Mag. Judith Leschanz
Geschäftsführerin der Secur-Data Betriebsberatungs-GmbH; Vorstandsvorsitzende des Vereins österreichischer betrieblicher und behördlicher Datenschutzbeauftragter; Group Data Officer der Telekom Austria AG

Mag. Katja Wyrobek
Senior Consultant und Juristin bei der Secur-Data Betriebsberatungs-GmbH

Datenschutz nach der Datenschutz-Grundverordnung

Zur Notwendigkeit eines Datenschutz-Managementsystems

1. Einleitung

Bevor man ein Datenschutz-Managementsystem in Angriff nehmen kann, ist es wichtig, sich zu vergegenwärtigen, mit welcher Rechtslage man sich auseinandersetzen muss. Dieser Artikel bietet Ihnen eine Einleitung zum Thema „Datenschutz" und soll Ihnen die Grundzüge der Datenschutz-Grundverordnung (DSGVO)[1] erläutern. In Zahlen besteht die DSGVO aus 11 Kapiteln mit 99 Artikeln, einschließlich 173 Erwägungsgründen, die sich jeweils auf einen oder sogar mehrere Artikel beziehen und diese erläutern bzw konkretisieren und normativen Charakter besitzen. Dazu gibt es jeweils noch nationalstaatliche Datenschutzgesetze in den EU-Ländern, Verordnungen und andere Sondergesetze, die beispielsweise die Verfahren regeln und Strafbestimmungen konkretisieren oder Tatbestände konkretisieren (zB im Arbeitsrecht).

Zunächst ist allerdings zu klären, in welchem Kontext die DSGVO anwendbar ist. Anders als die frühere Datenschutz-Richtlinie[2] gilt die DSGVO als EU-Verordnung unmittelbar in jedem Mitgliedstaat der EU. Sie hat allgemeine Geltung und ist in allen Teilen verbindlich einzuhalten. Das unterscheidet sie grundsätzlich von der einer sogenannten EU-Richtlinie, die in nationale Gesetze umzusetzen ist und daher fragmentierte Rechtslagen erzeugt. Den Mitgliedstaaten wurden jedoch über sogenannte Öffnungsklauseln bestimmte Freiheiten eingeräumt, Sachverhalte rechtlich individuell-nationalstaatlich zu regeln. Obwohl die DSGVO eine EU-Verordnung ist, kommt ihr durch die 69 Öffnungsklauseln Richtliniencharakter zu. Österreich hat beispielsweise als Öffnungsklausel das Alter für eine datenschutzrechtliche Selbstbestimmung mit 14 Jahren festgelegt, deren Rahmen 13 bis 16 Jahre betrug. Daher gilt, dass eine Einwilligung für die Datenverarbeitung bei Diensten der Informationsgesellschaft in Österreich ab 14 Jahren ohne Zustimmung der Erziehungsberechtigten erteilt werden kann. Als weitere Öffnungsklausel ist das sogenannte Medienprivileg zu nennen, das journalistisch tätige Akteure, unabhängig von ihrer Rechtsform, von einem Großteil des Anwendungsbereichs der DSGVO ausgenommen hat.

2. Begriffsbestimmungen

2.1. Vorbemerkung

Die DSGVO ist in 11 Kapitel eingeteilt, die unterschiedliche Adressaten betreffen. Während die allgemeinen Bestimmungen und Grundsätze der Kapitel I und II sämtliche Rechtsunterworfene treffen, ist Kapitel III insbesondere für das Verhältnis von Betroffenen und Verantwortlichen relevant.

2.2. Die Rollenverteilung in der DSGVO

Unter dem *„Verantwortlichen"* versteht man den Hauptverantwortlichen der Datenverarbeitung, also den Betreiber der Datenanwendung. Ausschlaggebend ist dabei die Autonomie, über Zweck und Mittel der Verarbeitung von personenbezogenen Daten zu entscheiden. Dieser Autonomie mangelt es einem sogenannten *„Auftragsverarbeiter"*, der ebenfalls eine natürliche oder juristische Person sein kann, allerdings nicht frei, sondern auf ausdrückliche Weisung und somit *„im Auftrag"* eines Verantwortlichen Daten verarbeitet und keine eigene Verfügungsgewalt über Datenanwendung oder -verarbeitung besitzt.

Als dritte Rolle ist zudem die *„betroffene Person"* zu nennen. Sie ist Trägerin sogenannter personenbezogener Daten und genießt den Schutz der in der DSGVO gewährleisteten Rechte. Wichtig ist dabei die Unterscheidung natürlicher und juristischer Person. Im österreichischen Datenschutzgesetz (DSG) ist das Grundrecht auf Datenschutz in § 1 Abs 1 DSG als Jedermannsrecht ausgestaltet. Die DSGVO sieht in ihren Erwägungsgründen jedoch keinen Schutz für juristische Personen vor. Eine GmbH genießt nur das Recht auf Geheimhaltung, während das Grundrecht auf Datenschutz nur für Menschen gilt.

Als weitere Einschränkung ist das Datenschutzrecht für Verstorbene zu nennen. Es ist den Mitgliedstaaten im Rahmen einer oben genannten Öffnungsklausel freigestellt worden, auch Verstorbene als Träger des Datenschutzrechts auszustatten. Weder Österreich noch Deutschland haben Gebrauch von dieser Öffnungsklausel gemacht, was dazu führt, dass mit dem Tod einer natürlichen Person

das Datenschutzrecht entfällt. Persönlichkeitsrechtliche Aspekte bleiben davon jedoch unberührt, sodass bei der Verarbeitung personenbezogener Daten Verstorbener weiterhin Grenzen bestehen.

2.3. Personenbezogene Daten

Personenbezogene Daten kommen überall vor. Es wird zwischen *„personenbezogenen Daten“* und *„besonderen Kategorien personenbezogener Daten“* unterschieden. Alle Informationen, die sich auf eine bestimmbare natürliche Person beziehen lassen, gehören dazu. Neben Staatsbürgerschaft, Adresse und Geburtsdatum zählen auch Interessen, Kontostand, Verhalten, Anfragen und Korrespondenzen zu personenbezogenen Daten. Zu den besonderen Kategorien gehören unter anderem Allergieinformationen, Krankenstände, sexuelle Orientierung und Religionsbekenntnis.

2.4. Verarbeitung

Der Begriff *„Verarbeitung“* umfasst sämtliche Tätigkeiten, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Darunter fallen insbesondere das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Daher lässt sich zusammenfassend feststellen, dass von der Erhebung bis zur Auslesung über die Vernichtung personenbezogener Daten sämtliche denkbaren Prozesse von der Anwendung der DSGVO betroffen sind. Jede Visitenkarte, die man in sein Kontaktbuch überträgt, oder jeder Vertrag, der Name und Anschrift eines Betroffenen enthält, ist eine Form von Datenverarbeitung.

Dies sind nur ausgewählte Beispiele. Umfassende Datenverarbeitungsprozesse können auch die Übermittlung in ein Drittland beinhalten oder die Aufarbeitung in Datenbanken und die Verknüpfung mit anderen Datensätzen, die eine Profilbildung ermöglichen.

3. Die wichtigsten Änderungen im Überblick

Der Anwendungsbereich der DSGVO ist durch das sogenannte Marktortprinzip auch auf Anbieter ohne Niederlassungen oder Geschäftssitz in der EU erweitert worden. Damit fallen auch Anbieter aus den USA, Asien oder Afrika unter das Datenschutzregime der DSGVO, wenn sie ihre Waren oder Dienstleistungen an EU-Bürger richten, und es trifft sie die Verpflichtung, Vertreter für die jeweils zuständigen Datenschutzbehörden zu benennen. Denn grundsätzlich besteht der sogenannte One-Stop-Shop-Mechanismus, das heißt, dass insgesamt nur eine Behörde für ein Verfahren zuständig ist und sich im Rahmen der Amtshilfe mit anderen Behörden koordiniert und eine gemeinsame Verfahrensführung stattfindet.

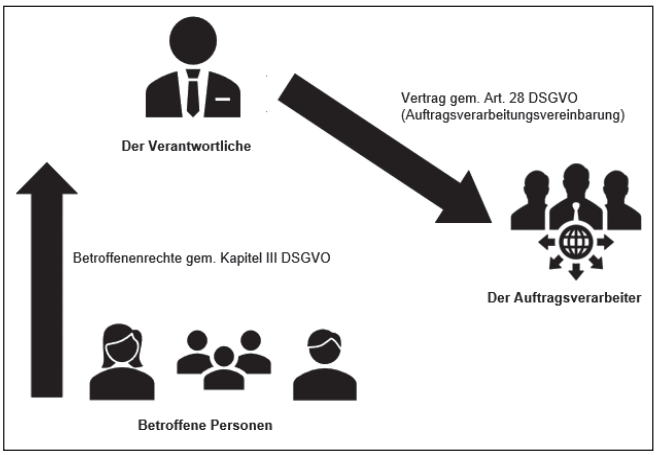

Abbildung 1

Neben Beschwerdeverfahren, in denen Betroffene sich an die Aufsichtsbehörde wenden können, wenn Betroffenenrechte nicht eingehalten werden, können weitere Verfahren aufgrund von Verstöße gegen die neuen, umfassenden Dokumentationspflichten eingeleitet werden. Darunter fällt unter anderem die Erstellung von Verzeichnissen von Verarbeitungstätigkeiten, die die Rolle des Verantwortlichen nochmals deutlich manifestieren. Während es in Österreich vor der DSGVO das sogenannte Datenverarbeitungsregister (DVR)[3] gab, ist der Verantwortliche nun selbst dafür zuständig, seine Datenverarbeitungsprozesse zu dokumentieren und auf Nachfrage auch der Behörde bereitzustellen. Es ist nicht vorgesehen, dass das Verarbeitungsverzeichnis an die Öffentlichkeit gelandet, da es sich um ein internes Dokumentationspapier handelt, das die Datenwendungen nach Datensubjekten, Kategorien und Empfängern gliedert.

Weitere Dokumentationspflichten sind im Hinblick auf die Datenschutz-Folgenabschätzung bei Verarbeitungsprozessen, die ein hohes Risiko für die Rechte und Freiheiten betroffener Personen bewirken, zu beachten. Hierzu hat die österreichische Datenschutzbehörde zwei Verordnungen erlassen: eine, die Prozesse und Sachverhalte beschreibt, für die jedenfalls eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V),[4] und eine, für die eine Datenschutz-Folgenabschätzung entfällt (DSFA-AV),[5] da sich das Risiko nur in einem geringen Ausmaß bewegt.

Beide Listen sind nicht abschließend formuliert und es sollte daher darauf geachtet werden, dass man im Zweifel seine eigene Risikoeinschätzung bei Datenverarbeitungsprozessen dokumentiert und begründet.

4. Strafen

Die mit Abstand wichtigste Änderung betrifft das Bußgeldregime und die hohen Strafen, die sich an der absoluten Summe von bis zu € 20 Mio orientieren oder 4 % des Umsatzes betragen können. Entscheidend ist dabei, welche Summe höher ist. So ist das aktuelle Erkenntnis der Datenschutzbehörde vom 23. 10. 2019 zu nennen, in dem die

Österreichische Post AG für die unrechtmäßige Verarbeitung von Daten zur Parteiaffinität von 2,2 Mio Betroffenen zu einer Strafe in Höhe von € 18 Mio verurteilt wurde (nicht rechtskräftig).[6]

Neben den umfassenden Dokumentationspflichten trifft von nun an auch viele Verantwortliche die Pflicht zur Bestellung eines Datenschutzbeauftragten. Dieser hat eine konkrete Funktionsbeschreibung und dient als Schnittstelle für Betroffene, Aufsichtsbehörde, Personal und Geschäftsführung, um eine rechtskonforme Datenverarbeitung zu überwachen und gegebenenfalls beratend zur Verfügung zu stehen und nach außen zu kommunizieren. Öffentliche Stellen haben zwingend einen Datenschutzbeauftragten zu bestellen. Bei privaten Stellen, das heißt Unternehmen und anderen privaten Einrichtungen, entscheiden die Art, der Umfang und die Frage, ob Datenverarbeitung als Kerntätigkeit durchgeführt wird, ob eine verpflichtende Bestellung notwendig ist oder lediglich mit einem sogenannten Datenschutzkoordinator gearbeitet werden kann.

5. Grundsätze der Datenverarbeitung

5.1. Allgemeines

Die wesentliche Säule der DSGVO findet sich in Kapitel II leg cit. Diese firmiert unter dem Titel *„Grundsätze der Datenverarbeitung“* und darf als Bedienungsanleitung für den rechtskonformen Umgang mit personenbezogenen Daten verstanden werden. Nur wenn sämtliche Aspekte beachtet werden, ist die Verarbeitung überhaupt zulässig und darf erfolgen. Verstöße gegen die Grundsätze der DSGVO zählen zu den teuersten Tatbeständen im DSGVO-Bußgeldkatalog. Aus diesem Grund ist es besonders wichtig, sich zu vergegenwärtigen, ob die Grundsätze wirklich eingehalten werden.

Abbildung 2

5.2. Grundsatz der Rechtmäßigkeit

Zu Beginn jeder Datenverarbeitung muss der Grundsatz der Rechtmäßigkeit eingehalten werden. Dazu zählen eine gültige Rechtsgrundlage sowie eine Verarbeitung nach Treu und Glauben. Weiters ist der Grundsatz der Transparenz zu beachten, wonach für die betroffene Person nachvollziehbar sein muss, wieso und auf welcher Rechtsgrundlage die Daten verarbeitet werden. Liegt beispielsweise keine gültige Rechtsgrundlage vor, ist dies ein Verstoß gegen den Grundsatz der Rechtmäßigkeit und führt gegebenenfalls zu einem Beschwerde- bzw Schadenersatz und/oder Bußgeldverfahren.

5.3. Grundsatz der Zweckbindung

Neben der Rechtmäßigkeit ist der Grundsatz der Zweckbindung von besonderer Bedeutung. Jede Datenerhebung hat einem festgelegten eindeutigen Zweck zu folgen, dem eine Rechtsgrundlage vorsteht. Das heißt, dass Daten nicht willkürlich für irgendwelche Zukunftsszenarien erhoben bzw gesammelt werden dürfen. Zudem beschränkt dieser Grundsatz die Weiterverarbeitung von Daten, für mit dem ursprünglichen Zweck nicht zu vereinbarende Datenverarbeitungen.

5.4. Grundsatz der Datenminimierung

Nachdem die Kombination aus Zweck und Rechtsgrundlage das erste Gerüst der Datenverarbeitung darstellt, ist weiters zu beachten, dass ein für den Zweck der Datenerhebung angemessenes Maß zu wahren ist. Es ist also schon im Vorhinein die Frage zu stellen, wie viele Daten man wirklich benötigt. „Datensammeln“ ist nicht mit den Grundsätzen der Datenverarbeitung zu vereinbaren und die Verarbeitung personenbezogener Daten muss auf das notwendige Maß beschränkt sein.

5.5. Grundsatz der Richtigkeit

Es ist nicht nur aus Eigeninteresse sinnvoll und zweckmäßig, sondern auch gesetzlich vorgeschrieben, dass personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand zu sein haben. Der Verantwortliche hat angemessene Maßnahmen zu treffen, damit personenbezogene Daten, die in Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden. Darunter zu verstehen sind sowohl Namens- und Adressänderungen als auch Negativmerkmale zur Bonität oder zum Kontostand.

5.6. Grundsatz der Speicherbegrenzung

Neben der Datenminimierung, also der Anfangsfrage, wie viele Daten man benötigt, basiert der Grundsatz der Speicherbegrenzung auf der Frage, wie lange man Daten verarbeiten darf. Die Frage nach gesetzlichen Aufbewahrungsfristen oder der „Lebensdauer“ von Daten muss der Verantwortliche gegebenenfalls im Einzelfall beantworten, allerdings hat jeder Betroffene das Recht, dass seine Daten ab einem bestimmten Zeitpunkt nicht mehr verarbeitet werden. Dazu zählt das Erreichen des Zwecks, der Ablauf von Löschfristen im Gesetz oder ein einfaches Löschbegehren, wenn die Interessen des Betroffenen überwiegen.

5.7. Grundsatz der Integrität und Vertraulichkeit

Neben den rechtlichen Anforderungen an eine rechtmäßige Datenverarbeitung treffen Verantwortliche auch die Verpflichtung zur Einrichtung von angemessenen Sicherheitsmaßnahmen. Während der Begriff *„Integrität“* vor einer Veränderung der Daten schützen soll, wird unter *„Vertraulichkeit“* gefordert, dass keine unbefugte oder unrechtmäßige Offenlegung personenbezogener Daten stattfindet. Es ist dafür Sorge zu tragen, dass personenbezogene Daten vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen geschützt werden.

5.8. Rechenschaftspflicht

Sämtliche oben geschilderten Grundsätze sind nicht nur einzuhalten, es trifft den Verantwortlichen auch eine Rechenschaftspflicht. Auf Anfrage durch eine Aufsichtsbehörde oder Gericht muss es jederzeit nachweisbar sein, dass die Datenverarbeitung stets im Einklang mit den Grundsätzen steht. Auch ein Verstoß gegen solche Nachweispflichten führt gegebenenfalls zu einem Bußgeldverfahren.

6. Rechtmäßigkeit der Datenverarbeitung

Die DSGVO ermöglicht es, in das Grundrecht auf Geheimhaltung und Privatsphäre einzugreifen. Dieser Erlaubnisvorbehalt basiert auf einer rechtmäßigen Verarbeitung. Neben den übergeordneten Grundsätzen ist im Besonderen immer eine gültige Rechtsgrundlage anzuführen.

Der Katalog an möglichen Rechtsgrundlagen ist abschließend in sechs Bedingungen geschildert. Alle Rechtsgrundlagen sind gleichwertig, allerdings nicht unterschiedlich nachhaltig bzw stark in ihrer Ausprägung. Zudem können mehrere Rechtsgrundlagen aufeinandertreffen. Es gilt jedoch grundsätzlich, dass die Datenverarbeitung ohne eine Rechtsgrundlage absolut unzulässig ist.

Abbildung 3

7. Warum braucht man ein Datenschutz-Managementsystem?

Aus den umfangreichen Rechenschaftspflichten des Verantwortlichen leitet sich die Notwendigkeit eines Datenschutz-Managementsystems ab. Datenschutz gestaltet sich nicht als einmaliges Ereignis, sondern bedarf einer nachhaltigen Überprüfung, Weiterentwicklung und Beobachtung (Zyklus). Nachdem die Grundlagen der DSGVO erläutert wurden, soll hier ein Überblick zum Aufbau eines Datenschutz-Managementsystems dargestellt werden. Für eine Vielzahl von KMU und Einzelunternehmen ist mit Hinblick auf die Organisationsgröße und den Umfang der Datenverarbeitung sinngemäß eine Abstufung zu treffen. Jedes Managementsystem sollte dennoch auf den Grundsätzen der Messbarkeit, Steuerung und Kontrolle aufgebaut werden.

8. Die drei Säulen eines Datenschutz-Managementsystems

8.1. Vorbemerkung

Ein einfaches Datenschutz-Managementsystem wird üblicherweise auf drei Säulen aufgebaut. Dazu zählen die präventive Säule, die operative Säule und die Remediation (Fehlermanagementsystem).

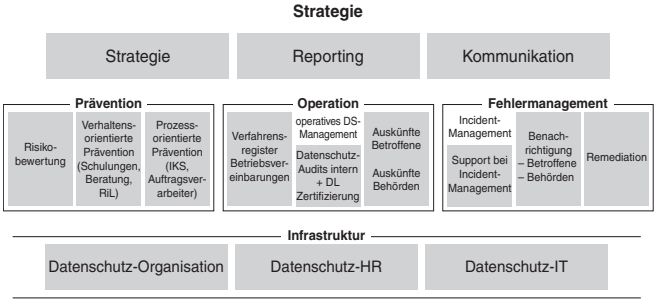

Abbildung 4

8.2. Prävention

Beginnt man ein Datenschutz-Managementsystem aufzubauen, startet man üblicherweise mit einer Risikoanalyse. Die wichtigsten Fragen belaufen sich auf die üblichen Risken beim Thema „Datenschutz“, die im eigenen Geschäftsfeld entstehen können, und wie diese zu klassifizieren sind. Nach dem Erkennen der Risiken sollte man interne Maßnahmen setzen, um diese zu minimieren.

Die präventive Säule im Datenschutz-Managementsystem unterteilt man am besten wiederum in zwei Punkte und verwendet eine prozessuale und eine verhaltensorientierte Prävention. Eine prozessuale oder technische Prävention verhindert auf technische oder organisatorische Weise die Möglichkeit einer Verletzung des Schutzes personenbezogener Daten (*data breach*). Als Beispiel kann man hier eine *Data-loss*-Prevention oder eine automatische Löschung von E-Mails oder ein Druckermanagementsystem nennen. Erstere verhindert, dass personenbezogene Daten aus Datenbanken manuell entzogen werden können und Zweiteres ist eine Regelfunktion in E-Mail-Programmen, welche diese automatisch nach einer bestimmten Zeit (zB nach

sechs Monaten oder einem Jahr nach Erhalt) löscht und in ein Archivsystem verschiebt. Ein Druckermanagement kann beispielsweise so ausgestaltet werden, dass Dokumente nur gedruckt werden können, wenn man weitere Sicherheitsmaßnahmen (wie beispielsweise Passwörter) implementiert. Man kann auf eine große Anzahl an technischen und organisatorischen Maßnahmen zurückgreifen, welche je nach Bedarf und Risiko angewendet werden können.

Verhaltensorientierte Prävention bedeutet, im Unternehmen eine Datenschutzkultur (*awareness*) zu schaffen und richtiges Verhalten zu schulen bzw zu fördern. Dies kann man mittels verschiedener Trainings (Präsenzschulung oder auch E-Learning), aber auch mittels Richtlinien bzw Arbeitsanweisungen ausgestalten. Wichtig ist dabei, dass den Mitarbeitern der rechtskonforme Umgang mit Daten und Datensicherheit gezeigt und laufend fortentwickelt wird.

8.3. Operatives Datenschutz-Managementsystem

Hierunter versteht man alle direkten Datenschutzaufgaben (wie zB die bereits angesprochenen Dokumentationspflichten, wie das Führen von Verarbeitungsverzeichnissen, die Gestaltung von Datenschutz-Folgenabschätzungen und die Ausübung der Betroffenenrechte). Insbesondere die Rechte auf Auskunft und Löschung werden in der Praxis am häufigsten ausgeübt und sollten daher prozessual so abgestimmt werden, dass eine fristgerechte und korrekte Erledigung gewährleistet ist. Je nach Größe des Betriebs und Umfang der Datenverarbeitung können zusätzlich etwaige Zertifizierungen von Datenanwendungen oder der Datensicherheit, Betriebsvereinbarungen für Datenschutz im Beschäftigungskontext sowie interne und externe Audits umgesetzt werden.

8.4. Fehlermanagement

Zu einem Datenschutz-Managementsystem gehören auch die Evaluation der Risiken und der Umgang damit. Die Organisation sollte prozessual so abgestimmt werden, dass jeder Beteiligte zB weiß, wie intern mit einem *data breach* umzugehen ist, damit eine rasche interne Behandlung gewährleistet ist. Zu beachten ist auch ein entsprechendes Krisenmanagement.

Ein Prozess zum Krisenmanagement sollte folgende Fragen beantworten:

- Wann wird eine Meldepflicht an die Behörde ausgelöst?
- Wie sieht die Meldung an die Behörde aus?
- Wann und wie sind die Kunden zu informieren?

Eine Meldung sollte sofort ab Kenntnis, spätestens aber innerhalb von 72 Stunden an die Behörde erfolgen. Damit diese Frist eingehalten werden kann, ist es wichtig, die Mitarbeiter so zu schulen, dass sie einen *data breach* sofort erkennen und an die richtige Stelle weiterleiten bzw melden. Danach muss (mit dem Verantwortlichen) rasch entschieden werden, ob es sich dabei überhaupt um einen *data breach* handelt. In der Praxis bewährt sich ein „Trockentraining" eines Datenschutzvorfalles, da dies im Ernstfall viel Zeit spart und bereits maßgeblich sensibilisiert.

Insgesamt ist daher jedem Verantwortlichen anzuraten, im Vorhinein seine Strukturen zu analysieren und Maßnahmen zu treffen.

9. Zusammenfassung

Die Anforderungen an Verantwortliche sind durch die DSGVO gestiegen, haben allerdings auch eine weitreichende Autonomie geschaffen. Der unmittelbare Handlungsbedarf ist bei nahezu jedem Unternehmen oder jeder öffentlichen Stelle bemerkbar. Das einheitliche Datenschutzregime unterliegt zwar an einigen Stellen einer nationalstaatlichen Fragmentierung, sodass dies für grenzüberschreitende Datenverarbeitungsprozesse zu beachten ist, führt jedoch zu einer objektivierbaren Datenverarbeitung mit klaren Rechten und Pflichten. Während die Rechte der betroffenen Personen wesentlich gestärkt wurden und die Wahrnehmung im Bereich Datenschutz sich stark verändert hat, treffen den Verantwortlichen und den Auftragsverarbeiter ebenfalls weitreichende Pflichten. Es ist jedem Verantwortlichen anzuraten, sich einen Überblick über seine Datenverarbeitungsprozesse zu verschaffen und nötigenfalls zu handeln. Die Einrichtung eines Datenschutz-Managementsystems ist je nach Betriebsgröße und Datenverarbeitungsumfang eine taugliche Maßnahme.

Anmerkungen:

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates 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), ABl L 119 vom 4. 5. 2016, S 1.

[2] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates 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] Siehe https://dvr.dsb.gv.at/at.gv.bka.dvr.public/DVRRecherche.aspx.

[4] Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V), BGBl II 2018/278.

[5] Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), BGBl II 2018/108.

[6] Siehe https://www.ots.at/presseaussendung/OTS_20191029_OTS0095/strafverfahren-gegen-oesterreichische-post-ag.

Korrespondenz:

Mag. Judith Leschanz
E-Mail: j.leschanz@secur-data.at

Mag. Katja Wyrobek
E-Mail: k.wyrobek@secur-data.at