www.oejz.at

Österreichische

JURISTEN ZEITUNG

ÖJZ

Chefredakteur Gerhard Hopf
Redaktion Robert Fucik, Kurt Kirchbacher, Hans Peter Lehofer
Evidenzblatt Christoph Brenn, Helge Hoch, Eckart Ratz, Ronald Rohrer, Martina Weixelbraun-Mohr
Anmerkungen Andreas Konecny, Martin Spitzer

09

Mai 2018

385 – 432

ISSN 0029-9251 Österreichische Post AG PZ 17Z041036 P Verlag Manz, Gutheil Schoder Gasse 17, 1230 Wien

MANZ

Die DSGVO im privaten Bereich

Europarechtliche Vorgaben an Unternehmen[1)]

ÖJZ 2018/52
DSGVO; DSG
Verantwortlicher; Compliance; Einwilligung; Datenschutz-Folgenabschätzung; Geldbußen

Die DSGVO verändert die datenschutzrechtlichen Rahmenbedingungen und betrifft dabei zentral private Unternehmen. Grundlegende Fragen stellen sich zu den Pflichten der datenschutzrechtlich Verantwortlichen in den Unternehmen ebenso wie zum One-Stop-Shop-Prinzip für Unternehmen. Das Datenschutzanpassungsgesetz 2018 schafft darüber hinaus (wenige) österreichische Spezifika.

Von Konrad Lachmayer

Inhaltsübersicht:

1) Der nachstehende Beitrag basiert auf Vorträgen des Autors zum Thema im Rahmen des Forums Öffentliches Recht des Juristenverbandes sowie auf zahlreichen weiteren Vorträgen zum Datenschutzrecht im Jahr 2017. Der Beitrag bezieht sich auch auf *Lachmayer,* Die DSGVO im öffentlichen Bereich. Europarechtliche Vorgaben an die staatliche Verwaltung, ÖJZ 2018, 112.

A. Grundsätzliches

1. Alles neu oder doch alles beim Alten?

Mit der Datenschutz-Grundverordnung (DSGVO) werden die datenschutzrechtlichen Spielregeln in Europa nach langer Vorlaufzeit[2] neu gefasst; sie treten mit 25. 5. 2018 in Kraft. Die DSGVO bezieht öffentliche ebenso wie private Datenverarbeitung mit ein.[3] Bei näherer Betrachtung bestehen aber viele Unterschiede für diese zwei Regelungsbereiche.[4] Diesem Umstand geschuldet wurden die spezifischen Charakteristika der Regulierung für den öffentlichen Bereich gesondert analysiert.[5]

Bei einer allgemeinen Betrachtung bestehen mehr Gemeinsamkeiten als Unterschiede zwischen der DSGVO und der DS-RL. Insoweit kann die DSGVO als Weiterentwicklung der bestehenden datenschutzrechtlichen Regeln verstanden werden. Die grundlegende Veränderung ist vielmehr rechtlich-konzeptioneller Art, indem eine unmittelbar anwendbare Verordnung staatliche Umsetzung obsolet werden lässt und die Rolle des innerstaatlichen Gesetzgebers auf nationale Anpassungen reduziert.[6] Damit verbunden ist auch eine funktionelle Aufwertung der unabhängigen Datenschutzbehörde (DSB), deren Aufgaben und Befugnisse erweitert werden und die mit erheblicher (verwaltungsstrafrechtlicher) Sanktionsgewalt ausgestattet wird.

Abgesehen von inhaltlichen Änderungen im Detail sticht als wesentliche Neuerung die Privatisierung der rechtlichen Datenschutzverwaltung ins Auge. Während bisher Datenverarbeitungen an ein von der Behörde geführtes Register (DVR) gemeldet werden mussten, wird dieses Register nun durch interne Dokumentationspflichten, Risikoabwägungen und Informationspflichten, für die das Unternehmen verantwortlich ist, ersetzt. Insoweit ist gem Art 24 Abs 1 DSGVO als primäre Pflicht des datenschutzrechtlich Verantwortlichen hervorzuheben, dass dieser – um dem Schutz personenbezogener Daten gerecht zu werden – *„geeignete technische und organisatorische Maßnahmen"* setzt, um *„sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt"*. Es kommen aufgrund dieser Vorgaben den Unternehmen aber auch anderen Personen im privaten (aber nicht persönlich-familiären) Bereich neue administrative Aufgaben zu, die es intern zu bewältigen gilt.

Insoweit macht die DSGVO weder *„alles neu"* noch belässt sie *„alles beim Alten"*. Es werden einerseits bestehende Prinzipien und Rechte ausgebaut, aber andererseits die unternehmensinternen Aufgaben vervielfältigt und die Kontrolle durch eine starke Aufsichtsbehörde ergänzt.

2. Begrifflichkeiten, Rollenverteilung und Prinzipien

Art 4 DSGVO nimmt ausführliche Begriffsbestimmungen vor, wobei die beispielhafte Konkretisierung des Personenbezugs von Daten durch explizite Erwähnung etwa von genetischen Daten dem Standard des 21. Jh angepasst wurde. Als neue Kategorie wurden sogenannte pseudonymisierte Daten eingeführt, die als personenbezogene Daten gelten, aber dem Datenschutz besser gerecht werden. Pseudonymisierung bezieht sich in diesem Sinne auf *„die Verarbeitung personenbezogener Daten in einer Weise, dass die[se] ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden"* und technische sowie organisatorische Maßnahmen diese Trennung gewährleisten.[7] Weiterhin werden sensible Daten als sog *„besondere Kategorien von Daten"* gem Art 9 DSGVO stärker geschützt. Die bestehende Differenzierung unterschiedlicher Verarbeitungsprozesse personenbezogener Daten wurde zugunsten einer allgemeinen Definition von *„Verarbeitung"* gem Art 4 Z 2 DSGVO aufgegeben.

Auch bei der datenschutzrechtlichen Rollenverteilung gab es abgesehen von begrifflichen Änderungen keine signifikanten Neuerungen. So differenziert die

2) Siehe dazu etwa *Lachmayer,* Zur Reform des europäischen Datenschutzes. Eine erste Analyse des Entwurfs der Datenschutz-Grundverordnung, ÖJZ 2012, 841.
3) Zu den unterschiedlichen Dimensionen des Datenschutzes zwischen staatlichen und privaten Perspektiven s allgemein *Lachmayer,* Die Multidimensionalität des Datenschutzrechts. Zur Notwendigkeit der Ausdifferenzierung datenschutzrechtlicher Regelungen, in FS Berka (2013) 121.
4) Die Unterscheidung wird allerdings in der DSGVO nicht immer konsequent vorgenommen. So bezieht sich etwa Art 3 Abs 1 DSGVO auf die „Niederlassung eines Verantwortlichen" und meint damit etwa auch den Sitz einer Behörde oder einer anderen öffentlichen Stelle.
5) Siehe *Lachmayer,* ÖJZ 2018, 112.
6) Siehe das Datenschutz-Anpassungsgesetz 2018 BGBl I 2017/120. Zahlreiche weitere materienspezifische Anpassungsgesetze befinden sich derzeit im parlamentarischen Prozess bzw in Vorbereitung.
7) Art 4 Z 5 DSGVO.

DSGVO zwischen der „*betroffenen Person*“,[8] dem datenschutzrechtlich „*Verantwortlichen*“,[9] der über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet,[10] und dem „*Auftragsverarbeiter*“,[11] der die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet. Schließlich wird die ö DSB als datenschutzrechtliche Aufsichtsbehörde gem Art 4 Z 21 iVm Art 51 ff DSGVO tätig.

Die datenschutzrechtlichen Prinzipien gem Art 5 DSGVO entsprechen ebenfalls den bisher bestehenden Grundsätzen des Datenschutzrechts. Über die „*Rechtmäßigkeit*“ und die „*Verarbeitung nach Treu und Glauben*“ hinaus betont die DSGVO die „*Transparenz*“. Weiterhin bleiben „*Zweckbindung*“, „*Datenminimierung*“, „*Richtigkeit*“, „*Speicherbegrenzung*“ sowie „*Integrität und Vertraulichkeit*“ zentrale datenschutzrechtliche Prinzipien. Hervorgehoben wird die „*Rechenschaftspflicht*“ des Verantwortlichen, der für die Einhaltung dieser Prinzipien nicht nur verantwortlich ist, sondern deren Einhaltung er auch nachweisen können muss.

B. Der Anwendungsbereich der DSGVO für Unternehmen

1. Der sachliche und räumliche Anwendungsbereich

Der sachliche Anwendungsbereich der DSGVO bezieht sich auf die automatisierte Verarbeitung personenbezogener Daten sowie auf die nicht automatisierte Verarbeitung, die in einem Dateisystem[12] gespeichert wird bzw werden soll. Im Rahmen dieses breiten Anwendungsbereichs besteht gem Art 2 Abs 2 lit a DSGVO die Einschränkung, dass Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, davon ausgenommen werden. Im Hinblick auf wirtschaftliche Tätigkeiten (auch im Non-profit-Bereich) ist davon auszugehen, dass der Anwendungsbereich des Unionsrechts jedenfalls eröffnet ist.[13] Dies ergibt sich bereits aus Art 1 DSGVO, der iVm Art 16 AEUV den „*freien Verkehr personenbezogener Daten in der Union*“ in den Mittelpunkt rückt. Ausnahmen beziehen sich vielmehr auf bestimmte Facetten des öffentlichen Bereichs.[14] Im privaten Bereich besteht daher nur dann eine Ausnahme, wenn die Verarbeitung personenbezogener Daten „*durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten*“ stattfindet.

Als Grenze des sachlichen Anwendungsbereichs ist auch der Personenbezug der Daten anzusehen. So sind anonymisierte Daten (aufgrund des nicht mehr bestehenden Personenbezugs) nicht von der DSGVO erfasst. Eine besondere Herausforderung entsteht diesbezüglich aber aufgrund der immer weitergehenden technischen Möglichkeiten der Rückführung von anonymisierten Daten zu konkreten Personen.

Dieses breite Verständnis des sachlichen Anwendungsbereichs der DSGVO setzt sich bei der Regelung des räumlichen Anwendungsbereichs fort. Im Inneren der EU spielt für die Anwendbarkeit der DSGVO ein grenzüberschreitender Bezug keine Rolle; wie sich bereits aus Art 1 Abs 3 DSGVO ergibt, ist diese auch auf rein innerstaatliche Sachverhalte anzuwenden. Zusätzlich weitet Art 3 Abs 2 DSGVO den Anwendungsbereich weit über die Union hinaus aus. So ist die Verordnung ebenso für die Verarbeitung personenbezogener Daten anwendbar, wenn keine Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der Union besteht, sondern Waren oder Dienstleistungen an in der Union befindliche Personen angeboten werden oder das Verhalten von Personen in der Union beobachtet wird. Damit verbunden ist gem Art 27 DSGVO auch die Verpflichtung, sowohl für Verantwortliche als auch für Auftragsverarbeiter schriftlich einen Vertreter in der Union zu benennen, der in einem Mitgliedstaat, auf den sich das Angebot oder die Beobachtung aus dem Drittstaat bezieht, niedergelassen sein muss.[15]

Während die Durchsetzbarkeit dieses – letztlich globalen – Anspruchs unklar bleibt, wird damit jedenfalls ein weitgehender Anspruch zur Einhaltung der DSGVO im internationalen Datentransfer durch Private erhoben. Schließlich verlangt die Verordnung auch die Einhaltung der DSGVO von Unternehmen, die in der Union niedergelassen sind, wenn diese die Daten international an andere Personen übermitteln möchten.[16]

2. Besonderer Schutz

Im Zusammenhang mit dem Anwendungsbereich der DSGVO sind Besonderheiten in Hinblick auf zwei Personengruppen hervorzuheben: einerseits die (für Österreich spezifische) Einschränkung des Schutzes für juristische Personen und andererseits die spezielle Regulierung des Datenschutzes für Kinder.

Durch die Nichtanpassung des Grundrechts auf Datenschutz bleibt auf verfassungsrechtlicher Ebene ein Restbereich des Datenschutzes für juristische Personen (als Betroffene) bestehen. Dieser wird aber nicht mehr durch einfachgesetzliche Regelungen konkretisiert, wodurch die (schon bisher geringe) Bedeutung dieses österr Spezifikums in der Praxis noch weiter zurückgehen wird.[17]

8) Art 4 Z 1 DSGVO.
9) Art 4 Z 2 DSGVO (vormals „Auftraggeber“).
10) Dies kann alleine oder gemeinsam mit anderen geschehen. Zur Konstellation mehrerer Verantwortlicher s Art 26 DSGVO.
11) Art 4 Z 8 DSGVO (vormals „Dienstleister“).
12) Siehe Art 4 Z 6 DSGVO der das Dateisystem als „jede strukturierte Sammlung personenbezogener Daten [ansieht], die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird“.
13) Bemerkenswerterweise erweitert aber § 4 DSG (hier und in weiterer Folge idF des Datenschutz-Anpassungsgesetz 2018) den Anwendungsbereich auf die gesamte staatliche Verwaltung. Davon ausgenommen wird nur das Sicherheitspolizei- und Strafrecht, für das die §§ 36–61 DSG ein besonderes Regelungsregime vorsehen und auf das in diesem Zusammenhang nicht näher eingegangen wird.
14) Siehe *Lachmayer,* ÖJZ 2018, 112.
15) Die gem Art 27 Abs 2 DSGVO damit verbundenen Ausnahmen bleiben restriktiv, womit bereits bei einer nicht gelegentlichen Verarbeitung die Verpflichtung besteht, einen Vertreter zu benennen.
16) Art 44–50 DSGVO.
17) Siehe zu dieser Debatte etwa *Anderl/Hörlsberger/Müller,* Kein einfachgesetzlicher Schutz für Daten juristischer Personen, ÖJZ 2018, 14; *Knyrim/Maurer,* Der Datenschutz für die juristische Person bleibt bestehen (Interview mit *E. Riedl*), Dako 2017, 74; *Leissler,* Datenschutz für juristische Personen – ein Blick in die Zukunft, ecolex 2017, 1222.

Auch wenn sich am bisher bestehenden Schutz für Kinder durch die DSGVO nichts ändert, so regelt Art 8 DSGVO zumindest die Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft. Im Hinblick auf den durch die DSGVO für die Mitgliedstaaten geschaffenen Spielraum zwischen der Vollendung des 13. Lebensjahrs bis hin zur Vollendung des 16. Lebensjahrs hat sich der österr Gesetzgeber für eine Mittelvariante entschieden. § 4 Abs 4 DSG sieht vor, dass die Einwilligung *„zur Verarbeitung personenbezogener Daten des Kindes rechtmäßig ist, wenn das Kind das vierzehnte Lebensjahr vollendet hat"*. Die unionsrechtlich gestellten Bedingungen an diese Übertragung der Einwilligungsmöglichkeit von den Erziehungsberechtigten auf das Kind sehen vor, dass dem Jugendlichen ein *„Angebot von Diensten der Informationsgesellschaft"* 1. direkt 2. gemacht wird. Beide Voraussetzungen sind im datenschutzrechtlichen Kontext weit zu verstehen. Insb die erste Kategorie ist nicht etwa auf Angebote aus dem Internet beschränkt. Der Verantwortliche ist jedenfalls verpflichtet, *„unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen"* zu unternehmen, dass die Einwilligung der Erziehungsberechtigten (wenn erforderlich) erfolgt.

C. Die Pflichten des datenschutzrechtlich Verantwortlichen

1. Die Verantwortlichkeit des Verantwortlichen

Die DSGVO sieht eine Reihe neuer Pflichten für den datenschutzrechtlich Verantwortlichen vor. Ausgangspunkt ist dabei – wie erwähnt – die Herstellung geeigneter technischer und organisatorischer Maßnahmen iSd Art 24 Abs 1 DSGVO. Als zentrale Pflichten sind insb folgende zu nennen:

- interne Dokumentationspflichten (insb die Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten gem Art 30 DSGVO),[18]
- Risikoabwägung und Datenschutz-Folgenabschätzung gem Art 35 f DSGVO,
- technische und organisatorische Maßnahmen der Datensicherheit gem Art 32 DSGVO,
- externe Informationspflichten (insb gem Art 12 ff DSGVO oder iZm der Einwilligung gem Art 7 DSGVO)[19] und Verpflichtung zur *data breach notification* gem Art 33 f DSGVO,
- Durchführung von Verfahren zur Abwicklung der Betroffenenrechte,
- Verschwiegenheitspflichten gem § 6 DSG,
- Festlegung und Dokumentation sämtlicher hier genannter Maßnahmen iSd Art 24 Abs 1 DSGVO.[20]

Diese Pflichten treffen grundsätzlich nicht nur datenschutzrechtlich Verantwortliche, sondern auch die Auftragsverarbeiter.[21]

2. Von der Melde- zur Dokumentationspflicht

Die DSGVO schafft eine signifikante Ausweitung der Pflichten der datenschutzrechtlich Verantwortlichen. Das bestehende Modell der Meldung an die DSB unter Ausnahmen für Standardanwendungen im Rahmen der Standard- und MusterVO wurde ersetzt durch ein Geflecht von Dokumentationspflichten, die ihren Ausgangspunkt in dem Verzeichnis der Verarbeitungstätigkeiten gem Art 30 DSGVO finden.

Im Zentrum der neu geschaffenen Verpflichtungen stehen interne Dokumentationspflichten. Gem Art 30 DSGVO wird es allen Verantwortlichen auferlegt, ein Verzeichnis aller datenschutzrechtlichen Verarbeitungstätigkeiten, die in ihrer Zuständigkeit liegen, zu erstellen. Damit verbunden sind die Erfassung der Zwecke der Verarbeitung, die Kategorien betroffener Personen und Empfänger, die Fristen für die Löschung verschiedener Kategorien sowie eine allgemeine Beschreibung der mit der Verarbeitung verbundenen technisch-organisatorischen Maßnahmen.[22] Dieses Verzeichnis ist auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen.

Für Unternehmen und Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, besteht gem Art 30 Abs 5 DSGVO eine Ausnahme von der Aufzeichnungspflicht, wenn eine Datenverarbeitung kein *„Risiko für die Rechte und Freiheiten der betroffenen Personen"* darstellt, *„nur gelegentlich erfolgt"* oder keine Verarbeitung besonderer Datenkategorien darstellt.[23] Diese Voraussetzungen zur Wahrnehmung der Ausnahme werden aber typischerweise nicht vorliegen. Sobald aber über 250 Mitarbeiter der Einrichtung zugerechnet werden können, sind selbst jene Datenverarbeitungen dokumentarisch zu erfassen, die nur gelegentlich vorgenommen werden.

Die Dokumentationspflichten beschränken sich allerdings nicht auf die Erstellung des Verzeichnisses der Verarbeitungstätigkeiten, sondern beziehen sich auf alle technischen und organisatorischen Maßnahmen iSd Art 24 Abs 1 DSGVO, die im Rahmen der Verpflichtungen des datenschutzrechtlich Verantwortlichen gesetzt werden. Insb sind damit auch jene Bereiche angesprochen, die in den folgenden Abschnitten näher behandelt werden.

3. Risikoabwägung und Datenschutz-Folgenabschätzung

Auf Basis der im Verzeichnis der Verarbeitungstätigkeiten ermittelten Datenverarbeitungen ist es für Unternehmen erforderlich, eine Risikobewertung(-abwägung) vorzunehmen,[24] an der vielfältige weitere Verpflichtungen der DSGVO anknüpfen. Es ist daher für das jeweilige Unternehmen erforderlich festzustellen, inwieweit von der jeweiligen Datenverarbeitung, die nach dem Zweck der Verarbeitung differenziert wird,

18) Siehe dazu sogleich unter C.2.
19) Siehe dazu sogleich unter C.5.
20) Siehe dazu sogleich unter C.2.
21) Auf die spezifischen Fragestellungen der Auftragsverarbeiter sowie auf das Verhältnis zwischen Verantwortlichen und Auftragsverarbeiter kann in diesem Zusammenhang nicht näher eingegangen werden; s dazu etwa *Anderl/Tlapak,* Vom Dienstleister zum Auftragsverarbeiter – was ändert sich mit der DSGVO? ZTR 2017, 59.
22) Siehe Art 30 Abs 1 DSGVO; auch für Auftragsverarbeiter des öffentlichen Dienstes gelten gem Art 30 Abs 2 DSGVO entsprechende Dokumentationspflichten.
23) Siehe dazu näher unter *Lachmayer,* ÖJZ 2018, 112.
24) Siehe ErwGr 77.

„ein Risiko für die Rechte und Freiheiten der betroffenen Personen" ausgeht. Ausgangspunkt dieser Betrachtung sind die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung.[25] Diese können bereits selbst erhöhte Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten. Darüber hinaus sind aber auch die unterschiedlichen Eintrittswahrscheinlichkeiten und die Schwere der Risiken bei der Abwägung zu berücksichtigen. Je nach Ergebnis dieser Risikoabwägung sind geeignete technische und organisatorische Maßnahmen zu setzen, die in einem angemessenen Verhältnis zu diesen Verarbeitungstätigkeiten und den damit verbundenen Risiken stehen müssen.[26]

Als eine besondere Form der Risikoabwägung sieht Art 35 DSGVO die sog *„Datenschutz-Folgenabschätzung"* vor, die durchzuführen ist, wenn ein hohes Risiko für die Rechte und Freiheiten Betroffener vorliegt. Diese setzt damit implizit bereits eine allgemeine Risikobewertung bzw -abwägung voraus. Die Datenschutz-Folgenabschätzung enthält gem Art 35 Abs 7 DSGVO zumindest eine *„systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung"*, *„eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge"*, *„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* [wird]".

Verpflichtend ist eine solche Datenschutz-Folgenabschätzung insb dann durchzuführen, wenn eine systematische und umfassende Bewertung persönlicher Aspekte betroffener Personen (etwa Profiling) vorgenommen wird, eine umfangreiche Verarbeitung besonderer Kategorien von Daten erfolgt oder eine systematische und umfangreiche Überwachung öffentlich zugänglicher Bereiche vorgenommen wird. Eine von der DSB zu erstellende Positivliste, wann jedenfalls eine Datenschutz-Folgenabschätzung durchzuführen ist, fehlt ebenso wie eine Negativliste, die von der DSB erstellt werden kann, wann keine Datenschutz-Folgenabschätzung erforderlich ist.

Nur wenn nach Durchführung der Datenschutz-Folgenabschätzung der Verantwortliche – trotz hohem datenschutzrechtlichen Risiko – *„keine Maßnahmen zur Eindämmung des Risikos trifft"*, hat dieser gem Art 36 DSGVO vor Verarbeitung der personenbezogenen Daten die DSB zu konsultieren. Die Konzeption der *„vorherigen Konsultation"* erschwert den Zugang zur DSB, da die Voraussetzungen für eine derartige Konsultation bereits das Eingeständnis in sich tragen, dass eine Verarbeitung nicht im Einklang mit der DSGVO steht. Eine entsprechende Involvierung der DSB erscheint daher nicht praxistauglich ausgestaltet und wird daher in der Praxis kaum relevant werden. Nichtsdestoweniger besteht – insb bei Beschwerden vor der DSB – die Notwendigkeit für Verantwortliche nachzuweisen, dass bei einem hohen Datenschutzrisiko eine Datenschutz-Folgenabschätzung durchgeführt wurde sowie welche technischen und organisatorischen Maßnahmen im Anschluss daran gesetzt wurden, um das entstandene Risiko zu reduzieren.

4. Technische und organisatorische Maßnahmen

Wie bereits deutlich geworden ist, handelt es sich bei den *„technischen und organisatorischen Maßnahmen"* (TOM) um einen Zentralbegriff der DSGVO. Eine Konkretisierung dieser Maßnahmen findet sich an unterschiedlichen Stellen im Rahmen der DSGVO. IdZ ist etwa Art 25 DSGVO zu erwähnen, der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen einmahnt. So kann der Verantwortliche bereits bei der Ausgestaltung der eingesetzten Technik (data protection by design) sowie bei der Auswahl datenschutzfreundlicher Voreinstellungen (data protection by default) einen wesentlichen Beitrag zum Datenschutz leisten. Dem Einsatz von Pseudonymisierung, also der Trennung von Personenbezug und Datenverarbeitung, kommt in diesem Kontext ebenso besondere Bedeutung zu.

Mit technischen Maßnahmen sind insb die Verpflichtung zur Datensicherheit gem Art 32 DSGVO angesprochen. Je nach Risiko der Datenverarbeitung ist ein angemessenes Schutzniveau in Hinblick auf die Datensicherheit zu gewährleisten. Art 32 Abs 1 DSGVO sieht insb folgende Maßnahmen als relevant an: *„die Pseudonymisierung und Verschlüsselung personenbezogener Daten"*; *„die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen"*; *„die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen"* sowie *„ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung"*. Als allgemeine Zielsetzung im Zusammenhang mit der Datensicherheit betont Art 32 Abs 2 DSGVO, dass es die Vernichtung, den Verlust oder die Veränderung von personenbezogenen Daten zu verhindern gilt, unabhängig davon, ob die Verletzung des Datenschutzes unbeabsichtigt oder unrechtmäßig war oder sie in Form unbefugter Offenlegung oder durch unbefugten Zugang zu personenbezogenen Daten entstanden ist.

Organisatorische Maßnahmen beziehen eine Managementstrategie des Unternehmens zur Implementierung der notwendigen, in der DSGVO vorgesehenen Elemente des Datenschutzes ebenso mit ein wie etwa Schulungsmaßnahmen oder Informationen an MitarbeiterInnen. Eine organisatorische Maßnahme kann aber beispielsweise auch in der Einrichtung eines Datenschutzbeauftragten bestehen. Auch wenn gem Art 37 ff DSGVO im privaten Bereich nur in sehr seltenen Fällen[27] eine verpflichtende Einsetzung eines

25) So Art 24 Abs 1 DSGVO.
26) Art 24 Abs 2 DSGVO.
27) Gem Art 37 Abs 1 DSGVO hat die Benennung eines Datenschutzbeauftragten – abgesehen vom öffentlichen Bereich – zu erfolgen, wenn „die Kerntätigkeit des Verantwortlichen [...] 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 [...] in der umfangreichen Verarbei-

Datenschutzbeauftragten vorgesehen ist, kann die Einbindung eines Datenschutzbeauftragten eine adäquate organisatorische Maßnahme darstellen, um ein spezifisches Risiko der Datenverarbeitung zu adressieren. Sobald aber ein Datenschutzbeauftragter eingerichtet wird, sind auch die gem Art 37 ff DSGVO vorgesehenen Bedingungen zu berücksichtigen.

Technische und organisatorische Maßnahmen eröffnen auch das Potential für Standardisierungen und Zertifizierungen gem Art 42 DSGVO. Mit datenschutzspezifischen Zertifizierungsverfahren sowie mittels Datenschutzsiegeln und -prüfzeichen soll eine praxisorientierte Umsetzung der DSGVO ermöglicht werden. Die aus der Verordnung folgenden Verpflichtungen des Verantwortlichen werden allerdings durch die Zertifizierung nicht gemindert. Insofern wird sich weisen, inwieweit diese Möglichkeiten in der Praxis relevant werden. Verhaltensregeln gem Art 40 DSGVO ermöglichen es wiederum Verbänden und anderen Vereinigungen, für bestimmte Wirtschaftsbereiche spezifische Vorgaben zu entwickeln.

5. Informationspflichten und Data Breach Notification

Neben den umfangreichen internen Dokumentationspflichten bestehen gem Art 12 ff DSGVO auch externe Informationspflichten, um gegenüber den betroffenen Personen Transparenz zu gewährleisten (die bisher durch das Datenschutzverarbeitungsregister umgesetzt wurde). Gem Art 12 Abs 4 DSGVO sind Informationen an die Betroffenen grundsätzlich unentgeltlich zur Verfügung zu stellen. Derartige Informationen müssen insb zum Zeitpunkt der Erhebung von personenbezogenen Daten zur Verfügung gestellt werden. Der *„Verantwortliche erleichtert [damit] der betroffenen Person die Ausübung ihrer Rechte"*.[28] Diese Informationen beziehen sich gem Art 13 Abs 1 DSGVO insb auf den Namen und die Kontaktdaten des Verantwortlichen, die Zwecke und Rechtsgrundlage der Verarbeitung sowie gegebenenfalls auf Empfänger oder Übermittlungen in Drittländer (und spiegeln auf diese Weise die bereits durch das Verzeichnis der Verarbeitungstätigkeiten bestehenden internen Dokumentationen wider). Darüber hinaus sind gem Art 13 Abs 2 DSGVO auch die Dauer der Speicherung, das Bestehen von Rechten sowie gesetzliche Grundlagen zu nennen. Eingeschränkt werden die Informationspflichten nur im Falle, dass die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden.[29]

Neben der aus der Erfüllung eines Vertrags stammenden Rechtmäßigkeit der Datenverarbeitung[30] steht die Einwilligung der betroffenen Person[31] im Zentrum der Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch private Unternehmen.[32] Die Vorgaben an die Einwilligung konkretisiert Art 7 DSGVO, die jedenfalls *„in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache"* vorzunehmen ist, wobei eine jederzeitige Widerrufsmöglichkeit bestehen muss, über die der Betroffene auch aufzuklären ist.[33]

Eine andere Form der Informationspflicht betrifft die schon bisher bestehende Data Breach Notification, die gem Art 33 DSGVO eine Meldung binnen 72 Stunden durch den Verantwortlichen an die zuständige Aufsichtsbehörde vorsieht, wenn es zu einer Verletzung des Schutzes personenbezogener Daten gekommen ist. Damit sind etwa Fälle von Hacking ebenso angesprochen wie der Verlust eines USB-Sticks im öffentlichen Raum, der personenbezogene Daten enthalten hat. Der Verantwortliche hat jedenfalls die Verletzungen des Datenschutzes zu dokumentieren und der Aufsichtsbehörde den Zugriff auf diese Dokumentation zu ermöglichen.

6. Die Rechte der betroffenen Personen

Auf Basis der verstärkten Informationspflichten des Verantwortlichen stehen weiterhin die klassischen Rechte der betroffenen Personen, insb ein Recht auf Auskunft, Berichtigung und Löschung, zur Verfügung. Die Frist für die Beantwortung des Auskunftsersuchens wurde auf ein Monat reduziert, wobei diese Frist um zwei weitere Monate verlängert werden kann, wenn *„dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist"*[34]. Überdies wird die Auskunftspflicht bei exzessiven Anträgen einer Person eingeschränkt. Bestehen Zweifel an der Identität der betroffenen Person, so kann der Verantwortliche zur Bestätigung der Identität zusätzliche Informationen anfordern. Der Verantwortliche hat eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen. Eine Erweiterung sieht idZ Art 20 DSGVO mit dem Recht auf Datenübertragbarkeit vor. Basiert die Datenverarbeitung auf Einwilligung oder Vertrag und findet diese mithilfe automatisierter Verfahren statt, so besteht für die betroffene Person das Recht, die sie betreffenden personenbezogenen Daten *„in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln"*. Die damit verbundenen technischen Herausforderungen können mitunter beachtlich sein und sind daher für Unternehmen von besonderer Bedeutung.

Das Recht auf Berichtigung[35] besteht ebenso wie das Recht auf Löschung[36] weiterhin. Ein damit verbundenes Recht auf Vergessenwerden, wie es in Klammer und unter Anführungszeichen bei Art 17 DSGVO Erwähnung findet, wurde damit allerdings nicht umgesetzt. Es bleibt daher vielmehr bei der rechtlichen Verpflichtung, bei Wegfall des Zwecks der Verarbeitung die damit verbundenen personenbezogenen Daten zu löschen, und dem korrespondierenden Recht

tung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht".

28) Art 12 Abs 2 DSGVO.
29) Siehe Art 14 DSGVO.
30) Art 6 Abs 1 lit b DSGVO.
31) Art 6 Abs 1 lit a DSGVO.
32) Vereinzelt wird darüber hinaus auch die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung gem Art 6 Abs 1 lit c DSGVO relevant.
33) Art 7 Abs 3 DSGVO.
34) Art 12 Abs 3 DSGVO.
35) Art 16 DSGVO.
36) Art 17 DSGVO.

der betroffenen Person, diese Löschung einzufordern. Eine technische Lösung, die einen automatisierten Prozess der Löschung nach einem vorher festgelegten Ablaufdatum hervorruft, ist damit nicht verbunden.

7. Zwischenresümee: Datenschutz-Compliance für Unternehmen

Aus Unternehmenssicht zeigen sich deutlich erhöhte Verpflichtungen im Rahmen interner administrativer Maßnahmen zur Gewährleistung des Datenschutzes. Diese erscheinen der Bedeutung personenbezogener Daten im Informationszeitalter des 21. Jh durchaus angemessen. Die damit verbundene Problematik einer angemessenen Datenschutz-Compliance hängt aber zentral von der weiteren Ausgestaltung der Überprüfung der oftmals vagen Formulierungen der DSGVO durch die jeweils zuständige nationale Aufsichtsbehörde ab. Aufgrund der an die Verpflichtungen geknüpften hohen verwaltungsstrafrechtlichen Geldbußen entsteht aber für Unternehmen auf diese Weise ein hohes Compliance-Risiko, das durch wirtschaftlich vertretbare Maßnahmen zu keiner Garantie der vollständigen Einhaltung der Regeln der DSGVO führen kann.

In diesem Spannungsfeld besteht aber umgekehrt für Unternehmen die Möglichkeit, an den unterschiedlichen Verpflichtungen der DSGVO anzusetzen und damit den Nachweis zu erbringen, dass für das jeweilige Unternehmen der Schutz personenbezogener Daten einen integralen Bestandteil des Managements darstellt. Aufbauend auf dem Verzeichnis der Verarbeitungstätigkeiten und den damit verbundenen Risikoanalysen können die internen technischen und organisatorischen Maßnahmen so implementiert werden, dass sie die Prinzipien des Datenschutzrechts gewährleisten. Daran anschließend kann die Erfüllung von Informationspflichten ebenso wie die Vertiefung bestehender Strukturen zur Gewährleistung der Rechte von betroffenen Personen die datenschutzrechtlichen Verpflichtungen abrunden.

Der DSGVO gelingt es auf diese Weise, jedenfalls den unternehmensbezogenen Bereich[37] für das Thema Datenschutz zu sensibilisieren. Es liegt sodann an der finanziellen, personellen und sonstigen Ressourcenausstattung der nationalen DSB, um eine Effektuierung der Vorgaben gewährleisten zu können.

8. Sonderregime der DSGVO und österr Spezifika

a) Sonderregelungen in der DSGVO

Über die allgemeinen Regeln des Datenschutzes hinaus eröffnet es die DSGVO den Mitgliedstaaten, in unterschiedlichen sachlichen Zusammenhängen abweichende Regeln vorzusehen. Vorschriften für besondere Verarbeitungssituationen regeln Art 85 ff DSGVO etwa im Zusammenhang mit der Meinungsäußerungs- und Informationsfreiheit, der Datenverarbeitung im Beschäftigungskontext oder wissenschaftlichen Forschungszwecken. Gem Art 85 Abs 2 DSGVO können Mitgliedstaaten für *„die Verarbeitung, die zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt“,* Abweichungen von den Kernkapiteln vorsehen, wenn diese erforderlich sind. Die daran anknüpfende Bestimmung des § 9 DSG konkretisiert allerdings die Einschränkungen nicht, sondern verweist die Frage der Anwendbarkeit wiederum pauschal an die Verwaltung weiter. Insoweit ist fraglich, ob die nationale Regelung den verfassungsgesetzlichen Vorgaben im Hinblick auf das Legalitätsprinzip (hinreichende Bestimmtheit) Genüge tun kann. Im Gegensatz dazu konkretisiert § 7 DSG die Verarbeitung für wissenschaftliche Forschungszwecke, indem etwa eine Genehmigung von Datenverarbeitungen durch die DSB vorgesehen wird. Diesbezüglich auffällig ist allerdings die Novellierung des FOG im Rahmen des *„Datenschutz-Anpassungsgesetzes – Wissenschaft und Forschung“,* das breitflächige Ausnahmen von der DSGVO sowie ua auch von § 7 DSG vorsieht.[38] Im Beschäftigungskontext kann an bestehende Regelungen, wie etwa § 96 Abs 1 Z 3 ArbVG, angeknüpft werden.

b) Sonderregelungen im DSG

Sonderregelungen finden sich aber nicht nur auf europäischer Ebene, sondern auch im nationalen DSG, wobei das Datenschutz-Anpassungsgesetz 2018 auch nationale Besonderheiten fortschreibt. Zu erwähnen ist einerseits das Datengeheimnis gem § 6 DSG ebenso wie die Bildverarbeitung gem §§ 12 f DSG. § 6 DSG konstituiert ein sog *„Datengeheimnis“,* das Verantwortliche, Auftragsverarbeiter ebenso wie MitarbeiterInnen verpflichtet, *„personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht“.*

§§ 12 f DSG weiten das bisherige Konzept der Videoüberwachung auf Bildaufnahmen inklusive mitverarbeiteter akustischer Informationen aus. Dieses Konzept folgt dem alten Modell des DSG 2000, womit auch die Frage nach der Vereinbarkeit mit der DSGVO anzusprechen ist. Die Regelung bezieht sich zentral auf den privaten Bereich und damit auf einen Kernbereich der DSGVO. Inwieweit die als Rechtfertigung herangezogenen Öffnungsklauseln gem Art 6 Abs 2 und 3 sowie Art 23 DSGVO als Rechtsgrundlage dienen können,[39] kann an dieser Stelle nicht näher erörtert werden; es sei aber dennoch angemerkt, dass die Unionsrechtskonformität der Regelung bei einer kritischen Untersuchung erst nachzuweisen wäre.

D. Rechtsdurchsetzung und Rechtsschutz

1. Vielfältige Herausforderungen für die Datenschutzbehörde

Trotz der regelmäßigen Erwähnung der hohen Geldbußen gem Art 83 DSGVO, die in *„jedem Einzelfall*

37) *Lachmayer,* Datenschutzrecht als Öffentliches Wirtschaftsrecht, in *Jahnel* (Hrsg), Jahrbuch Datenschutzrecht und E-Government (2013) 9.
38) Siehe den Ministerialentwurf 10/ME 26. GP.
39) Siehe 1164 BlgNR 25. GP 13 f.

wirksam, verhältnismäßig und abschreckend" ausgestaltet sein sollen, steht die DSB vor zahlreichen organisatorischen Herausforderungen, auf die abschließend in aller Kürze eingegangen werden soll. Nicht nur für die Unternehmen, sondern auch für die DSB bedeutet die Erfüllung der mit den Aufgaben- und Befugniserweiterungen entstandenen Kompetenzen eine große Herausforderung in personeller, finanzieller und organisatorischer Hinsicht. Dies wirkt auf private Unternehmen insoweit zurück, als die Kontaktmöglichkeiten mit der Behörde relativ gering sind. Die Ausübung der Aufgaben und Befugnisse wird aber auch zeigen, wie die DSB ihre Rolle zur Überwachung des Datenschutzes anlegen wird.

2. (K)Ein One-Stop-Shop?

Gem Art 56 Abs 6 DSGVO ist die federführende Aufsichtsbehörde der einzige Ansprechpartner des Verantwortlichen. Mit dieser Bestimmung soll den Unternehmen entgegengekommen und das sogenannte One-Stop-Shop-Prinzip umgesetzt werden. Die Vision eines einzigen Ansprechpartners knüpft allerdings an dem Konzept einer federführenden Aufsichtsbehörde an. Scheinbar – und so wirkt es auf den ersten Blick – besteht eine einzige federführende Aufsichtsbehörde, konkret am Ort der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen.[40] Sobald aber ein Unternehmen über mehrere Niederlassungen in der Union verfügt, beginnen komplexe definitorische Zusammenhänge ineinanderzugreifen, die die Idee des One-Stop-Shop rasch wieder relativieren. Gem Art 4 Z 16 lit a DSGVO wird die Hauptniederlassung nicht primär durch den Ort der Hauptverwaltung definiert, sondern nach jenem Ort, an dem „*die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten*" getroffen werden. Diese Definition setzt aber an der jeweiligen Verarbeitung personenbezogener Daten an, womit unterschiedliche Niederlassungen die Entscheidungen hinsichtlich der Zwecke und Mittel der jeweiligen Verarbeitung an unterschiedlichen Orten treffen können (etwa Personalentscheidungen am Ort der Hauptverwaltung, forschungsbezogene Datenverarbeitungen am Sitz der Forschungsniederlassung usw). Damit besteht aber je nach Datenverarbeitung eine andere Hauptniederlassung und damit verbunden eine andere federführende Aufsichtsbehörde. Die Feststellung der federführenden Aufsichtsbehörde hängt sodann von der Ermittlung durch die Behörde oder der Angabe des Unternehmens ab, wo die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung tatsächlich getroffen werden.[41]

3. Europäische Koordination

Über die nationale Ebene hinaus arbeiten die nationalen Aufsichtsbehörden in komplexen Kooperationsmechanismen zusammen, die der Vereinheitlichung des datenschutzrechtlichen Vollzugs dienen sollen.[42] Inwieweit die vorgesehenen Mechanismen nicht zu gegenseitigen Blockaden führen oder aber zu einem starken Netzwerk effektiver Datenschutzbehörden, wird sich weisen. An der Regelungsstruktur der DSGVO ist jedenfalls auffällig, dass eine starke administrative Kooperation der Verwaltungsbehörden etabliert wird, während die im Rechtsschutz nachfolgenden Gerichte in derartige Kooperationsansätze nicht eingebunden sind. Letztlich wird es am EuGH liegen, eine einheitliche Auslegung der DSGVO zu garantieren. Die damit verbundenen (längeren) Zeithorizonte bedeuten allerdings eine Herausforderung für die durch die DSGVO angestrebte Harmonisierung.

E. Ausblick

Die Entwicklungen des Datenschutzes bleiben dynamisch. Viele Vorgaben harren der Konkretisierung, etwa durch die Europäische Kommission, den Europäischen Datenschutzausschuss und die nationalen Datenschutzbehörden. Von diesen Entwicklungen hängt aber auch die konkrete Ausgestaltung des Datenschutzes im privaten Bereich ab. Bis dahin sind die Verantwortlichen im privaten Bereich, seien es Unternehmen oder aber auch etwa Vereine, gut beraten, ihre eigenen auf der DSGVO basierenden datenschutzrechtlichen Strategien im Rahmen ihrer Organisation umzusetzen, um der geforderten Datenschutz-Compliance Genüge zu tun.

40) Art 56 Abs 1 DSGVO.
41) Siehe dazu ausführlich *Lachmayer,* Art 56 DSGVO, in *Eßer/Kramer/v. Lewinski* (Hrsg), Auernhammer – Datenschutz-Grundverordnung[6] (2018, in Druck).
42) Siehe *v. Lewinski,* Datenschutzaufsicht in Europa als Netzwerk, NVwZ 2017, 1483.

➜ In Kürze

Der Beitrag setzt sich mit Fragen der DSGVO iZm privaten Unternehmen auseinander. Ausgehend von einem weiten sachlichen und räumlichen Anwendungsbereich stehen die vielfältigen Pflichten der datenschutzrechtlich Verantwortlichen im Vordergrund. Die zentrale Herausforderung besteht dabei in der Etablierung angemessener technischer und organisatorischer Maßnahmen, die den Schutz personenbezogener Daten gewährleisten sollen. Diese beinhalten interne Dokumentationspflichten und Maßnahmen zur Datensicherheit ebenso wie externe Informationspflichten und die Gewährleistung der Rechte der betroffenen Personen. Der durch die DSGVO avisierte One-Stop-Shop wird für transnationale Unternehmen mit mehreren Niederlassungen in der Union allerdings nur im Ausnahmefall zur Verfügung stehen.

➜ Zum Thema

Über den Autor:
Univ.-Prof. (SFU) Dr. Konrad Lachmayer ist Professor für Öffentliches Recht, Europarecht und Grundlagen des Rechts an der Sigmund Freud Privatuniversität in Wien.
Kontaktadresse: Fakultät für Rechtswissenschaften, Sigmund Freud Privatuniversität, Freudplatz 1, 1020 Wien. E-Mail: konrad.lachmayer@jus.sfu.ac.at, Internet: www.lachmayer.eu
Vom selben Autor erschienen:
Die DSGVO im öffentlichen Bereich. Europarechtliche Vorgaben an die staatliche Verwaltung, ÖJZ 2018, 112; Das EU-US Privacy Shield Konzept. Zum Umgang mit rechtskulturellen Unterschieden im Datenschutzrecht, JusIT 2017, 23; *Lachmayer* in *Eßer/Kramer/v. Lewinski* (Hrsg), Auernhammer-Kommentar. Datenschutz-Grundverordnung[6] (2018) Art 56, Art 60–62 DSGVO. ➜

Literatur:
Gantschacher/Jelinek/Schmidl/Spanberger (Hrsg), Datenschutz-Grundverordnung. Kommentar (2017); *Feiler/Forgó,* EU-DSGVO. Kurzkommentar (2017); *Knyrim* (Hrsg), Datenschutz-Grundverordnung. Praxishandbuch (2016); *Eßer/Kramer/v. Lewinski* (Hrsg), Auernhammer-Kommentar. Datenschutz-Grundverordnung[6] (2018).