SCHAUB & BRUNS
Steuerberater

Ulrich Schaub
Steuerberater, vBP

Markus Bruns
Steuerberater, Dipl.-Kfm.

Am Sportplatz 8
37412 Herzberg am Harz

Tel.: 05521/9945-0
Fax: 05521/9945-55

Datenschutzgrundverordnung – was ist zu tun?

Inhalt

Die Datenschutzgrundverordnung (DSGVO) wurde am 25.05.2016 verabschiedet. Nach einer Übergangsfrist von zwei Jahren trat sie am 25.05.2018 in Kraft. Als Verordnung ist sie in den Mitgliedstaaten unmittelbar anwendbar (vgl. Art. 288 Abs. 2 AEUV); es bedarf insoweit keines Umsetzungsakts wie bei Richtlinien. Zur Ausfüllung von Öffnungsklauseln und zur Anpassung des nationalen Datenschutzrechts an die Vorgaben der DSGVO wurde das deutsche Bundesdatenschutzgesetz (BDSG) – inzwischen bereits zweimal – geändert; die neue Fassung trat ebenfalls am 25.05.2018 in Kraft, die Änderungen durch das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz sind am **26.11.2019** in Kraft getreten.

Die DSGVO bringt einige Änderungen mit sich; insbesondere wurden die Sanktionen drastisch verschärft. Unternehmen sollten die Vorgaben der DSGVO daher ernst nehmen; Grund zur Panik besteht allerdings nicht.

I. Rechtsgrundlagen und Anwendungsbereich

1. Rechtsgrundlagen

Die DSGVO ist als EU-Recht vorrangig vor nationalem Recht anzuwenden. Sie betrifft die automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisiere Verarbeitung personenbezogener Daten, die in einem Datensystem gespeichert sind oder werden sollen. Dabei sind personenbezogene Daten nach Art. 4 Nr. 1 Hs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Hinweis: Jedes Unternehmen, das seine Lohnbuchhaltung, Personaldaten, Kundendaten etc. mittels EDV verarbeitet, muss sich mit den DSGVO-Regelungen befassen, d.h. grundsätzlich jeder, der beruflich oder wirtschaftlich tätig

ist. Allein die persönliche und familiäre Datennutzung im Haushalt ist ausgenommen. .

2. Anwendungsbereich

Die Bestimmung des Geltungsbereichs der DSGVO richtet sich nach dem **Niederlassungsprinzip** (vgl. Art. 3 Abs. 1 DSGVO). Dieses wird durch das **Marktortprinzip** erweitert (vgl. Art. 3 Abs. 2 DSGVO). Danach gilt die DSGVO für alle datenverarbeitenden Unternehmen mit dem Sitz in der EU und für Anbieter mit Sitz außerhalb der EU, soweit sie ihre Angebote – gleich ob entgeltlich oder unentgeltlich – an Bürger in der EU richten oder das Verhalten von EU-Bürgern beobachten, sofern sich diese in der EU aufhalten.

3. Grundprinzipien

Es gilt das sog. **Verbot mit Erlaubnisvorbehalt** (vgl. Art. 6 DSGVO). Danach ist jede Verarbeitung personenbezogener Daten verboten, es sei denn, es gibt eine Erlaubnis. Wesentliche Erlaubnistatbestände stellen die Einwilligung des Betroffenen, die Verarbeitung zur Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen, die Verarbeitung aufgrund rechtlicher Verpflichtung sowie die Verarbeitung zur Wahrung berechtigter Interessen (vgl. Art. 6 DSGVO) dar. Personenbezogene Daten von Beschäftigten dürfen insbesondere für Zwecke des Beschäftigungsverhältnisses verarbeitet werden (Art 88 Abs. 1 DSGVO, § 26 Abs. 1 BDSG-neu)

Hinweis: Die Verarbeitung von personenbezogenen Daten der Arbeitnehmer im Rahmen der Lohnabrechnung ist für die Durchführung des Beschäftigungsverhältnisses erforderlich. Ferner bestehen rechtliche Verpflichtungen nach der Abgabenordnung und der Sozialgesetzbücher. Im Beschäftigungsverhältnis können ferner Kollektivvereinbarungen eine Rechtsgrundlage für die Datenverarbeitung begründen (vgl. Art. 88 DSGVO). Damit eigenen sich insbesondere Betriebsvereinbarungen als Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis (z.B. im Hinblick auf die Nutzung von Daten zur Unternehmenskommunikation etc.).

Eine **Einwilligung** eignet sich im Verhältnis zu den Beschäftigten als belastbare Grundlage für die Datenverarbeitung nur bedingt. Denn sie muss freiwillig erteilt worden sein, erfordert eine Belehrung des Einwilligenden und ist – mit Wirkung für die Zukunft – frei widerruflich. Musste die Einwilligungserklärung der Beschäftigten bisher zwingend schriftlich abgegeben werden, genügt gem. § 26 Abs. 2 Satz 3 BDSG n.F. nunmehr eine **elektronische Erklärung**. § 126a BGB verlangt insoweit, dass der Aussteller der Erklärung dieser seinen Namen hinzufügt und das Dokument mit einer qualifizierten elektronischen Signatur versieht.

Hinweis: Es ist unklar, ob § 126a BGB zur Konkretisierung der Anforderungen an eine elektronische Erklärung der Einwilligung gem. § 26 BDSG n.F. herangezogen werden kann. Die Einheit der Rechtsordnung spricht dafür, auf die allgemeinen Regelungen des BGB abzustellen. Der Zweck der Neuregelung, eine Erleichterung für den Rechtsverkehr zu schaffen, spricht allerdings dagegen, so dass ggf. auch eine einfache Email genügt. Bis zu einer klaren Positionierung der Datenschutzbehörden sollten allerdings die Anforderungen des § 126a BGB beachtet werden.

Die **Zweckbindung** stellt ein weiteres wichtiges Prinzip dar. Hiernach dürfen Daten grundsätzlich nur für den Zweck verwendet werden, für den sie auch erhoben wurden. Sollen personenbezogene Daten für einen anderen Zweck verarbeitet werden, als für denjenigen, für den sie erhoben wurden, bedarf es grds. einer erneuten Erlaubnis (vgl. Art. 6 Abs. 4 DSGVO).

Unverändert von wesentlicher Bedeutung ist der **Transparenzgrundsatz** (Art. 5 Abs. 1 DSGVO). Der Verantwortliche muss die betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten unterrichten. Art. 12 DSGVO verlangt dabei, dass dies in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer einfachen und klaren Sprache erfolgt.

Eine allgemeine **Nachweispflicht** des Verantwortlichen beinhaltet Art. 24 Abs. 1 DSGVO. Hiernach setzt der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.

Art. 5 Abs. 2 DSGVO sieht eine Nachweispflicht für die Einhaltung der aufgeführten Grundsätze vor (sog. **Rechenschaftspflicht**).

II. Datenschutzbeauftragter (DSB)

Eine Regelung zum Datenschutzbeauftragten findet sich in Art. 37 ff. DSGVO.

1. Benennung(spflicht) und Stellung des DSB

Nach Art. 37 Abs. 5 DSGVO ist der DSB aufgrund seiner beruflichen Qualifikation und seines Fachwissens im Datenschutzrecht und der Datenschutzpraxis sowie zur Erfüllung seiner in Art. 39 DSGVO genannten Aufgaben zu benennen. Zwingend zu benennen ist ein Datenschutzbeauftragter bei **nicht-öffentlichen Stellen** (Behörden und öffentliche Stellen haben – mit Ausnahme von Gerichten – stets einen DSB zu benennen) dann, wenn

- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder

- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gem. Art. 9 oder von per-

sonenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 besteht.

Hinweis: Unter Kerntätigkeit ist (vgl. Erwägungsgrund 97) jeweils die Haupttätigkeit und nicht die Verarbeitung personenbezogener Daten als bloße Nebentätigkeit zu verstehen. Daher ist die Verarbeitung von Beschäftigtendaten durch den Arbeitgeber nicht erfasst.

Das **neue und zum 26.11.2019 modifizierte Bundesdatenschutzgesetz** statuiert – eröffnet durch die DSGVO (Art. 37 Abs. 4 DSGVO) – weitergehende Vorgaben: Gem. § 38 Abs. 1 Satz 1 BDSG n.F. ist ein Datenschutzbeauftragter zu benennen, soweit in der Regel mindestens**,** seit dem **20 Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten im Unternehmen beschäftigt sind; bis zum 26.11.2019 lag der Schwellenwert bei zehn Personen. Geringfügig Beschäftigte, Auszubildende, Praktikanten, Teilzeitkräfte und freie Mitarbeiter sind bei der Ermittlung des Schwellenwerts ebenfalls zu berücksichtigen. Sie werden jeweils als eine Person gezählt. Eine „ständige" Beschäftigung liegt vor, wenn die betreffende Person in Ausübung ihrer Tätigkeit immer wieder mit der automatisierten Verarbeitung personenbezogener Daten befasst ist, ohne dass dies den Schwerpunkt der Tätigkeit ausmachen muss.

Ferner statuiert § 38 Abs. 1 Satz 2 BDSG eine Benennungspflicht unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen, wenn der Verantwortliche oder Auftragsverarbeiter Verarbeitungen vornimmt, die einer Datenschutz-Folgeabschätzung nach Art. 35 DSGVO unterliegen oder sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeiten.

Es kann ein **interner oder ein externer** Datenschutzbeauftragter benannt werden (Art. 37 Abs. 6 DSGVO). Auch der interne Datenschutzbeauftragte – der zugleich Beschäftigter des Unternehmens ist – muss im Hinblick auf die Erfüllung seiner Aufgaben als Datenschutzbeauftragter **weisungsfrei** sein und direkt der obersten Managementebene (Geschäftsführung resp. Vorstand) berichten. Ferner genießt der interne Datenschutzbeauftragte Sonderkündigungsschutz, d.h. er kann nur aus wichtigem Grund gekündigt werden (§ 6 Abs. 4 BDSG n.F). Die Anhebung des Schwellenwerts (auf 20 Personen) dürfte einen wichtigen Grund für Unternehmen, die die Schwelle nicht mehr erreichen, zur Abberufung eines bestellten Datenschutzbeauftragten darstellen. Der Gesetzgeber hat keine Übergangsregelung zum Schutz hiervon betroffener interner Datenschutzbeauftragter vorgesehen.

Hinweis: Eine „Unternehmensgruppe" (= Konzern) darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung (= Tochtergesellschaft) aus der Datenschutzbeauftragte leicht erreicht werden kann (vgl. Art. 37 Abs. 2 DSGVO). Zum Erfordernis der leichten Erreichbarkeit dürfte – neben dem Beherrschen der deutschen Sprache sowie die ggf. abweichenden Unternehmenssprache – gehören, dass der gemeinsame Datenschutzbeauftragte die Tochtergesellschaften binnen eines angemessenen Zeitrahmens aufsuchen kann. Innerhalb Europas dürfte dies (ggf. mit dem Flugzeug) gewährleistet sein.

Der Verantwortliche oder der Auftragsverarbeiter haben die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen (z.B. auf der Unternehmenshomepage im Rahmen des Impressums) und diese der zuständigen Aufsichtsbehörde mitzuteilen.

2. Aufgaben des DSB

Die Aufgaben des Datenschutzbeauftragten ergeben sich aus Art. 39 DSGVO. Hiernach obliegen dem Datenschutzbeauftragten folgende Pflichten:

- *Unterrichtung oder Beratung des Verantwortlichen oder des Auftragsverarbeiters und der mit der Datenverarbeitung Beschäftigten bzgl. ihrer datenschutzrechtlichen Pflichten,*

- *umfassende Überwachung der Einhaltung der DSGVO sowie der unternehmensinternen Strategie für den Schutz personenbezogener Daten sowie Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter sowie deren Sensibilisierung für datenschutzrechtliche Fragestellungen,*

- *Beratung im Zusammenhang mit der Datenschutzfolgenabschätzung und Überwachung ihrer Durchführung sowie*

- *Zusammenarbeit mit der Aufsichtsbehörde und Tätigkeit als Anlaufstelle für diese in mit der Verarbeitung zusammenhängenden Fragen.*

3. Haftung des DSB

In zivilrechtlicher Hinsicht kommen haftungsrechtlich insbesondere Schadenersatzansprüche gegen den Datenschutzbeauftragten in Betracht, sofern dieser gegen seine Pflichten verstößt.

Art. 82 DSGVO regelt zwar zunächst nur einen Schadensersatzanspruch des Betroffenen gegenüber der verantwortlichen Stelle im Fall unzulässiger oder unrichtiger Datenverwendungen. Diese Haftung ist gem. Art. 82 Abs. 3 DSGVO ausgeschlossen, wenn der Verantwortliche nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Nach den allgemeinen schuldrechtlichen (vgl. § 280 BGB) oder deliktischen Grundsätzen (vgl. §§ 823 ff. BGB) ist allerdings ggf. ein Rückgriff beim Datenschutzbeauftragten möglich, wenn die verantwortliche Stelle einem Betroffenen zum Schadenersatz verpflichtet ist, sofern der Datenschutzbeauftragten eine Pflichtverletzung begangen hat. Beim internen Datenschutzbeauftragten greifen zu dessen Gunsten die Grundsätze über den innerbetrieblichen Schadensausgleich (vgl. *Niklas*, NZA 2017, 1091 ff.).

Hinweis: Es empfiehlt sich zu prüfen, ob einem internen Datenschutzbeauftragtem Versicherungsschutz eingeräumt

werden kann. Im Hinblick auf die Haftungsrisiken und Rückgriffsmöglichkeiten empfiehlt sich u.U. die Ernennung eines externen Datenschutzbeauftragten auf der Grundlagen eines Geschäftsbesorgungsvertrags.

III. Verfahrensverzeichnis, Schutzmaßnahmen und Folgenabschätzung

1. Verfahrensverzeichnis

Ein zentrales Dokument im Datenschutzrecht ist das sog. Verfahrensverzeichnis (vgl. Art. 30 DSGVO). Dieses hat – nach neuer Rechtslage – der Verantwortliche im Sinne von Art. 4 Abs. 1 Nr. 7 DSGVO zu fertigen und nicht der Datenschutzbeauftragte. Es sind folgende **Pflichtangaben** zu beachten:

- Name und Kontaktdaten des Verantwortlichen, dessen Vertreter sowie ggf. des Datenschutzbeauftragten,

- Zwecke der Verarbeitung,

- Beschreibung der Kategorien Betroffener und personenbezogener Daten,

- Kategorien von Empfängern der Daten,

- ggf. Übermittlungen von Daten an ein Drittland/eine internationale Organisation,

- (nach Möglichkeit) Fristen für die Löschung der Daten,

- (nach Möglichkeit) allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

2. Schutzmaßnahmen

Art. 32 DSGVO bestimmt, dass unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Technische und organisatorische Maßnahmen, „TOMs“). Die Maßnahmen, die zu den TOMs gehören, sind insbesondere Folgende:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten;

- Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

- Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

3. Folgenabschätzung

Neu ist die sog. Datenschutz-Folgenabschätzung gem. Art. 35 Abs. 1 DSGVO. Diese ersetzt die bisherige Vorabkontrolle (vgl. § 4d Abs. 5 BDSG a.F.). Sie unterfällt der Nachweispflicht gem. Art. 24 Abs. 1 DSGVO. Bei der Datenschutz-Folgenabschätzung wird insbesondere die Eintrittswahrscheinlichkeit und Schwere eines möglichen Risikos bewertet. Dafür ist der Rat des Datenschutzbeauftragten einzuholen (Art. 35 Abs. 2 DSGVO). Ferner haben die Aufsichtsbehörden eine Liste mit Verarbeitungsvorgängen, für die eine Folgenabschätzung vorzunehmen ist, zu veröffentlichen.

Art. 35 Abs. 7 DSGVO bestimmt den Inhalt einer Folgenabschätzung. Hierzu gehören u.a.

- eine systematische Bezeichnung der geplanten Vorgänge und Zwecke der Verarbeitung, eine Bewertung von Notwendigkeit und Verhältnismäßigkeit in Bezug auf den Zweck;

- eine Bewertung des Risikos für die Rechte und Freiheiten der Betroffenen;

- die geplanten Abhilfemaßnahmen und Sicherheitsvorkehrungen.

IV. Informationspflichten und Betroffenenrechte

Art. 13 DSGVO beinhaltet einen Katalog an Informationen, über die unterrichtet werden muss (sog. **Datenschutzerklärung**). Die Erklärung muss auch auf der Webseite leicht durch einfachen Link erreichbar sein; sie darf nicht in den AGB „versteckt“ werden. Zu informieren ist über Folgendes:

- Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters;

- ggf. Kontaktdaten des Datenschutzbeauftragten;

- Zweck der Verarbeitung der Daten;

- Rechtsgrundlage der Verarbeitung;

- ggf. die Empfänger/Kategorien von Empfängern der Daten;

- ggf. die Absicht, die Daten an Stellen außerhalb der EU/des EWR zu übermitteln;

- Dauer der Speicherung der Daten oder die Kriterien für die Festlegung dieser Dauer;

- Bestehen eines Rechts auf Auskunft sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder auf Widerspruch sowie des Rechts auf Datenübertragbarkeit;

- Beschwerderecht bei der Aufsichtsbehörde;

- Erklärung, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob der betroffene Nutzer verpflichtet ist, die Daten bereitzustellen und welche Folgen es hat, wenn er dem nicht nachkommt;

- Widerrufsrecht bei Einwilligung als Grundlage der Verarbeitung.

Hinweis: Die Datenschutzerklärungen auf den Webseiten sollten auf ihre Konformität mit der DSGVO hin überprüft werden. Dies auch vor dem Hintergrund, dass damit zu rechnen ist, das auf Abmahnungen „spezialisierte" Anwälte bei Fehlen in der Datenschutzerklärung leichtes Spiel haben.

Die Datenschutzgrundverordnung bringt auch Änderungen bei den **Rechten der Betroffenen**. Das **Auskunftsrecht** gem. Art. 15 Abs. 1 DSGVO beinhaltet einen umfangreichen Katalog an Informationen, welche diejenigen, die Daten verarbeiten, den betroffenen Personen auf formlose Anfrage hin unverzüglich (= spätestens innerhalb eines Monats) mitteilen muss.

Die Betroffenen können künftig gem. Art. 15 Abs. 3 DSGVO eine kostenlose Kopie aller verarbeiteten Daten verlangen (**Zugriffsrecht**). Art. 16 DSGVO gewährt dem Betroffenen das Recht, vom Verantwortlichen zu verlangen, unrichtige oder unvollständige Daten zu berichtigen oder zu vervollständigen (**Berichtigungsrecht)**. Art. 17 Abs. 1 DSGVO regelt die **Löschungspflich**t. Der Betroffene hat künftig in folgenden Fällen das Recht, vom Verantwortlichen zu verlangen, dass seine Daten gelöscht werden:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

- Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gem. Art. 6 Abs. 1 lit. a) oder Art. 9 Abs. 2 lit. a) DSGVO stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

- Die betroffene Person legt gem. Art. 21 Abs. 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gem. Art. 21 Abs. 2 Widerspruch gegen die Verarbeitung ein.

- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gem. Art. 8 Abs. 1 erhoben.

Art. 17 Abs. 2 DSGVO regelt das **Recht auf Vergessenwerden**. Hiernach muss derjenige, der die Daten öffentlich gemacht hat, ggf. auch weitere Datenverarbeiter über das Löschungsverlagen informieren, damit diese auch Links resp. Kopien der Daten löschen.

Art. 19 DSGVO verpflichtet den Verantwortlichen, die Datenempfänger über Berichtigung, Löschung und Sperrung zu informieren (**Benachrichtigung**). Zudem statuiert Art. 20 Abs. 1 DSGVO das Recht auf Datenübertragbarkeit (**Portabilität**). Hiernach hat der Betroffene das Recht, seine Daten „mitzunehmen".

V. Datenpannen: Melde-/Benachrichtigungspflichten

Wenn Kundendaten unrechtmäßig in die Hände von Dritten geraten, unbeabsichtigt vernichtet oder verändert werden oder verloren gehen, treffen den Verantwortlichen die in Art. 33 und 34 DSGVO genannten Pflichten. Hiernach sind insbesondere die zuständige Aufsichtsbehörde und die Betroffenen zu informieren. Die Meldung hat grundsätzlich innerhalb von 72 Stunden zu erfolgen. Ist die Verletzung allerdings voraussichtlich nicht mit einem Risiko für die persönlichen Rechte und Freiheiten der von der Datenschutzverletzung betroffenen Person verbunden, besteht keine Meldepflicht (vgl. Art. 33 Abs. 1, Art. 34 Abs. 1 DSGVO).

VI. Auftragsverarbeitung

Wenn eine Verarbeitung im Auftrag eines Verantwortlichen erfolgt, arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet (vgl. Art. 28 DSGVO).

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags, der den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.

Der Vertrag muss schriftlich oder in einem elektronischen Format vorliegen. Den Auftragsverarbeiter treffen verschiedene neue Pflichten, u.a. die Pflicht zur Einrichtung eines Verfahrensverzeichnisses oder die Pflicht zur Durchführung technischer und organisatorischer Maßnahmen und zur Bestellung eines Datenschutzbeauftragten (vgl. Art. 32, 37 DSGVO).

Hinweis: Der Auftragsverarbeiter ist weisungsgebunden und zur Verschwiegenheit verpflichtet. Subunternehmer darf der Auftragsverarbeiter nur dann einsetzen, wenn der Verantwortliche dem zugestimmt hat (vgl. Art. 28 Abs. 2 DSGVO).

VII. Zivilrechtliche Haftung und Geldbußen

Art. 82 DSGVO bestimmt, dass – durch kausale Verletzung der DSGVO-Vorgaben herbeigeführte – materielle und immaterielle Schäden durch den Verantwortlichen oder den Auftragsverarbeiter zu erstatten sind. Der Umfang der Haftung ergibt sich aus Art. 82 Abs. 3 DSGVO beinhaltet eine **Exkulpationsmöglichkeit**: Hiernach ist der Verantwortliche oder der Auftragsverarbeiter von der Haftung gem.

Abs. 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Hinweis: Eine Vorsorge vor zivilrechtlicher Inanspruchnahme verlangt, dass Datenschutzmaßnahmen umfassend dokumentiert werden und den Nachweispflichten gem. Art. 24 DSGVO Genüge getan wird.

Ferner sieht Art. 83 DSGVO Bußgelder vor. Nach Art. 83 Abs. 1 DSGVO hat jede Aufsichtsbehörde sicherzustellen, dass die Verhängung von Geldbußen nach diesem Artikel für Verstöße gegen diese Verordnung gemäß den Abs. 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist. Für Unternehmen kann das Bußgeld bis zu 20 Mio. € oder bis zu 4% des globalen Umsatzes betragen (vgl. Art. 83 Abs. 5 DSGVO). Zum Vergleich: § 43 Abs. 3 Satz 1 BDSG a.F. sah Bußgelder bis zu 50.000 € resp. bis zu 300.000 € vor.

VIII. Wesentliche Begriffe der DSGVO

Art. 4 DSGVO definiert die zentralen Begriffe der Datenschutzgrundverordnung. Grundlegend sind insbesondere folgende Begriffe:

- „**Personenbezogene Daten**" bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

- „**Verarbeitung**" bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie 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.

- „**Pseudonymisierung**" bezeichnet die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

- „**Verantwortlicher**" bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

- „**Auftragsverarbeiter**" bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

- „**Empfänger**" bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.

- „**Dritter**" bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

- „**Einwilligung**" bezeichnet der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

- „**Unternehmensgruppe**" bezeichnet eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht.

- „**Aufsichtsbehörde**" bezeichnet eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

Fazit

Nach gut 1 ½ Jahren DSGVO bleibt festzuhalten, dass unter der DSGVO bis vor wenigen Monaten signifikante Bußgelder lediglich in anderen EU-Staaten verhängt wurden: Die **britische Datenschutzaufsichtsbehörde** hat im Juli 2019 ein Millionen-Bußgeld gegen British Airlines aufgrund „schwacher Sicherheitsvorkehrungen" verhängt. Das Bußgeld betrug ca. 1,5% des Jahresumsatzes aus dem Jahr 2017. Ein Bußgeld von ca. 3% des Jahresumsatzes verhängte die ICO gegen die Hotelkette Marriott, nachdem diese einen Datenschutzvorfall nach Art. 33 DSGVO gemeldet hatte.

Ferner hat die **französische Datenschutzaufsicht** Google mit einem Bußgeld von 50 Mio. € sanktioniert: Es seien Informationen zur Verwendung der erhobenen Daten und dem Speicher-Zeitraum für die Nutzer nicht einfach genug zugänglich.

Inzwischen haben allerdings auch in **Deutschland** die Datenschutzbehörden ihre Zurückhaltung aufgegeben:

Am 30.10.2019 verhängte die **Berliner Aufsichtsbehörde** ein Bußgeld von 14,5 Mio. € gegen die Immobiliengesellschaft Deutsche Wohnen SE wegen unrechtmäßiger Datenspeicherung. Die Behörde hatte 2017 festgestellt, dass das Unternehmen für die Speicherung personenbezogener Daten von Mietern ein Archivsystem verwendete, welches keine Möglichkeit vorsah, nicht mehr erforderliche Daten nach Zweckerfüllung und Ablauf der Aufbewahrungspflichten zu löschen. Somit konnte eine unzulässige Speicherung personenbezogener Daten von Mietern, wie z.B. Gehaltsbescheinigungen, Selbstauskunftsformulare, Auszüge aus Arbeits- und Ausbildungsverträgen, Steuer-, Sozial- und Krankenversicherungsdaten sowie Kontoauszüge festgestellt werden. Bei einer erneuten Prüfung im März 2019 konnte das Unternehmen, trotz ausgesprochener Empfehlung der Aufsichtsbehörde, weder eine Bereinigung des Datenbestands noch rechtliche Gründe für die fortlaufende Speicherung vorweisen. Die Aufsichtsbehörde qualifizierte die getroffenen Maßnahmen als unzureichend, um einen rechtmäßigen Zustand herzustellen und sah darin einen Verstoß gegen Art. 25 Abs. 1 DSGVO sowie Art. 5 DSGVO für den Zeitraum zwischen Mai 2018 und März 2019.

Der **Bundesbeauftragte für den Datenschutz und die Informationsfreiheit** verhängte ein Bußgeld von über 9,5 Mio. € gegen den Telekommunikationsdienstleister 1&1 Telecom GmbH. Nach Einschätzung des BfDI hatte das Unternehmen keine hinreichenden technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Kundendaten ergriffen. Bei der telefonischen Kundenbetreuung des Unternehmens sei die Angabe des Namens und des Geburtsdatums ausreichend gewesen, um weitere personenbezogene Kundendaten in Erfahrung zu bringen. In diesem Authentifizierungsverfahren sah der Bundesbeauftragte einen Verstoß gegen Art. 32 DSGVO.

Hinzuweisen ist ferner auf die **griechische Aufsichtsbehörde**, die Anfang August 2019 ein Bußgeld in Höhe von 150.000 € gegen PricewaterhouseCoopers Business Solutions SA wegen Auswahl und Anwendung ungeeigneter Rechtsgrundlagen (hier: Einwilligung von Beschäftigten) und der damit einhergehenden Verletzung der Rechenschaftspflicht verhängt hat.

Rechtsstand: 6.12.2019