbezogener Daten nur dann anzunehmen, wenn sie – im Gegensatz zu einem Fließtext – eine äußere Ordnung aufweist, nach der die verschiedenen Arten von Daten in einer bestimmten räumlichen Verteilung auf dem oder den manuellen Datenträger(n) oder in einer bestimmten physikalischen oder logischen Struktur dargestellt sind. Darüber hinaus müssen die Daten nach bestimmten Kriterien zugänglich sein, dh es bestehen vereinfachte Möglichkeiten der inhaltlichen Erschließung, zB durch alphabetische oder chronologische Sortierung oder durch automatisierte Erschließungssysteme. Unter Datei sind daher Karteien und Listen, nicht aber Akten und Aktenkonvolute zu verstehen (vgl RIS-Justiz RS0113846). Nach der Rsp setzt das Vorliegen einer manuellen Datei daher voraus, dass sie sich durch einen bestimmten „Organi-

Explizit ausgenommen von der DSGVO ist die Verarbeitung personenbezogener Daten durch natürliche Personen zu ausschließlich **persönlichen oder familiären Zwecken**. Für rein private Aktivitäten in Sozialen Medien gilt die DSGVO daher nicht.

2. Räumlicher Anwendungsbereich

Die DSGVO gilt in jedem Fall für Verantwortliche und Auftragsverarbeiter, die ihren Sitz innerhalb der EU haben sowie für die Verarbeitung im Rahmen der Tätigkeiten einer (selbständigen oder unselbständigen) Niederlassung in der EU. Eine wesentliche Neuerung ist die **Erweiterung des Anwendungsbereichs auf nicht in der EU niedergelassene Verantwortliche und Auftragsverarbeiter**, wenn diese Daten von betroffenen Personen, die sich in der EU aufhalten, verarbeiten, um ihnen Waren oder Dienstleistungen anzubieten⁹⁾ oder um ihr Verhalten zu beobachten (Profiling).¹⁰⁾ Letzteres betrifft insb die Beobachtung des Surfverhaltens, um gezielt Werbung zu betreiben.¹¹⁾

C. Datenschutzrechtliche Grundsätze

Bei jeder Verarbeitung personenbezogener Daten müssen die allgemeinen datenschutzrechtlichen Grundsätze des Art 5 eingehalten werden. Inhaltlich blieben diese gegenüber dem DSG 2000 weitgehend unverändert. Wie bisher gelten der **Grundsatz der Rechtmäßigkeit** und der Verarbeitung nach **Treu und Glauben**. Dabei geht es um eine faire Verarbeitung. Wesentlich ist die ausreichende Information der betroffenen Personen. Diese dürfen über die Umstände der Verarbeitung und ihre Rechte nicht in die Irre geführt oder im Unklaren gelassen werden. Dies ergibt sich auch aus dem **Transparenzgrundsatz**. Daten müssen in einer für die betroffenen Personen nachvollziehbaren Weise verarbeitet werden. Die Transparenz ist für die betroffenen Personen Voraussetzung für die Kontrolle über die Verwendung der eigenen Daten und damit wesentlich für den Datenschutz. Der Transparenzgrundsatz wird durch **umfangreiche Informationspflichten**, die bei jeder Erhebung von Daten zu beachten sind, konkretisiert (Art 13, 14, s unten).

Eine zentrale Rolle im Datenschutzrecht spielt der **Zweckbindungsgrundsatz**. Daten dürfen nur für **festgelegte, eindeutige und rechtmäßige Zwecke** ermittelt und weiterverwendet werden (Art 5 Abs 1 lit b). Ausgangspunkt für die Prüfung der Zulässigkeit der Datenverarbeitung ist stets der jeweilige Verarbeitungszweck. Sollen Daten später für einen anderen Zweck weiterverwendet werden, ist zu prüfen, ob hierfür eine ausreichende Rechtsgrundlage besteht. Neu ist, dass Daten ausnahmsweise auch für einen anderen Zweck weiterverwendet werden dürfen als jenen, für den die Daten ursprünglich erhoben wurden, sofern der ursprüngliche und der neue Zweck miteinander vereinbar sind. Die Vereinbarkeit ist stets anhand einer Reihe von Kriterien zu prüfen, ua ausgehend von den vernünftigen Erwartungen der betroffenen Personen.

Nach dem **Grundsatz der Datenminimierung** dürfen Daten nur verwendet werden, soweit sie für den

jeweiligen Verarbeitungszweck wesentlich sind und über das erforderliche Ausmaß nicht hinausgehen (Art 5 Abs 1 lit d). Mit Daten ist daher möglichst sparsam umzugehen. Nach dem **Grundsatz der Speicherbegrenzung** dürfen Daten darüber hinaus nur so lange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist. Danach sind die Daten zu löschen oder zu anonymisieren, soweit die Daten nicht aufgrund gesetzlicher Verpflichtungen länger aufbewahrt werden müssen.¹²⁾ Nach dem **Grundsatz der sachlichen Richtigkeit und Aktualität** dürfen Daten nur so verwendet werden, dass sie im Hinblick auf den Verwendungszweck sachlich richtig sind. Wenn nötig sind sie zu aktualisieren. Der **Grundsatz der Datenintegrität und Vertraulichkeit** erfordert, dass angemessene technische und organisatorische Datensicherheitsmaßnahmen getroffen werden.

Die DSGVO statuiert nun ausdrücklich eine **Rechenschaftspflicht** des Verantwortlichen (Art 5 Abs 2). Dieser muss die Einhaltung der obigen Grundsätze nachweisen können und daher entsprechend dokumentieren. Nach Möglichkeit sind die Grundsätze durch geeignete technische und organisatorische Maßnahmen umzusetzen („privacy by design“).

D. Rechtmäßigkeit der Verarbeitung

Die DSGVO verfolgt – wie auch schon das DSG 2000 – das Prinzip, dass jede Verarbeitung personenbezogener Daten verboten ist, soweit diese nicht unter einen **Erlaubnistatbestand** fällt. Eine Verarbeitung „normaler“, nicht sensibler Daten ist nach Art 6 DSGVO nur rechtmäßig, wenn die betroffene Person ihre **Einwilligung** erteilt hat, die Daten zur **Erfüllung** eines Vertrags mit der betroffenen Person verarbeitet werden, eine **gesetzliche Verpflichtung** besteht, die Verarbeitung dem **Schutz lebenswichtiger Interessen** oder der **Erfüllung öffentlicher Aufgaben** dient, oder der Verantwortliche ein **berechtigtes Interesse**¹³⁾ an der Verarbeitung hat, soweit die Interessen der betroffenen Person nicht überwiegen.¹⁴⁾ Sensible Daten¹⁵⁾ dürfen nur unter den strengeren Voraussetzungen des Art 9 verarbeitet werden. →

sationsgrad' der ‚Akten‘ auszeichnen muss. Ein solcher Organisationsgrad wurde von den Gerichten bei Papierakten stets verneint (vgl etwa OGH 6 Ob 225/15 d).

9) Vgl Art 3 Abs 2 lit a iVm ErwGr 23 DSGVO.

10) Vgl Art 3 Abs 2 lit b iVm ErwGr 24 DSGVO.

11) Vgl *Tretzmüller*, Der globale Anwendungsbereich der DSGVO – warum die DSGVO auch in Drittländern umgesetzt werden sollte (muss), *Dako* 2018/6 (9).

12) Gesetzliche Aufbewahrungspflichten gibt es insb im Steuerrecht, in der Buchhaltung, im Arbeitsrecht.

13) Zu diesen zählen zB die Direktwerbung (ErwGr 47), die Verarbeitung der Daten von Kunden- und Beschäftigtendaten innerhalb einer Unternehmensgruppe (ErwGr 48) oder die Gewährleistung von Netz- und Informationssicherheit (ErwGr 49).

14) Während nach § 8 Abs 1 Z 4 DSG 2000 ein „überwiegendes“ berechtigtes Interesse des Auftraggebers erforderlich war, reicht nach Art 6 DSGVO ein zumindest gleichwertiges Interesse. Bezüglich dieses Erlaubnistatbestands kommt es daher zu einer Absenkung der Schwelle. Vgl auch G. *Kunnert* in *Grabenwarter/Graf/Ritschl* (Hrsg), Neuerungen im europäischen Datenschutzrecht für Unternehmen (2017) 28 f.

15) Art 9 DSGVO spricht von „besonderen Kategorien personenbezogener Daten“. Darunter fallen Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und

Die Voraussetzungen für eine rechtmäßige **Einwilligung** wurden konkretisiert und zudem verschärft. Eine Einwilligung der betroffenen Person ist demnach „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“ (Art 4 Z 11 DSGVO). Wie bisher muss eine Einwilligung **in informierter Weise**, in Kenntnis der Sachlage erfolgen. Schriftliche Ersuchen um Einwilligung müssen in verständlicher Form, in klarer und einfacher Sprache erfolgen. Neu ist, dass eine Einwilligung stets **aktiv** erteilt werden muss. Eine bereits angehakete Checkbox reicht daher nicht.¹⁶⁾

Besondere Anforderungen gelten künftig hinsichtlich der **Freiwilligkeit** einer Einwilligung. Eine Einwilligung ist nur dann freiwillig, wenn die betroffene Person die Einwilligung verweigern kann, ohne daraus Nachteile zu erleiden.¹⁷⁾ Einwilligungen zu verschiedenen Verarbeitungszwecken müssen gesondert erteilt werden können. Die Erfüllung eines Vertrags einschließlich der Erbringung einer Dienstleistung darf nicht von einer Einwilligung abhängig gemacht werden, die für die Erfüllung des Vertrags nicht erforderlich ist.¹⁸⁾ In der Praxis kommt es vor allem im Internet häufig vor, dass bestimmte Services nur dann genutzt werden können, wenn die Nutzer einer Nutzung ihrer Daten für Werbezwecke zustimmen. Nach der DSGVO sind derartige Geschäftsmodelle nur eingeschränkt zulässig. Die DSGVO sieht kein absolutes **Koppelungsverbot** vor.¹⁹⁾ Denkbar wäre etwa, den Nutzern eine Wahlmöglichkeit zu bieten zwischen einem kostenlosen werbefinanzierten Modell, bei dem die Nutzer mit ihren Daten bezahlen, und einem kostenpflichtigen werbefreien Modell.²⁰⁾ Laut ErwGr 43 soll das Kriterium der Freiwilligkeit dann nicht erfüllt sein, wenn zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen ein klares Ungleichgewicht besteht. Als Beispiel wird das Verhältnis von Betroffenen zu Behörden angeführt. Ähnliches gilt auch für Arbeitsverhältnisse. Allerdings schließt die DSGVO Einwilligungen im Arbeitsverhältnis nicht generell aus. Vielmehr überlässt die VO es den MS, spezifische Regelungen über die Datenverarbeitung im Beschäftigungskontext zu erlassen.²¹⁾ Neu geregelt wurde die Einwilligung von Kindern, allerdings nur bezogen auf Dienste der Informationsgesellschaft (Art 8).²²⁾

Bei der Einholung einer Einwilligung muss auf das jederzeitige **Widerrufsrecht** hingewiesen werden, wie bisher schon von der Rsp gefordert. Bestehende Einwilligungen, die nicht den Anforderungen der DSGVO entsprechen, sind nicht verbindlich und müssen daher ggf neu eingeholt werden.²³⁾

E. Rechte der betroffenen Person

1. Modalitäten für die Ausübung der Betroffenenrechte

Art 12 enthält allgemeine Bestimmungen, die für alle Betroffenenrechte gem Art 13 bis 22 DSGVO relevant

sind. Der Verantwortliche ist verpflichtet, der betroffenen Person alle Informationen bzw Mitteilungen „in **präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache**“ zu übermitteln. Ferner muss der Verantwortliche der betroffenen Person die Ausübung ihrer Rechte möglichst erleichtern und eine Antragstellung auf elektronischem Wege ermöglichen.²⁴⁾ Im Gegensatz zum geltenden DSG 2000 kennt die DSGVO keinen Formzwang für die Antragstellung. Die Informationen sind unverzüglich, in jedem Fall aber **innerhalb eines Monats** nach Eingang des Antrags zur Verfügung zu stellen (Art 12 Abs 3). Bei komplexen oder zahlreichen Anträgen kann diese Frist um zwei Monate verlängert werden. Der Verantwortliche hat die Ansprüche der betroffenen Person grundsätzlich **kostenlos** zu erfüllen. Art 12 Abs 5 kennt eine Ausnahme für offenkundig unbegründete oder – insb im Fall von häufiger Wiederholung – exzessive Anträge. Diesfalls kann der Verantwortliche ein angemessenes Entgelt fordern, das die Verwaltungskosten der Informationserteilung oder die Durchführung der Maßnahme abdeckt, oder den Antrag überhaupt ablehnen.²⁵⁾

2. Aktive Informationspflichten

Bei jeder Erhebung von personenbezogenen Daten sind die aktiven Informationspflichten gem Art 13 und 14 DSGVO zu beachten. Art 13 sieht eine Reihe von Pflichtangaben bei der Erhebung von Daten bei den betroffenen Personen vor. Dies gilt insb für diverse Web- und Papierformulare, die von den betroffenen Personen auszufüllen sind (zB Anmelde- und Registrierungsformulare, Fragebögen, Anträge etc), auch wenn die Erhebung der Daten gesetzlich vorgesehen ist oder wenn die Daten zur Vertragserfüllung benötigt werden. Im Vergleich zur bisherigen Rechtslage wurden die Informationspflichten wesentlich ausgeweitet. So sind nun neben der Identität des für die

biometrische Daten, Gesundheitsdaten sowie Daten zum Sexualleben oder der sexuellen Orientierung.

16) ErwGr 32.

17) Vgl ErwGr 42, 43 DSGVO.

18) Siehe Art 7 Abs 4 DSGVO ErwGr 43.

19) Vgl Heckmann/Paschke in Ehmann/Selmayr, DSGVO (2017) Art 7 Rz 53.

20) Vgl Dürager/Kotschy, Neuerungen zur Zustimmung: Besteht nach der DS-GVO ein generelles Kopplungsverbot? <http://bim.lbg.ac.at/de/themen/datenschutz-grundverordnung> (Stand 16. 4. 2018); Haidinger, Koppelungsverbot, Doko 2017/5; Feiler/Forgo, EU-DSGVO Art 7 Rz 11, wonach bei der Prüfung der Erforderlichkeit der Einwilligung für die Vertragserfüllung auch die wirtschaftliche Notwendigkeit zu berücksichtigen sei. Siehe auch Pachinger, DSGVO: Aus Zustimmung wird Einwilligung, ecoloX 2017, 898 (899).

21) Insb können die MS nähere Regelungen darüber vorsehen, unter welchen Voraussetzungen personenbezogene Daten auf Grundlage einer Einwilligung der Arbeitnehmer verarbeitet werden dürfen, vgl ErwGr 155 DSGVO.

22) Nach Art 8 gilt für Einwilligungen eines Kindes in Bezug auf Dienste der Informationsgesellschaft ein Mindestalter von 16 Jahren. Darunter ist die Zustimmung der Eltern nötig. Die MS können die Altersgrenze auf bis zu 13 Jahre herabsetzen. In Ö gilt eine Grenze von 14 Jahren (§ 4 DSG).

23) Vgl Art 7 Abs 2 DSGVO ErwGr 171.

24) ErwGr 59.

25) Haidinger, Geltendmachung der Betroffenenrechte und das Auskunftsrecht nach der EU-Datenschutz-Grundverordnung (Teil VII), Doko 2016/73 (109).

Verarbeitung Verantwortlichen und dem Zweck der Verarbeitung zusätzlich die Rechtsgrundlagen der Verarbeitung, allfällige Empfänger, die Dauer der Datenspeicherung, Hinweise auf die Betroffenenrechte sowie das Recht zur Beschwerde bei der Datenschutzbehörde zu nennen und ist über mögliche Folgen der Nichtbereitstellung der personenbezogenen Daten zu informieren. Die Informationen müssen vor oder zeitgleich mit der Erhebung der Daten erteilt werden. Bei Erhebungen auf einer Website können die Informationen im Rahmen einer Datenschutzerklärung erteilt werden.

Nach Art 14 bestehen Informationspflichten ferner dann, wenn personenbezogene Daten nicht bei den betroffenen Personen selbst, sondern auf andere Weise, etwa aus öffentlichen Quellen oder von Dritten, erhoben werden. Die Pflichtangaben decken sich weitgehend mit jenen bei Erhebung der Daten bei den betroffenen Personen nach Art 13. Zusätzlich ist zu informieren über die verarbeiteten Datenkategorien und allenfalls verfügbare Informationen über Datenquellen. Werden die Daten aus öffentlichen Quellen oder von Dritten erhoben und intern weiterverarbeitet, müssen die Informationen spätestens innerhalb eines Monats nach Erlangung der Daten erteilt werden. Falls die Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, muss die Information spätestens zum Zeitpunkt der ersten Mitteilung an diese erfolgen. Falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, muss die Information spätestens zum Zeitpunkt der ersten Offenlegung erfolgen. Die Informationspflicht nach Art 14 entfällt, wenn die betroffene Person bereits über die Information verfügt, wenn die Erlangung oder Offenlegung gesetzlich vorgesehen ist oder wenn die Daten dem Berufsgeheimnis oder einer satzungsmäßigen Geheimhaltungspflicht unterliegen.

3. Auskunftsrecht

Nach Art 15 hat eine betroffene Person das Recht auf Auskunft, ob und in welchem Ausmaß sie betreffende personenbezogene Daten von dem Verantwortlichen verarbeitet werden. Die betroffene Person hat auch das Recht auf Erhalt einer Kopie ihrer Daten, wobei die Rechte und Freiheiten anderer Personen hierdurch nicht beeinträchtigt werden dürfen. Die zu beauskunftenden Informationen decken sich weitgehend mit § 26 DSG 2000. Abweichend davon wird in Art 15 DSGVO das Recht auf Auskunft über die Rechtsgrundlagen der Verarbeitung nicht explizit angeführt. Aus ErwGr 63 folgt jedoch, dass das Auskunftsrecht dazu dienen soll, die Rechtmäßigkeit der Verarbeitung überprüfen zu können. Daher wird die Rechtsgrundlage der Verarbeitung ebenfalls zu beauskunfteten sein, soweit sich dies nicht bereits aus dem Verarbeitungszweck ergibt. Über § 26 DSG 2000 hinausgehend hat der Verantwortliche auch über die Speicherdauer Auskunft zu geben und auf das Recht auf Berichtigung, Löschung, Widerspruch und Einschränkung der Verarbeitung hinzuweisen. Ausnahmen vom Auskunftsrecht bestehen hinsichtlich der Offenbarung von Geschäfts- oder

Berufsgeheimnissen und hinsichtlich des Schutzes geistigen Eigentums.

4. Recht auf Berichtigung und Löschung

Ähnlich wie § 27 DSG 2000 gewähren Art 16 und 17 DSGVO der betroffenen Person das Recht, unrichtige Daten richtigzustellen oder Daten löschen zu lassen. Der Verantwortliche ist verpflichtet, Daten auf Antrag eines Betroffenen sowie auch aus Eigenem zu löschen, wenn der Zweck der Verarbeitung wegfällt, wenn die Verarbeitung auf Grundlage einer Einwilligung erfolgte und diese widerrufen wird, wenn die betroffene Person erfolgreich Widerspruch erhoben hat, wenn die Daten unrechtmäßig verarbeitet wurden oder die Löschung aufgrund von gesetzlichen Verpflichtungen notwendig ist.²⁶⁾ Ergänzt wurde das Recht auf Löschung um ein **Recht auf Vergessenwerden**. Hat der Verantwortliche Daten öffentlich gemacht (zB auf einer Website), ist er verpflichtet, angemessene Maßnahmen zu treffen, um andere Verantwortliche, die die Daten (weiter)verarbeiten, von dem Löschungsbegehren in Kenntnis zu setzen.²⁷⁾ Ähnlich sieht Art 19 vor, dass der Verantwortliche alle Empfänger, denen er die Daten übermittelt hat, über die Berichtigung, Löschung oder Einschränkung der Verarbeitung zu informieren hat, solange dies nicht unmöglich ist oder einen unverhältnismäßigen Aufwand verursacht.

Ausnahmen von der Löschungspflicht bestehen ua zugunsten des Rechts auf Meinungs- und Informationsfreiheit²⁸⁾, zugunsten im öffentlichen Interesse liegender Archivzwecke und wissenschaftlicher Forschungszwecke, bei gesetzlichen Aufbewahrungspflichten sowie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

5. Recht auf Einschränkung

Das Recht auf Einschränkung (Art 18) ist als Begleitanspruch zu dem Recht auf Löschung, Berichtigung und Widerspruch zu sehen.²⁹⁾ Per definitionem handelt es um die „Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken“.³⁰⁾ ErwGr 67 nennt als mögliche Maßnahmen beispielhaft das vorübergehende Übertragen der personenbezogenen Daten auf ein anderes Verarbeitungssystem, das Sperren dieser Daten für bestimmte Nutzer oder das vorübergehende Entfernen von einer Website. Die betroffene Person hat ein Recht auf Einschränkung der Verarbeitung, wenn (a) die Richtigkeit der Daten bestritten wird, für die Dauer der Überprüfung, (b) die betroffene Person die Einschränkung anstelle ihres Rechts auf Löschung begehrt, (c) der Verantwortliche die Daten nicht länger benötigt und die betroffene Person diese zur Geltendmachung von Rechtsansprüchen benötigt und (d) bis

26) Haidinger, *Dako* 2017/34 (57).

27) Im Einzelnen ist die Bestimmung unklar. Nach dem Wortlaut müsste die betroffene Person verlangen, dass ihre Daten auch von anderen Verantwortlichen gelöscht werden; s dazu *Feiler/Forgo*, EU-DSGVO Art 17 Rz 8.

28) Vgl Art 85 DSGVO.

29) Haidinger, *Dako* 2017/34 (57).

30) Art 4 Z 3 DSGVO.

zur Entscheidung über einen Widerspruch. Den Verantwortlichen trifft eine Informationspflicht gegenüber der betroffenen Person, bevor die Einschränkung wieder aufgehoben wird.³¹⁾

6. Recht auf Datenübertragbarkeit

Gänzlich neu ist das Recht auf Datenübertragbarkeit (Art 20). Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen mitgeteilt hat, in einem „strukturierten, gängigen und maschinenlesbaren Format“ zu erhalten oder an einen anderen Verantwortlichen übertragen zu lassen. Damit soll eine bessere Kontrolle über die eigenen Daten ermöglicht werden.³²⁾ Praktisch relevant ist dies in erster Linie für den Wechsel von Diensteanbietern.³³⁾ Mögliche Anwendungsbeispiele sind die Übertragung von Musik-Wiedergabelisten beim Wechsel von Streaming-Diensten, E-Mails und Kontaktlisten beim Wechsel des Internetproviders oder Transaktionsdaten des Bankkontos beim Wechsel der Bank.³⁴⁾ Das Recht auf Datenübertragung besteht nur dann, wenn die Verarbeitung auf Grundlage einer Einwilligung oder eines Vertrags automatisiert erfolgt und wenn die Daten durch die betroffene Person bereitgestellt wurden.³⁵⁾

7. Widerspruchsrecht

Das Widerspruchsrecht ermöglicht der betroffenen Person, **gegen rechtmäßige Verarbeitungen** personenbezogener Daten vorzugehen. Art 21 unterscheidet drei Fälle. Einerseits geht es um Verarbeitungen, die vom Verantwortlichen auf überwiegende berechtigte Interessen oder auf die Wahrnehmung einer Aufgabe im öffentlichen Interesse als Rechtsgrundlage gestützt werden. Die betroffene Person kann aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen derartige Verarbeitungen Widerspruch erheben. Die betroffene Person muss hierfür das Vorliegen einer „**besonderen Situation**“ glaubhaft machen. In diesem Fall muss der Verantwortliche entweder zwingende schutzwürdige Gründe nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder nachweisen, dass die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Ferner gibt es ein gesondertes Widerspruchsrecht betreffend **Direktwerbung**. Hier ist ein Widerspruch jederzeit und auch ohne Begründung möglich. Bei einem Widerspruch dürfen die Daten nicht mehr für diesen Zweck verarbeitet werden. Es findet also keine weitere Interessenabwägung statt. Einen weiteren Spezialfall bildet der Widerspruch gegen eine Datenverarbeitung zu wissenschaftlichen oder historischen **Forschungszwecken** oder zu statistischen Zwecken. In diesem Fall ist das Widerspruchsrecht nur begrenzt ausübbar.³⁶⁾

8. Automatisierte Entscheidungen im Einzelfall und Profiling

Art 22 schützt den Betroffenen vor einer ausschließlich auf einer automatisierten Verarbeitung (einschl. Profi-

ling) beruhenden Entscheidung, die gegenüber der betroffenen Person **rechtliche Wirkung** entfaltet oder diese in ähnlicher Weise erheblich beeinträchtigt.³⁷⁾ Dadurch sollen Entscheidungen verhindert werden, die ohne menschliches Zutun getätigt werden.³⁸⁾ Eine automatisierte Entscheidung ist ausnahmsweise erlaubt, wenn diese für den Abschluss eines Vertrags erforderlich ist, gesetzlich zulässig ist, oder eine ausdrückliche Einwilligung der betroffenen Person vorliegt.

9. Folgen eines Verstoßes gegen Betroffenenrechte

Verstöße gegen Betroffenenrechte können mit empfindlich hohen **Geldbußen** von bis zu 20 Mio Euro oder im Fall eines Unternehmens von bis zu 4% des weltweit erzielten Jahresumsatzes sanktioniert werden.³⁹⁾ Die Geldbußen sollen wirksam, verhältnismäßig und abschreckend sein. Die Bemessung der Geldbuße richtet sich nach den Umständen des Einzelfalls, insb. nach Art, Schwere und Dauer des Verstoßes, Schadenshöhe, Verschuldensgrad etc.⁴⁰⁾ Darüber hinaus hat jede betroffene Person das Recht auf Beschwerde bei der Aufsichtsbehörde und auf einen wirksamen gerichtlichen Rechtsbehelf.⁴¹⁾

10. Sonstige wesentliche Neuerungen

Die bestehende **Meldepflicht bei Datenschutzverletzungen**⁴²⁾ wird mit der DSGVO wesentlich ausgeweitet. Künftig muss bei jedem Datenleck die Aufsichtsbehörde binnen 72 Stunden ab Kenntnis im Detail informiert werden, soweit nicht jegliches Risiko für die Rechte und Freiheiten betroffener Personen ausgeschlossen werden kann. Im Fall eines hohen Risikos für die betroffenen Personen müssen diese persönlich informiert werden.⁴³⁾

31) Siehe Art 18 Abs 3 DSGVO.

32) Siehe ErwGr 68.

33) Wie *Feiler/Forgo* (aaO Art 20 Rz 3) jedoch richtig hinweisen, gilt das Recht auf Datenübertragbarkeit nach dem Wortlaut nur gegenüber Verantwortlichen, nicht hingegen gegenüber Auftragsverarbeitern. Wenn ein Diensteanbieter (zB Cloud-Anbieter) Daten im Auftrag eines Kunden verarbeitet, ist er insoweit als Auftragsverarbeiter zu qualifizieren. Für das Recht auf Datenübertragbarkeit bliebe dann kaum ein Anwendungsbereich. Die Art-29-Datenschutzgruppe legt die Bestimmung sehr weit aus und interpretiert das Recht auf Datenübertragbarkeit in Richtung eines „privaten Informationsweiterverwendungsrechts“.

34) Vgl Leitlinien zum Recht auf Datenübertragbarkeit der Art-29-Datenschutzgruppe, WP 242.

35) Dies schließt nach der Art-29-Datenschutzgruppe auch „Beobachtungsdaten“ ein, wie Rohdaten eines Smart Meters, besuchte Websites, Suchverläufe, Logfiles, Standortdaten bei Mobilfunkanbietern. Nicht umfasst sind dagegen Daten, die der Verantwortliche selbst generiert hat, wie etwa Bewertungen und Schlüsse, die aus einem Nutzerverhalten gezogen werden.

36) *Haidinger*, Widerspruch, automatisierte Einzelentscheidungen und die Informationspflichten nach der DSGVO (Teil XII), *Dako* 2017/63 (103).

37) Vgl ErwGr 71 Satz 1.

38) *Hladik* in *Sydow* (Hrsg), Europäische Datenschutzgrundverordnung¹ (2017) Art 22 DSGVO.

39) Vgl Art 83 Abs 5 lit b DSGVO.

40) Vgl die Kriterien in Art 83 Abs 2 DSGVO; s auch „Leitlinien für die Anwendung und Festsetzung von Geldbußen“ der Art-29-Datenschutzgruppe, WP 253.

41) Siehe dazu den Beitrag von *Klauser*, Rechtsdurchsetzung im Datenschutz nach der DSGVO und dem DSG 2018 i d F des DS-DeregulierungsG 2018, *VbR* 2018/48, in diesem Heft auf S 89.

42) Vgl § 24 Abs 2 a DSG 2000.

43) Vgl Art 33, 34 DSGVO.

Die Verantwortlichen müssen künftig ein schriftliches **Verzeichnis der Verarbeitungstätigkeiten** führen. Dafür entfällt die bisherige Meldepflicht gegenüber dem Datenverarbeitungsregister. Für Datenverarbeitungen, bei denen das Risiko einer Verletzung von Rechten betroffener Personen voraussichtlich besonders hoch ist, ist vom Verantwortlichen vor Beginn der Datenverarbeitung eine **Datenschutz-Folgenabschätzung** durchzuführen. Dies betrifft insb Verarbeitungen, die der systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen dienen und/oder bei denen öffentlich zu-

gängliche Bereiche systematisch umfangreich überwacht werden.⁴⁴⁾

Schließlich müssen Behörden und Unternehmen, zu deren Kerntätigkeit die umfangreiche Verarbeitung sensibler Daten oder die umfangreiche und systematische Überwachung natürlicher Personen gehört, künftig einen **Datenschutzbeauftragten** bestellen (Art 37 ff, § 5 DSG).

44) Vgl Leitlinien zur Datenschutz-Folgenabschätzung der Art-29-Datenschutzgruppe, WP 248.

→ In Kürze

Ziel der DSGVO ist es, den betroffenen Personen die Kontrolle über ihre persönlichen Daten zurückzugeben und die Rechte der Einzelnen zu stärken. Sie sieht umfangreiche Informationspflichten vor und erleichtert die Ausübung der Rechte betroffener Personen. Für Unternehmen bringt die DSGVO eine erhöhte Selbstverantwortung und erweiterte Dokumentationspflichten. Durch die Ausdehnung des Anwendungsbereichs auf Verantwortliche in Drittländern und die drastischen Geldbußen soll ein effektiver Datenschutz gewährleistet werden.

→ Zum Thema

Über den Autor:

Mag. Georg Fellner, LL. M. ist Rechtsanwalt bei bkp Rechtsanwälte in Wien. E-Mail: g.fellner@bkp.at