MERKBLATT

Markus Isemann
Steuerberater

Bahnhofstr. 16 • 45525 Hattingen
Fon 02324 / 26363 • Fax 02324 / 21350
www.klewer-isemann.de

Datenschutzgrundverordnung tritt am 25.05.2018 in Kraft - Was ist zu tun?

Inhalt

I. Rechtsgrundlagen, Anwendungsbereich und Grundprinzipien

II. Datenschutzbeauftragter (DSB)

1. Benennung(spflicht) und Stellung des DSB

2. Aufgaben des Datenschutzbeauftragten

3. Haftung des DSB

4. Exkurs: Beschäftigtendatenschutz

III. Verfahrensverzeichnis, Schutzmaßnahmen und Folgenabschätzung

IV. Informationspflichten und Betroffenenrechte

V. Datenpannen: Melde-/Benachrichtigungspflichten

VI. Auftragsverarbeitung

VII. Zivilrechtliche Haftungsrisiken und Sanktionen

Die Datenschutzgrundverordnung (DSGVO) wurde am 25.05.2016 verabschiedet. Nach einer Übergangsfrist von zwei Jahren tritt sie am 25.05.2018 in Kraft. Als Verordnung ist sie in den Mitgliedstaaten unmittelbar anwendbar; 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 Datenschutzgesetz (BDSG) inzwischen geändert; die neue Fassung tritt ebenfalls am 25.05.2018 in Kraft.

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

I. Rechtsgrundlagen, Anwendungsbereich und Grundprinzipien

Das Datenschutzrecht bestimmt sich ab dem 25.05.2018 EU-weit nach der DSGVO. Es ist damit unionsweit harmonisiert. Die DSGVO lässt durch einige Öffnungsklauseln allerdings nationale (Sonder-)Regelungen zu. Die in der DSGVO definierten Grundprinzipien sind allerdings im Rahmen der Auslegung und Anwendung nationaler datenschutzrechtlicher Bestimmungen stets zwingend zu beachten.

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 etwa 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

Der Geltungsbereich der DSGVO richtet sich nach dem **Niederlassungsprinzip,** welches durch das **Marktortprinzip** erweitert wird. 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**. 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 dar.

Die **Einwilligung** zur Datenverarbeitung muss die in Art. 7 DSGVO genannten Bedingungen erfüllen. D.h. die Einwilligung muss insbesondere:

- in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen,
- klar von anderen Sachverhalten getrennt,
- freiwillig und
- einfach zu widerrufen sein.

Hinweis: Bisher erteilte Einwilligungen gelten zwar nach Auffassung des Düsseldorfer Kreises, als Gremium der unabhängigen Datenschutzbehörden des Bundes und der Länder, grds. fort, sofern sie der Art nach den Bedingungen der DSGVO entsprechen.

Es können sich jedoch insbesondere im Rahmen von Arbeitsverhältnissen im Hinblick auf die Freiwilligkeit Zweifel ergeben. Soweit ausschließlich die Einwilligung Rechtsgrundlage der Verarbeitung ist, sollte in Zweifelsfällen eine Nachbelehrung vor dem 25.05.2018 erfolgen, weil – Erforderlichkeit der Nachbelehrung vorausgesetzt – andernfalls spätestens am 25.05.2018 die Daten gelöscht werden müssten (vgl. Art. 17 Abs. 1 DSGVO).

Sicherheitshalber sollte eine „neue“ Einwilligung nach der DSGVO, insbesondere mit Belehrung über das Widerrufsrecht eingeholt 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. und im Zweifel einer erneuten Erlaubnis; allerdings können bei einer Zweckänderung auch andere Erlaubnistatbestände – z. B. die Erforderlichkeit zur Vertragserfüllung – greifen.

Unverändert von wesentlicher Bedeutung ist der **Transparenzgrundsatz**. 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**).

4. Exkurs Beschäftigtendatenschutz – Erlaubnis zur Datenverarbeitung:

Eine **Einwilligung** (Art. 6 Abs. 1 Satz 1 lit. a) DSGVO, § 26 Abs. 2 BDSG-neu) 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.

Personenbezogene Daten von Beschäftigten dürfen jedoch insbesondere für Zwecke des Beschäftigungsverhältnisses verarbeitet werden (Art. 88 Abs. 1 DSGVO, § 26 Abs. 1 Satz 1 BDSG-neu). Häufig greift bereits dieser Erlaubnistatbestand der Erforderlichkeit der Datenverarbeitung für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses. Daneben kann sich eine Zulässigkeit der Datenverarbeitung auch aufgrund der Erforder-

lichkeit der Verarbeitung zur Erfüllung einer gesetzlichen Verpflichtungen ergeben (

Der Arbeitgeber muss z. B. im Rahmen der Lohnabrechnung, ggf. der Gewährung von Zusatzurlaub gegenüber schwerbehinderten Mitarbeitern (vgl. § 208 SGB IX) sowie den Verpflichtungen im Rahmen des betrieblichen Eingliederungsmanagements („bEM“, vgl. § 167 Abs. 2 SGB IX) personenbezogene Daten verarbeiten. Insoweit bedarf es keiner Einwilligung der betroffenen Personen. Ferner bestehen rechtliche Verpflichtungen nach der Abgabenordnung und der Sozialgesetzbücher.

Im Beschäftigungsverhältnis können darüber hinaus auch Kollektivvereinbarungen eine Rechtsgrundlage für die Datenverarbeitung begründen (. Damit eigenen sich insbesondere Betriebsvereinbarungen als Rechtsgrundlage für die Verarbeitung personenbezogener Daten (z.B. im Hinblick auf die Nutzung von Daten zur Unternehmenskommunikation etc.)

II. Datenschutzbeauftragter (DSB)

Regelungen zum Datenschutzbeauftragten finden 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 personenbezogenen 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 Bundesdatenschutzgesetz** beinhaltet – eröffnet durch die DSGVO (Art. 37 Abs. 4 DSGVO) – weitergehende Vorgaben: Gem. § 38 BDSG-neu ist ein Datenschutzbeauftragter zu benennen, soweit in der Regel mindestens **zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten im Unternehmen beschäftigt sind. 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-neu eine Benennungspflicht unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen, wenn der Verantwortliche oder Auftragsverarbeiter Verarbeitungen vornimmt, die einer **Datenschutz-Folgenabschätzung** 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. 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 (vgl. § 38 Abs. 2 BDSG-neu).

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 der ggf. abweichenden Unternehmenssprache – gehören, dass der gemeinsame Datenschutzbeauftragte die Gruppengesellschaften 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** (vgl. Art. 37 Abs. 7 DSGVO). Die Aufsichtsbehörden stellen z.T. für die Meldung auf ihrer Homepage ein Formular zur Verfügung, in welches die Angaben eingetragen werden können. Stets möglich ist eine Übermittlung der Angaben per Email.

2. Aufgaben des DSB

Die Aufgaben des DSB ergeben sich aus Art. 39 DSGVO. Hiernach obliegen ihm 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.

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 (neuen) 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.*

Das Verzeichnis ist (auch) in deutscher Sprache zu führen, da es den Aufsichtsbehörden auf deren Anforderung hin unverzüglich vorzulegen ist. Es muss stets aktuell sein.

Hinweis: Änderungen des Verzeichnisses sollten nicht durch Überschreiben der bestehenden Version durchgeführt werden. Denn die alten Inhalte sind vor dem Hintergrund der Rechenschaftspflicht verfügbar zu halten. Daher sollten Vorversionen aufbewahrt und das geänderte (aktuelle) Verzeichnis mit dem Änderungsdatum versehen werden.

2. Schutzmaßnahmen („TOMs“)

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, sog. „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. 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.*

Erforderlich ist eine Datenschutz-Folgenabschätzung nach Art. 35 Abs. 1 DSGVO insbesondere in folgenden Fällen:

- *Systematische und umfassende 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 ähnlich erheblicher Weise beeinträchtigen;*
- *umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gem. Art. 9 Abs. 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DSGVO oder*
- *systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.*

IV. Informationspflichten und Betroffenenrechte

Art. 13, 14 DSGVO beinhaltet einen Katalog an Informationen, über die – aktiv – unterrichtet werden muss (sog. **Datenschutzerklärung**). Art. 13 DSGVO betrifft die Informationspflichten bei der Direkterhebung; Art. 14 DSGVO hat die indirekte Datenerhebung bei Dritten zum Gegenstand. Die Information muss auch auf der Webseite leicht durch einfachen Link erreichbar sein; sie darf nicht in den AGB „versteckt“ werden. Zu informieren ist insbesondere 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.*

Von besonderer Bedeutung sind die Informationspflichten im Beschäftigungsverhältnis. Denn insoweit sind alle Beschäftigte – Bewerber, Neueinstellungen, Bestandsmitarbeiter, Leiharbeitnehmer – ab dem 25.05.2018 entsprechend zu informieren. Die Information kann z. B. – damit der Verantwortliche auch den erforderlichen Nachweis erbringen kann (vgl. Art. 24 DSGVO) – per Email an die Beschäftigten versandt, mit der Hauspost verteilt oder zusammen mit der Verdienstbescheinigung übermittelt werden.

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 sog. „**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).

Hinweis: Welche Aufsichtsbehörde zuständig ist, bestimmt sich nach dem jeweiligen Landesrecht. Hat der Verantwortliche oder Auftragsverarbeiter mehrere Niederlassungen in der EU, ist für die Bestimmung der zuständigen Aufsichtsbehörde die Hauptniedererlassung iSd. Art. 4 Nr. 16 DSGVO maßgeblich. Wenn sich mehrere Behörden für zuständig oder für unzuständig halten oder wenn die Zuständigkeit aus anderen Gründen zweifelhaft ist, treffen die Aufsichtsbehörden die Entscheidung gemeinsam nach Maßgabe des § 18 Abs. 2 BDSG-neu.

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 („nur“) Bußgelder bis zu 50.000 € resp. bis zu 300.000 € vor.

Fazit

Das Inkrafttreten der Datenschutzgrundverordnung steht unmittelbar vor der Tür. Unternehmen sollte den neuen Vorgaben Aufmerksamkeit widmen. Völlig Ignoranz gegenüber den Vorgaben der DSGVO wird teuer. Andererseits ist Panik fehl am Platz. **Bis zum 25.05.2018 unbedingt zu erledigen sind die Erstellung des Verfahrensverzeichnisses sowie die Anpassung der Datenschutzerklärung.** Soweit ein Datenschutzbeauftragter zu benennen ist oder freiwillig benannt wird, sind dessen Namen und Kontaktdaten – idealerweise im Impressum auf der Homepage – bekannt zu machen. Zudem ist die (zuständige) Aufsichtsbehörde zu informieren (Art. 37 Abs. 7 DSGVO). Ferner sollte eine schriftliche Verpflichtung von Personen, die mit personenbezogenen Daten in Berührung kommen, auf das Datengeheimnis eingeholt werden.

Auf Anpassungsbedarf hin zu prüfen sind u.a. Verträge mit Auftrags(daten)verarbeitern. Kollektivvereinbarungen (namentlich Betriebsvereinbarungen), die als Rechtsgrundlage für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten dienen (vgl. Art. 88 DSGVO), an die Vorgaben der DSGVO angepasst werden. Gleiches gilt für die Formulare von Einwilligungserklärungen im Sinne von Art. 7 DSGVO.