Liebe Leserin,
lieber Leser,

in nunmehr rund zwei Monaten tritt eine grundlegende Novellierung des Datenschutzrechts in Kraft: Das Datenschutzgesetz 2000 wird durch eine Verordnung der Europäischen Union, die Datenschutz-Grundverordnung, ersetzt. Diese Verordnung gilt unmittelbar in den Mitgliedstaaten, steht jedoch in Anbetracht einer Vielzahl von Öffnungsklauseln – der Ermächtigung der Mitgliedstaaten, abweichende nationalstaatliche Regelungen zu treffen – einer gewissen Modifikation auf einzelstaatlicher Ebene offen. Damit einhergehen wird eine umfassende Novellierung des österreichischen Datenschutzgesetzes, dessen Grundsatzbestimmungen beibehalten, dessen überwiegender Teil aber unter Berufung auf vorgenannte Öffnungsklauseln neu gefasst wird. Angeschlossen möchten wir Ihnen einen in Anbetracht von Umfang und Komplexität der neuen Vorgaben verhältnismäßig kurzen Überblick über jene Rechtslage geben, die ab 25.5.2018 gilt.

Warum wir gerade Ihnen diese Informationen zukommen lassen? Weil die Datenschutz-Grundverordnung nicht etwa nur für Großunternehmen gilt, sondern einen äußerst weiten Anwendungsbereich hat: Ihr unterfallen auch klein- und mittelständische Unternehmen, Einzelunternehmen, Behörden und öffentliche Stellen, und alle anderen Personen, sofern Sie personenbezogene Daten nicht bei einer ausschließlich privaten oder familiären Tätigkeit verarbeiten. Wir alle werden daher eher früher als später mit dem neuen Datenschutzrecht in Kontakt treten, zumal die Automatisierung und Digitalisierung der westlichen Welt mit enormer Kraft voranschreiten.

Beim Studium der folgenden Seiten wünschen wir den Ihnen als Betroffene (siehe Punkt 3.) viel Spaß, den Verantwortlichen unter Ihnen hingegen vor allem gute Nerven.

Eva Schmelz / Dorian Schmelz

Schmelz Rechtsanwälte OG / Sitz: Klosterneuburg / FN 476430h des LG Korneuburg / ADVM-Code: P 210258 / UID: ATU 69433534
Geschäftskonto: IBAN AT91 3236 7000 0001 3391 / Fremdgeldkonto: IBAN AT68 3236 7000 0001 3417 / BIC RLNWATWW367

KONTAKT KLOSTERNEUBURG (KANZLEISITZ)
adr: 3400 Klosterneuburg, Stadtplatz 4 Top 2
tel: +43 2243 327 44
fax: +43 2243 284 23

KONTAKT WIEN
adr: 1090 Wien, Währinger Straße 16 Top 12
tel: + 43 1 946 11 60
fax: +43 2243 284 23

KONTAKT ONLINE
mail: office@rechtampunkt.at
web: www.rechtampunkt.at
fb: www.facebook.com/rechtampunkt

1. Die DSGVO im Überblick

Bereits am 4.5.2016 trat die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, besser bekannt als **Datenschutz-Grundverordnung** (**DSGVO**) in Kraft. Die Verordnung regelt und vereinheitlicht die Verarbeitung personenbezogener Daten natürlicher Personen, die Rechte von Betroffenen sowie und Pflichten der Verantwortlichen.

Die Bestimmungen der DSGVO gelten trotz ihres bereits vor knapp zwei Jahren erfolgten Inkrafttretens erst **ab 25.5.2018**. Bis zu diesem Zeitpunkt müssen alle Datenanwendungen an die neue Rechtslage angepasst werden. Wenngleich die DSGVO in allen Mitgliedstaaten der EU unmittelbar anwendbar ist, enthält sie zahlreiche Öffnungsklauseln, die den nationalen Gesetzgeber berechtigen, bestimmte Bereiche gesetzlich zu regeln. Es wird insofern auch künftig ein österreichisches Datenschutzrecht geben.

Von der DSGVO erfasst wird, wer in irgendeiner Art und Weise personenbezogene Daten verarbeitet, beispielsweise eine Kundenkartei führt, Rechnungen ausstellt oder Lieferantendaten speichert.

Mit der DSGVO geht gleichzeitig ein Paradigmenwechsel einher. Anders als bisher müssen nunmehr die **notwendigen Maßnahmen selbständig gesetzt werden**. Es gilt der Grundgedanke, dass jeder, der Daten verarbeitet, sich selbst um den Schutz derselben kümmern muss. Die Behörden kommen erst ins Spiel, wenn bereits etwas „schief gegangen" ist. Dies wird bei der großen Mehrheit von jenen Personen, die personenbezogene Daten systematisch verwenden, zu einem akuten und erheblichen Anpassungsbedarf führen, zumal die im Fall eines Verstoßes gegen die DSGVO drohenden Verwaltungsstrafen existenzbedrohende Höhen erreichen.

2. Vom Datenschutzgesetz zur DSGVO

Die ersten österreichischen Regelungen zum Datenschutzrecht stammen ursprünglich aus dem Jahr 1978. Im Jahr 2000 erfolgte mit dem Datenschutzgesetz 2000 eine grundregelnde Neufassung des österreichischen Datenschutzrechts. Das österreichische Datenschutzrecht ist also überraschend alt und in mancherlei Hinsicht nicht optimal für das 21. Jahrhundert geeignet.

Der Gesetzgeber entschied sich einst für die Einführung eines Datenverarbeitungsregisters (DVR), in dem jeder Unternehmer die von ihm automationsunterstützt verarbeiteten Daten nach Art und Zweck einzutragen hatte. Es sollte öffentlich erkennbar sein, wer welche Daten aus welchem Grund verarbeitet. Auf diese Weise hatten die Behörden (aktuell die Datenschutzbehörde) Kontrollmöglichkeiten und betroffene Personen effektive Möglichkeit, ihnen zustehende Rechte, sich gegen eine ungerechtfertigte Verwendung ihrer Daten zu schützen, auszuüben. Zu diesen Rechten gehörten beispielsweise das Recht auf Geheimhaltung der Daten, das Recht auf Unterlassung der unzulässigen Verwendung und das Recht auf Auskunft, Richtigstellung und Löschung der Daten. Der Erfolg dieses Systems war jedoch überschaubar, wenn man berücksichtigt, dass in der Praxis zahlreiche Unternehmen keine Registrierung im DVR vornahmen. Eine der wesentlichen Neuerungen der DSGVO liegt deshalb darin, dass das DVR abgeschafft wird. Umgekehrt hat jedoch der Datenverarbeiter selbst ein Verzeichnis der Verarbeitungstätigkeiten zu führen, dessen Struktur jener der Eintragungen im DVR ähnelt.

3. Begriffsbestimmungen

Die DSGVO verwendet einige Begriffe, die einer näheren Darlegung bedürfen:

Als „**personenbezogene Daten**“ versteht man alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Ausreichend ist es, wenn die Informationen einer Person lediglich irgendwie zugeordnet und damit ein Personenbezug hergestellt werden kann. Betroffene Personen sind allerdings immer nur natürliche Personen; Im Vergleich zur bisherigen Rechtslage stellt die Tatsache, dass juristische Personen nicht vom Schutzbereich der DSGVO umfasst sind, ein wesentliches Novum dar.

Unter den Begriff der personenbezogenen Daten fallen etwa der Name, das Geburtsdatum, die Adresse, aber auch Fotos, Telefonnummer, Autokennzeichen oder die IP-Adresse einer Person. Eine abschließende Aufzählung der personenbezogenen Daten ist nicht möglich.

Unter „**Verarbeitung**“ von Daten fällt nahezu jeder denkbare und auf personenbezogene Daten bezogene Vorgang. Beispielhaft lassen sich hier 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, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten nennen.

Ein weiterer wichtiger Begriff ist jener des Verantwortlichen. Ein „**Verantwortlicher“** ist eine natürliche oder juristische Person, die – allein oder gemeinsam mit anderen – über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Eng damit verknüpft ist der sogenannte „**Auftragsverarbeiter**“. Darunter ist eine natürliche oder juristische Person zu verstehen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, beispielsweise ein IT-Dienstleister.

„**Betroffene Person**“ ist eine identifizierte oder identifizierbare natürliche Person. Gemeint ist damit jeweils die natürliche Person, deren Daten verarbeitet werden.

4. Anwendungsbereich der DSGVO

4.1 Persönlicher Anwendungsbereich

Nur wenige Personen sind vom Anwendungsbereich der DSGVO ausgeschlossen. Nicht erfasst werden insbesondere Datenverarbeitungen durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten sowie Datenverarbeitungen durch gewisse Sicherheitsbehörden.

4.2 Sachlicher Anwendungsbereich

Die Datenschutzgrundverordnung findet Anwendung auf die ganz oder teilweise automatisierte Verarbeitung oder Übermittlung von personenbezogenen Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert werden (zB in einem manuellen Karteisystem).

Aufgrund der Technologieneutralität der DSGVO ist nicht nur die automatisierte, sondern auch die manuelle Verarbeitung personenbezogener Daten von der Schutzwirkung der Verordnung umfasst – eine wesentliche Änderung zur aktuellen Rechtslage.

4.3 Räumlicher Anwendungsbereich

Die DSGVO gilt für alle Datenverarbeitungen personenbezogener Daten von EU-Bürgern. Sie gilt insofern für die Verarbeitungen im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters innerhalb der EU, unabhängig davon, ob die Verarbeitung der Daten selbst in der Europäischen Union stattfindet.

Der räumliche Anwendungsbereich erstreckt sich in manchen Fällen sogar noch weiter. So sind auch Verarbeiter bzw Unternehmen (die ihren Sitz nicht in der EU haben) von der Verordnung umfasst, wenn sie Waren oder Dienstleistungen gezielt an betroffene Personen in der EU anbieten oder Personen in der EU beobachten. Bei der Beurteilung, ob Waren oder Dienstleistungen in einem Mitgliedstaat angeboten werden, wird gesamthaft zu beurteilen sein. Der bloße, auch in der EU abrufbare, Internetauftritt reicht dafür nicht. In den Erwägungsgründen wird zudem klargestellt, dass jede derzeit bekannte Form des Trackings bzw Profilings unter das „Beobachten" fallen.

Der räumliche Anwendungsbereich kann vertraglich nicht geändert werden; eine Rechtswahlklausel ist sohin nicht möglich.

5. Ziele und Grundsätze der DSGVO

5.1 Zielsetzung der DSGVO

Die Ziele der DSGVO sind der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen sowie insbesondere deren Recht auf Schutz personenbezogener Daten und auf freien Verkehr personenbezogener Daten. Um diese Ziele zu erreichen, statuiert die DSVGO einige grundlegende Prinzipien, denen die Datenverarbeitung fortan zu gehorchen hat.

5.2 Grundsatz der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Jeder, dem personenbezogene Daten anvertraut werden, hat diese in (i) rechtmäßiger, (ii) den schutzwürdigen Interessen der Betroffenen entsprechender, (iii) transparenter Weise und (iv) nach Treu und Glauben zu verarbeiten.

Was genau unter diesen hehren Grundsätzen zu verstehen ist, wird die Rechtsprechung näher zu determinieren haben. Beispielhaft sei angeführt, dass personenbezogene Daten nur dann verarbeitet werden dürfen, wenn eine Rechtsgrundlage hierfür besteht, etwa weil die Verwendung der konkreten personenbezogenen Daten erforderlich ist, um seine eigenen vertraglichen Pflichten gegenüber dem Dateninhaber zu erfüllen. Die anlasslose „Vorratsdatenspeicherung" wird daher wesentlich eingeschränkt.

5.3 Grundsatz der Zweckbindung

Die vom Betroffenen zur Verfügung gestellten personenbezogenen Daten dürfen nur im Rahmen der den Betroffenen bekannten Zweckbestimmung für festgelegte, eindeutige und rechtmäßige Zwecke genutzt werden.

5.4 Grundsatz der Datenminimierung

Die Nutzung der personenbezogenen Daten hat dem Verarbeitungszweck zu entsprechen, muss maßgeblich und darf nicht übermäßig sein. Ganz grundsätzlich gesprochen soll sich die Datenverarbeitung an den Zielen der Datenvermeidung bzw Datensparsamkeit orientieren.

5.5 Grundsatz der Datenrichtigkeit

Der Datenverantwortliche hat sicherzustellen, dass die ihm vorliegenden personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem aktuellen Stand sind. In diesem Rahmen sollen alle nötigen Schritte gesetzt werden, dass jene Daten, die im Hinblick auf die Verarbeitung unrichtig sind, umgehend berichtigt oder gelöscht werden.

5.6 Grundsatz der Speicherbegrenzung

Personenbezogene Daten dürfen nur für den Zeitraum, den der Zweck der Verarbeitung erfordert, gespeichert werden. Ein Beispiel hierfür wäre etwa das Aufbewahren von Buchhaltungsdaten zur Erfüllung der steuer- und unternehmensrechtlichen Aufbewahrungspflichten.

5.7 Grundsatz der Integrität und Vertraulichkeit

Die Verarbeitung personenbezogener Daten hat stets auf eine Weise zu erfolgen, die eine angemessene Sicherheit der Daten gewährleistet. Dies umfasst auch den Schutz vor unbefugter bzw unrechtmäßiger Verarbeitung oder vor unbeabsichtigtem Verlust bzw unbeabsichtigter Zerstörung durch technische Maßnahmen.

5.8 Grundsatz der Rechenschaftspflicht

Jeder Verantwortliche ist verpflichtet, die Einhaltung der obigen Grundsätze nachweisen zu können. Zu diesem Zweck bestehen Dokumentationspflichten, bspw ist jede Ausübung eines Betroffenenrechts zu dokumentieren.

6. Rechtmäßigkeit der Datenverarbeitung

Sowohl nach der derzeitigen als auch nach der künftigen Rechtslage dürfen personenbezogene Daten von „Betroffenen“ nur dann verarbeitet werden, wenn deren Verarbeitung rechtmäßig ist. Dies ist dann der Fall,

- wenn die Verarbeitung von Daten **zur Erfüllung eines Vertrags** unmittelbar notwendig ist, etwa bei der Abwicklung eines Online-Kaufs; oder

- wenn **berechtigte Interessen des Verantwortlichen** an der Datenverarbeitung vorliegen und diese Interessen des Verantwortlichen gegenüber jenen der Betroffenen auf Datenschutz überwiegen. Denkbar ist aber auch die Einwilligung des Betroffenen bzw. die Erfüllung einer rechtlichen Verpflichtung des Datenverarbeiters oder einer Aufgabe im öffentlichen Interesse. Daten dürfen dabei jeweils nur im unbedingt erforderlichen Maß erhoben werden; oder

- wenn eine **gültige Einwilligung der betroffenen Person** vorliegt. Eine Einwilligung ist dann gültig, wenn sie freiwillig, dh frei von jedem Zwang, und durch eine eindeutig bestätigende Handlung erteilt werden.

  Das Einwilligungsersuchen des Verantwortlichen, der eine erteilte Einwilligung nachweisen können muss, muss leicht verständlich, leicht zugänglich und in klarer Sprache erfolgen. Zudem muss sich das Ansuchen um die Einwilligung klar von andern Sachverhalten, etwa durch Hervorheben, unterscheiden. Betroffene Personen müssen gleichzeitig über die jederzeitige Widerrufbarkeit der Einwilligung informiert werden, ebenso darüber, welche Daten auf welche Art zu welchem Zweck verarbeitet werden. Wichtig ist, dass die Datenverarbeitung nur im Rahmen der Einwilligung zulässig ist.

7. Rechte der betroffenen Personen

7.1 Allgemeines

Die DSGVO stärkt die Rechte der betroffenen Personen, deren personenbezogenen Daten verarbeitet werden. Dabei bieten insbesondere die neuen Transparenz- und Informationspflichten einen deutlich stärkeren Schutz als die derzeit geltenden Bestimmungen.

7.2 Informationsrecht

Betroffene Personen sind, sofern die Daten direkt bei der betroffenen Person selbst erhoben werden, noch bei Erhebung personenbezogener Daten über deren Verarbeitung zu informieren. In diesem Fall sind der betroffenen Person Name und Kontaktdaten des Verantwortlichen bzw des Datenschutzbeauftragten, der Zweck und die Rechtsgrundlage der Verarbeitung sowie gegebenenfalls die berechtigten Interessen, die vom Verantwortlichen verfolgt werden, und die Empfänger der Daten bekannt zu geben. Zudem ist der Verantwortliche verpflichtet, betroffene Personen zum Zeitpunkt der Datenerhebung über die Dauer deren Speicherung sowie das Recht der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch und Datenübertragbarkeit bzw über das Bestehen eines Rechts auf Widerspruch der Einwilligung zu informieren. Zuletzt muss die betroffene Person darüber in Kenntnis gesetzt werden, ob die Verarbeitung der Daten vertraglich oder gesetzlich erforderlich ist.

Werden die Daten nicht beim Betroffenen selbst erhoben (etwa bei einer Abfrage der Kreditwürdigkeit bei einer Auskunftei) muss zusätzlich zu den oben bereits genannten Informationen angegeben werden, aus welcher Quelle die Daten stammen und gegebenenfalls, ob sie aus öffentlich zugänglichen Quellen stammen. Im Gegenzug können jedoch Informationen darüber, ob die Bereitstellung der Daten gesetzlich oder vertraglich erforderlich ist und die Folgen der Nichtbereitstellung weggelassen werden.

7.3 Auskunftsrecht

Auf Anfrage durch die betroffene Person hat diese Anspruch auf Auskunft zu den folgenden Informationen: Zweck der Datenverarbeitung, Kategorien der Daten, die Dauer der Speicherung, Herkunft der Daten (sofern diese nicht beim Betroffenen selbst erhoben wurden) und Empfänger der Daten. Macht eine betroffene Person Gebrauch von ihrem Auskunftsrecht, so hat der Verantwortliche dem durch Kopie aller personenbezogenen Daten – gegebenenfalls auch auf elektronischem Weg – zu entsprechen.

7.4 Recht auf Berichtigung, Löschung und zur Einschränkung der Verarbeitung

Schon bisher konnten betroffene Personen bei Unternehmen eine Datenauskunft beantragen und die Löschung bzw Berichtigung ihrer Daten verlangen. Durch die DSGVO kommt das Recht, die Verarbeitung dieser Daten einzuschränken, hinzu. Konkret stehen betroffenen Personen nunmehr folgende Rechte zu:

- Unverändert steht der betroffenen Person das **Recht zu, Auskunft darüber zu erhalten**, welche sie betreffenden personenbezogenen Daten verarbeitet werden.

- Möchte eine betroffene Person Gebrauch von ihrem **Recht auf Einschränkung** machen, so ist dies nur in vier Fällen möglich. Nämlich dann, wenn die betroffene Person die personenbezogenen Daten bereits bestritten hat, solange der Verantwortliche die Richtigkeit der Daten überprüft; oder, wenn die betroffene Person Widerspruch gegen die Verarbeitung der Daten erhebt, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen des Betroffenen überwiegen; oder wenn die Verarbeitung unrechtmäßig ist; oder wenn sich der Zweck der Verarbeitung erledigt hat, die Daten aber zur Geltendmachung von Rechtsansprüchen des Betroffenen notwendig sind. In Folge eines zu Recht geltend gemachten Einschränkungsantrags darf der Verantwortliche die Daten nur noch speichern, aber keine sonstigen Verarbeitungsschritte setzen.

- Das **Recht auf Berichtigung**: Dieses setzt voraus, dass die Daten unrichtig oder unvollständig sind. In diesem Fall hat der Verantwortliche die Daten der betroffen Person richtig zu stellen.

- Voraussetzung für das **Löschungsrecht** ist das Vorliegen einer der folgenden Gründe: die personenbezogenen Daten sind für die Zwecke, zu denen sie erhoben wurden, nicht mehr nötig; die betroffene Person hat ihre Einwilligung zur Datenverarbeitung widerrufen; die personenbezogenen Daten wurden unrechtmäßig verarbeitet. Stellt eine betroffene Person einen solchen Löschungsantrag, so hat der Verantwortliche die Daten umgehend zu löschen.

Der Antrag kann formlos, allenfalls sogar mündlich, gestellt werden, muss jedoch begründet werden. Offenkundig unbegründete Anträge kann der Verantwortliche ablehnen oder ein angemessenes Entgelt für Anspruchsdurchsetzung verlangen. Die Beweislast für die Unbegründetheit trifft im Zweifel den Verantwortlichen. Bestehen Zweifel an der Identität einer betroffenen Person, so ist diese verpflichtet ihre Identität nachzuweisen, indem etwa ein Personenausweis vorgelegt wird.

Der Verantwortliche hat den Antrag unverzüglich zu erledigen und zu beantworten, in jedem Fall aber binnen eines Monats ab dessen Eingang. Ist die Erledigung komplex oder liegen besonders viele Anträge vor, kann diese Frist um zwei weitere Monate verlängert werden; dies muss vom Unternehmer jedoch gut begründet werden.

7.5 Recht auf Datenübertragbarkeit

Durch die DSGVO eingeführt wird das Recht auf Datenübertragbarkeit. Betroffene Personen sollen befugt sein, ihre zur Verfügung gestellten personenbezogenen Daten von einer automatisierten Anwendung, auf eine andere Anwendung zu übertragen, ohne dass es technische Barrieren gibt oder dafür eine Gebühr verlangt wird. Betroffene sollen dadurch leichter von einem Anbieter zu einem anderen wechseln können, ohne den Verlust ihrer Daten befürchten zu müssen.

8. Datensicherheit

Jeder Verantwortliche hat dafür Sorge zu tragen, dass umfassende technische und organisatorische Sicherheitsvorkehrungen getroffen werden, um die **Sicherheit, Integrität und Vertraulichkeit** der personenbezogenen Daten zu wahren.

Dabei sind der verfügbare Stand der Technik, die Kosten der Implementierung der Schutzmaßnahmen, Art, Umfang und Zwecke der Datenverarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schweren der Risiken für die Rechte der betroffenen Personen zu berücksichtigen. Die Verordnung sieht im Falle von Verletzungen des Schutzes der Daten strenge Meldepflichten gegenüber der Datenschutzbehörde bzw gegenüber der betroffenen Person selbst vor.

Was sind nun **technische und organisatorische Sicherheitsvorkehrungen**, die dem momentan aktuellen **Stand der Technik** entsprechen? Die DSGVO schweigt zu diesem Thema. Vom deutschen Gesetzgeber werden folgende Maßnahmen angedacht:

- Zugangskontrollsysteme (wer hat Zugang zu meinem Serverraum?)
- Datenträgerkontrollsysteme (wer hat Zugriff auf Festplatten, USB-Sticks udgl?)
- Speicherkontrollsysteme und Übertragungskontrollsysteme (wer kann die von mir verarbeiteten Daten – etwa auf einem eigenen USB-Stick – speichern und wie werden solche Vorgänge abgebildet?)
- Benutzerkontrollsysteme (welche Benutzer meines Netzwerks haben auf welche Daten Zugriff?)
- Transportkontrollmaßnahmen (wie werden personenbezogene Daten auf Datenträgern transportiert?)
- Technische Maßnahmen zur Wiederherstellung von Daten (was passiert im Fall eines Datenverlusts, etwa infolge Hackings?)
- Technische Maßnahmen zur Sicherstellung der Datenintegrität und laufenden Verfügbarkeit von Tagen (welche Maßnahmen werden ergriffen, damit der Zugriff auf personenbezogene Daten möglichst ohne Unterbrechung und fehlerfrei sichergestellt wird?)
- Verfahren zur Pseudonymisierung und Verschlüsselung von Daten

Erfolgt trotz aller Sicherungsmaßnahmen eine Datenschutzverletzung, ist diese unverzüglich und möglichst innerhalb von 72 Stunden bei der **Datenschutzbehörde zu melden**, wenn dadurch ein Risiko für die Rechte der Betroffenen besteht. Eine vergleichbare Mitteilungspflicht der Unternehmen besteht im Verhältnis zu den Betroffenen.

9. Verzeichnis der Verarbeitungstätigkeiten

Zum Nachweis dafür, dass die Bestimmungen der DSGVO eingehalten wurden, hat jeder Verantwortliche bzw Auftragsverarbeiter ein **schriftliches oder elektronisches Verzeichnis aller Verarbeitungstätigkeiten** zu führen und dieses der Datenschutzbehörde auf Verlangen zur Verfügung zu stellen. Das Verzeichnis ermöglicht es, bei Bedarf einen Überblick über sämtliche in einer Einrichtung erfolgenden Tätigkeiten der Verarbeitung personenbezogener Daten zu verschaffen.

Eine Ausnahme von der Verpflichtung besteht, wenn ein Unternehmen weniger als 250 Mitarbeiter beschäftigt und

- die Datenverarbeitung keine Risiken für die Rechte und Freiheiten der betroffenen Personen birgt; und
- die Verarbeitung der Daten nur gelegentlich erfolgt; und
- die Verarbeitung weder sensible noch strafrechtlich relevante Daten betrifft.

Aufgrund dieser eng gefassten Ausnahmebestimmung wird die Pflicht zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten für die meisten Unternehmer den Regelfall darstellen.

Art.30 DSGVO schreibt einen bestimmten **Mindestinhalt** der zu erfassenden Informationen vor. Demnach sind neben dem Namen und den Kontaktdaten des Verantwortlichen auch die Verarbeitungszwecke, die Beschreibung der Betroffenenkategorien, die Beschreibung der Datenkategorien und die Empfängerkategorien in das Verzeichnis aufzunehmen. Wichtig und neu ist, dass auch ein Löschungskonzept integriert wird. Unternehmen müssen sich künftig somit gezielt mit den unterschiedlichen Aufbewahrungsfristen auseinandersetzen. Zuletzt müssen auch die technischen und organisatorischen Sicherheitsmaßnahmen dargelegt werden.

10. Datenschutz-Folgeabschätzung

Mit der DSGVO ist eine Verstärkung der Eigenverantwortlichkeit der Verantwortlichen verbunden. Ihrem Ziel dient das fallweise eingreifende Erfordernis der Erstellung einer Datenschutz-Folgeabschätzung.

Die Datenschutz-Folgeabschätzung ist eine **Risikoanalyse**, die bestimmte Datenverarbeitungen vorauszugehen hat. Es handelt sich dabei also um eine Abschätzung der Risiken und Folgen einer geplanten Datenverarbeitung, wenn die Art der Datenverarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der Betroffenen mit sich bringt.

Die DSGVO enthält lediglich eine *beispielhafte Auflistung von Fällen*, in denen ein hohes Risiko zu erwarten und sohin eine Datenschutz-Folgeabschätzung vorzunehmen ist. Ein solches Risiko besteht insbesondere im Fall

- einer systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlicher Weise erheblich beeinträchtigen;

- einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10;

- einer systematischen weiträumigen Überwachung öffentlich zugänglicher Bereiche.

Als **Mindestinhalt** einer solchen Datenschutz-Folgeabschätzung sind die geplanten Verarbeitungszwecke systematisch zu beschreiben. Dabei ist jedenfalls auch der Verarbeitungszweck zu berücksichtigen. Zudem ist eine Bewertung der Notwendigkeit und Verhältnismäßigkeit bezogen auf den Zweck der Datenverarbeitung aufzunehmen. Auf dieser Basis hat die Bewertung der Risiken und Folgen für die Rechte und Freiheiten der betroffenen Personen zu erfolgen. Nach Identifizierung der Risiken sind die geplanten Maßnahmen zur Bewältigung dieser Risiken und Verfahren zum Schutz der Daten festzulegen.

Ergeben sich aufgrund der Datenschutz-Folgeabschätzung Zweifel, dass die Datenverarbeitung zu risikobehaftet ist und der Verantwortliche nicht selbst ausreichende Abhilfemaßnahmen definieren kann, so ist die **Datenschutzaufsichtsbehörde vorab zu konsultieren**. Zweck ist die Eindämmung des Risikos. Die Behörde hat anschließend acht Wochen Zeit, um eine Empfehlung und adäquate Abhilfemaßnahmen vorzuschlagen. Kommt die Behörde zu der Ansicht, dass die geplante Datenverarbeitung nicht mit der DSGVO in Einklang zu bringen ist, kann diese untersagt werden.

11. Bestellung eines Datenschutzbeauftragten

Die Bestellung eines Datenschutzbeauftragten ist **verpflichtend**

- für Behörden bzw. öffentliche Stellen mit Ausnahme von Gerichten oder
- wenn die Kerntätigkeit eine Verarbeitungstätigkeit darstellt, die eine umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht.
- Auch bei der umfangreichen Verarbeitung sensibler oder strafrechtlich relevanter Daten ist die Bestellung eines Datenschutzbeauftragten verpflichtend.

Darüberhinausgehend kann ein Datenschutzbeauftragter selbstverständlich auf freiwilliger Basis bestellt werden. Der Datenschutzbeauftragte kann in jedem Fall ein eigener Mitarbeiter sein, aber auch extern – beispielsweise ein Anwalt oder dafür zertifizierter Anbieter – bestellt werden.

Dem Datenschutzbeauftragten obliegen dabei zumindest die folgenden **Aufgaben**: die Unterrichtung und Beratung der Verantwortlichen, der Auftragsverarbeiter und der Beschäftigten; die Überwachung der Einhaltung der DSGVO und nationaler Sonderregelungen; Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung; Zusammenarbeit mit der Aufsichtsbehörde.

Anders als bisher hat der Datenschutzbeauftragte damit nicht mehr nur eine **beratende und unterstützende Funktion** inne, vielmehr wird er zukünftig auch für die Umsetzung der von ihm vorgeschlagenen Maßnahmen verantwortlich sein.

Damit der Datenschutzbeauftragte seinen Aufgaben und Verpflichtungen nachkommen kann, ist es erforderlich, ihn schon frühzeitig in das Management personenbezogener Daten einzubinden. Zudem ist er umfassend zu unterstützen, sei es durch die **Zurverfügungstellung von Ressourcen**, dem Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen aber auch durch die Gewährung von Fortbildungsmöglichkeiten.

12. Verwaltungsstrafen und Schadenersatz

Wie auch bisher schon kann die Datenschutzbehörde im Fall von Rechtsverstößen der Datenverarbeiter Verwaltungsstrafen verhängen; Letztere werden jedoch drastisch erhöht. So sind nunmehr **Strafen von bis zu EUR 20.000.000,00 oder bis zu 4 % des erzielten Jahresumsatzes** im letzten Geschäftsjahr – je nachdem, welcher Betrag höher ist – möglich.

Zusätzlich zu den Erhöhungen der Verwaltungsstrafen wurden die Rechte der Betroffenen auf **Schadenersatz** erweitert. Jede natürliche Person, der wegen eines Verstoßes gegen die DSGVO ein materieller bzw immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Auftraggeber oder gegen den Dienstleister.

Wien, im März 2018