PROJEKT PÄDAGOGIK UND RECHT

Sicher im Spannungsfeld Pädagogik-Recht durch praxisgerechte Lösungen/ z.B. Prüfschema zulässige Macht/ seit 10 Jahren Ideen weiterentwickelt

EU-DATENSCHUTZGRUNDVERORDNUNG (DSGVO) - AB 25. 5.2018?

HTTPS://WWW.WBS-LAW.DE/IT-RECHT/DATENSCHUTZRECHT/DIE-EU-DATENSCHUTZGRUNDVERORDNUNG/#3

VORBEMERKUNG

Ab 25. Mai 2018 gilt auch in Deutschland die Datenschutzgrundverordnung (DSGVO) der Europäischen Union (EU). Durch das neue EU-Recht werden unmittelbar das bisherige Bundesdatenschutzgesetz (BDSG a.F.) und die EU-Datenschutzrichtlinie (Richtlinie 95/46/EG), auf der das BDSG basiert, abgelöst. **Zeitgleich tritt ein dazu gehöriges BDSG neuer Fassung (BDSG n.F.) in Kraft, das die DSGVO zum Teil modifiziert und konkretisiert.** Die DSGVO wird außerdem ergänzt werden durch die noch in Abstimmung befindliche EU-e-Privacy-Verordnung, die voraussichtlich 2019 in Kraft treten soll und Internet- und Telemediendienste betrifft.

Ziel der DSGVO ist zunächst ein weitestgehend einheitliches Datenschutzrecht innerhalb der EU. Darin sollen vor allem die Rechte und Kontrollmöglichkeiten derjenigen gestärkt werden, deren personenbezogene Daten verarbeitet werden (Betroffene). Personenbezogene Daten sollen dadurch stärker geschützt werden, gleichzeitig soll aber auch ihr freier Verkehr besser gewährleistet werden.

Wesentliche Elemente des bisherigen BDSG werden zwar erhalten bleiben. So gleichen die in Art. 5 DSGVO festgelegten Grundsätze der Datenverarbeitung, an denen sich die Verordnung orientiert, im Kern denen des BDSG a.F.: Rechtmäßigkeit, Zweckbindung, Datenminimierung (Datensparsamkeit), Richtigkeit, Zeitliche Beschränkung (Speicherbegrenzung), Integrität und Vertraulichkeit sowie eine Rechenschaftspflicht der Verantwortlichen für die Einhaltung dieser Grundsätze.

Dennoch wird es zukünftig einige Änderungen geben, die es zu beachten gilt – sowohl für Unternehmen als auch für Privatpersonen. Gerade für Unternehmen ist es wichtig, sich bereits jetzt in der Übergangsphase um die Umsetzung der neuen Regelungen zu kümmern und neue datenschutzrechtliche Prozesse zu etablieren. Sonst drohen im Extremfall immense Bußgelder für die verspätete Einführung der neuen Vorgaben. Hierzu beraten wir gerne.

ALLGEMEINES

Welches sind die wesentlichen Neuerungen?

Konkret in der neuen Verordnung geregelt werden vor allem die **Rechtsgrundlagen der Datenverarbeitung, die Rechte der Betroffenen** und **die Pflichten der Verantwortlichen**.

Die Rechte der Nutzer werden durch neue Transparenz- und Informationspflichten der datenverarbeitenden Unternehmen gestärkt. Betroffene sollen leichter Zugang zu ihren Daten und der Information über deren Nutzung haben. Außerdem wird das bislang nur gerichtlich konstruierte „Recht auf Vergessenwerden“, also der Anspruch auf Löschung personenbezogener Daten, nun in Gesetzesform gegossen.

Neben bereits bekannten Pflichten stellt die DSGVO auch weitergehende Anforderungen an den **Datenschutz in Unternehmen**. Neu ist beispielsweise die Pflicht, elektronische Geräte und Anwendungen datenschutzfreundlich voreinzustellen. Ebenfalls neu eingeführt wird die Pflicht zur Datenschutz-Folgenabschätzung bei besonderen Risiken für die erhobenen Daten, etwa durch neue Technologien.

Außerdem gilt die DSGVO auch für Unternehmen, die ihren Sitz außerhalb der EU haben, wenn sich ihre Angebote sich aber an EU-Bürger wenden. Dies hat weitreichende Konsequenzen etwa für Unternehmen wie Facebook und Google mit Sitz in den USA.

Der Bußgeldrahmen bei Verstößen wird erheblich erhöht und kann bis zu 4 Prozent des weltweiten Jahresumsatzes eines Unternehmens betragen.

Wann dürfen Daten verarbeitet werden?

Die **Datenverarbeitung (DV)** ist auch nach der DSGVO weiterhin nur zulässig, wenn es die Verordnung oder ein anderes Gesetz ausdrücklich erlaubt (Verbot mit Erlaubnisvorbehalt). So ist es derzeit auch im BDSG geregelt – hier wird sich also nichts Wesentliches ändern.

Die praktisch relevantesten **Erlaubnistatbestände** nach Art. 6 DSGVO sind:

- es liegt eine **Einwilligung** des Betroffenen vor. Art. 7 und Art. 8 DSGVO definieren die Anforderungen, die an diese Einwilligung zu stellen sind. So soll etwa das Mindestalter bei 16 Jahren liegen – es sei denn, die einzelnen Staaten senken die Altersgrenze auf maximal 13 Jahren ab, was in Deutschland aber nicht geschehen ist.
- die Verarbeitung ist **für die Erfüllung eines Vertrags** oder **zur Durchführung vorvertraglicher Maßnahmen** erforderlich.
- die Verarbeitung ist **zur Erfüllung einer rechtlichen Verpflichtung** erforderlich.
- die Verarbeitung ist **zur Wahrung der berechtigten Interessen** des Verantwortlichen oder eines Dritten erforderlich, wenn keine schutzwürdigen Interessen des Betroffenen überwiegen. Zwar hat man als Betroffener hiergegen ein Widerspruchsrecht, auf das er auch hingewiesen werden muss – doch es ist unklar, aus welchen Gründen ein solcher Widerspruch Erfolg haben könnte. Daher dürfte dieses Recht ins Leere laufen.

In Abs. 4 ist aber auch eine Regelung enthalten, nach der Daten später auch zu Zwecken verarbeitet werden dürfen, die nicht dem ursprünglichen Zweck der Erhebung entsprechen. Dies ist aber nur dann zulässig, wenn die Verarbeitung mit dem ursprünglichen Erhebungszweck kompatibel ist. Hierzu zählt ausdrücklich die Nutzung zu statistischen Zwecken. Allerdings müssen die Betroffenen darüber informiert werden.

Welche Daten dürfen nicht verarbeitet werden?

Ähnlich der bisherigen Regelung im BDSG sieht nun auch Art. 9 DSGVO **besondere Kategorien von Daten** vor, die grundsätzlich nicht verarbeitet werden dürfen. Dies sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, Gesundheitsdaten und Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person hervorgehen. Die Kategorien sind weiter als die im BDSG, insbesondere fallen auch biometrische Daten (Fingerprint, Stimmerkennung etc.) nun darunter.

Die Verarbeitung dieser Daten ist allerdings dann erlaubt, wenn ein Ausnahmetatbestand einschlägig ist. Im Wesentlichen ist das der Fall, wenn die betroffene Person eingewilligt hat oder die Verarbeitung zur Geltendmachung und Abwehr von Rechten und Ansprüchen erforderlich ist. Dieser Erlaubnistatbestand ist – anders als bisher im BDSG – aufgrund der europäischen Richtlinie nicht mehr auf die gerichtliche Geltendmachung oder Abwehr beschränkt.

Grundsätze der Datenverarbeitung

Art. 5 Abs. 1 DSGVO zählt die **Grundsätze** auf, die für die gesamte Datenverarbeitung gelten:

- **Rechtmäßigkeit** der Verarbeitung (vgl. Art. 6 DSGVO): Daten dürfen nur verarbeitet werden, wenn es eine gesetzliche Erlaubnisnorm gibt oder eine wirksame Einwilligung vorliegt.
- Verarbeitung nach **Treu und Glauben**
- **Transparenz** (vgl. Art. 12 ff. DSGVO): Betroffene sollen Ihr Grundrecht auch wahrnehmen können. Dafür brauchen sie insbesondere Informationen über die gespeicherten Daten.
- **Zweckbindung:** Die Zwecke der Datenverarbeitung müssen grds. bereits bei der Erhebung der Daten festgelegt sein.
- **Datenminimierung**: Daten müssen insbes. auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden.
- **Richtigkeit** der Datenverarbeitung (vgl. Art. 16, 17 DSGVO)
- **Speicherbegrenzung** (vgl. Art. 17 DSGVO, „Recht auf Vergessenwerden")
- **Integrität und Vertraulichkeit** (vgl. Art. 32 DSGVO): Sicherheit der Daten

Rechte der Betroffenen

Die Rechte betroffener Personen (Art. 12 – 23 DSGVO), deren Daten verarbeitet werden, bringen für Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO (im Folgenden: „Der Verantwortliche") neue Pflichten mit sich. Sie müssen daher ein **praktikables Verfahren etablieren**, um DSGVO-konform insbesondere auf folgende wichtige Ansprüche der Betroffenen reagieren zu können:

Auskunftsrecht

Die Betroffenen haben gem. Art. 15 DSGVO ein **umfassendes Auskunftsrecht.** Es ist weitestgehend mit dem bisherigen § 34 BDSG vergleichbar – neu ist jedoch, dass der Betroffene nun auch eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, verlangen kann.

Der Verantwortliche muss auf Verlangen der betroffenen Person eine Bestätigung darüber erteilen, ob er überhaupt personenbezogene Daten verarbeitet. Sofern dies der Fall ist, hat die betroffene Person das Recht auf weitergehende Auskunft im Hinblick auf die in Art. 15 Abs. 1 lit. a) – h) DSGVO genannten Informationen: So hat der Betroffene u.a. ein Auskunftsrecht über die Verarbeitungszwecke, die Kategorien personenbezogener Daten, die verarbeitet werden und über die Herkunft der Daten.

Der Verantwortliche muss die in Art. 15 DSGVO genannten Informationen „unverzüglich" zur Verfügung stellen – dies ist i.d.R. spätestens einen Monat nach der Anfrage, nur in Ausnahmefällen kann die Frist zwei Monate betragen (Art. 12 Abs. 3 DSGVO).

Die meisten Juristen gehen mit der DSGVO davon aus, dass es ein höchstpersönlicher Anspruch ist, den man nur selbst geltend machen kann oder der zumindest eine spezielle auf den Auskunftsanspruch gerichtete Vollmacht des Betroffenen erfordert.

Recht auf Datenübertragbarkeit

Der Betroffene wir durch das neu etablierte **Recht auf Datenübertragbarkeit (Datenportabilität)** gem. Art. 20 DSGVO befugt, ihre Daten „mitzunehmen". Das bedeutet, dass er einen Verantwortlichen anweisen kann, gewisse Daten von einer automatisierten Anwendung (etwa einem sozialen Netzwerk) auf eine andere Anwendung zu übertragen. Dieses Recht soll es Betroffenen erleichtern, von den Anbieter zu wechseln, ohne Daten zu verlieren. Diese müssen dann in einem strukturierten, maschinenlesbaren Format übermittelt werden. Das Recht besteht nur dann, wenn die Verarbeitung auf einer Einwilligung gemäß Art. 6 Abs. 1 lit. a) oder Art. 9 Abs. 2 lit. a) oder auf einem Vertrag gemäß Art. 6 Abs. 1 lit. b) beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Recht auf Löschung („Recht auf Vergessenwerden“)

Art. 17 DSGVO gibt Betroffenen qua Gesetz ein „Recht auf Vergessenwerden“. Der Gedanke, dass personenbezogene Daten gelöscht werden müssen, ist allerdings nicht neu. Das **Recht auf Löschung der eigenen Daten** besteht, wenn:

- 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 gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
- Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 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 gemäß Artikel 8 Absatz 1 erhoben.

Das Recht auf Vergessenwerden findet nach Abs. 3 allerdings **keine Anwendung**, wenn z.B.:

- die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information erforderlich ist
- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist
- die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89
  Absatz 1 erforderlich ist, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Bislang hatte es zu diesem Punkt lediglich Gerichtsentscheidungen gegeben und die Umsetzung der Löschpflicht war in großen Teilen unklar. Die neue Norm sieht hierzu eine detaillierte Prozedur vor.

Daneben ist in Art. 16 DSGVO ein „**Recht auf Berichtigung**“ geregelt. Danach können Betroffene verlangen, dass unrichtige personenbezogene Daten berichtigt und – unter Berücksichtigung der Zwecke der Verarbeitung- unvollständige personenbezogene Daten vervollständigt werden.

Schließlich regelt Art. 18 DSGVO das Recht auf Einschränkung der Verarbeitung. Danach hat die betroffene Person das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung unter gewissen Voraussetzungen (Art. 18 Abs. 1 lit. a – d DSGVO) zu verlangen.

Informationspflichten

Art. 13 und 14 DSGVO sehen für Verantwortliche umfangreiche Informationspflichten vor, die Betroffenen mitgeteilt werden müssen. Dabei ist auf eine präzise, transparente, verständliche und leicht zugängliche Form sowie eine klare und einfache Sprache zu achten (Art. 12 Abs. 1 DSGVO). Die Informationspflichten bestehen sowohl online (z.B. in der Datenschutzerklärung) als auch offline, etwa für Besucher vor Ort. Diese erweiterten Pflichten sollen den Datenschutz im Vergleich zu den aktuell geltenden Regelungen des BDSG stärken.

Dabei unterteilt die DSGVO nach Informationspflichten, wenn personenbezogene Daten direkt beim Betroffenen erhoben werden **(Art. 13 DSGVO)** und Situationen, in denen Daten von Dritten (also nicht bei der betroffenen Person selbst) bezogen werden **(Art. 14 DSGVO):**

Werden Daten **direkt beim Betroffenen erhoben**, müssen folgende Informationen **nach Art. 13 Abs. 1 DSGVO mitgeteilt werden**:

- Name und Kontaktdaten des Verantwortlichen,
- ggf. Kontaktdaten des Datenschutzbeauftragten (DSB),
- Zwecke der Datenverarbeitung
- Rechtsgrundlage der Datenverarbeitung
- Darstellung der berechtigten Interessen (wenn die Datenverarbeitung auf dem Tatbestand der Interessenabwägung gem. Art. 6 Abs. 1 f) DSGVO beruht),
- ggf. Empfänger oder Kategorien von Empfängern der Daten,
- ggf. Informationen zur Datenübermittlung in Drittländer,

Nach **Art. 13 Abs. 2** müssen folgende weitere Informationen **zur Verfügung gestellt werden**, um eine faire und transparente Datenverarbeitung zu gewährleisten:

- Dauer der Datenspeicherung – wenn nicht möglich, Kriterien für die Festlegung der Dauer
- Belehrung über Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht bei besonderer Situation, Datenportabilität und Beschwerderecht zur Aufsichtsbehörde),
- Wenn die Datenverarbeitung auf einer Einwilligung beruht: Hinweis auf das Recht zum jederzeitigen Widerruf
- Grundlage der Bereitstellung der Daten auf gesetzlicher oder vertraglicher Basis und Folgen der Nichtbereitstellung,
- Bestehen einer automatisierten Einzelfallentscheidung einschließlich Profiling (z.B. das Erstellen eines umfassenden Nutzerprofils oder die Bildung von sog. Scorewerten durch Verknüpfen, Speichern, Auswerten und Zusammenlegen von verschiedenen Daten zu einer Person.)
- die Information darüber, ob die Datenverarbeitung gesetzlich bzw. vertraglich vorgeschrieben ist bzw. für einen Vertragsschluss erforderlich ist

Werden Daten von Drittenbezogen (z.B. durch Übermittlung) und nicht direkt beim Betroffenen erhoben, gelten nach **Art. 14 DSGVO** leicht abgewandelte Informationspflichten:

- Nach Art 14 Abs. 1 DSGVO müssen im Wesentlichen die Gleichen Informationen mitgeteilt werden wie bei der Direkterhebung. Weil der Betroffene aber keine Kenntnis von der weiteren Verarbeitung hat, muss ihm zusätzlich mitgeteilt werden, welche Kategorien von personenbezogenen Daten verarbeitet werden.
- Nach Art. 14 Abs. 2 DSGVO muss die Datenquelle und auch die Information angegeben werden.

Werden die Daten **direkt beim Betroffenen** erhoben, müssen die Informationen gem. Art. 13 DSGVO zum **Zeitpunkt** der Erhebung der personenbezogenen Daten mitgeteilt bzw. zur Verfügung gestellt werden. Bei der **weiteren Verarbeitung der Daten durch Dritte** kann die Information nach Art. 14 DSGVO auch später erfolgen. Der Verantwortliche muss die Informationen nachträglich innerhalb einer angemessenen Frist nach Erlangung der Daten mitteilen – die Frist ist abhängig von den spezifischen Umständen, darf aber maximal einen Monat andauern.

Von den Informationspflichten gelten allerdings einige **Ausnahmen**. So hat der Betroffene etwa keinen Informationsanspruch, wenn er bereits über diese Informationen verfügt. Der Anspruch ist auch dann ausgeschlossen, wenn die Informationserteilung einen unverhältnismäßig hohen Aufwand darstellt oder gar unmöglich ist. In diesem Fall ist allerdings eine öffentliche Bekanntmachung dieser Information, z.B. auf einer Webseite, erforderlich. Diese genannten Ausnahmen beziehen sich jedoch nur auf die Informationspflichten gem. Art. 14 DSGVO.

Die Datenschutzerklärung anpassen

Grundsätzlich muss **jeder Webseitenbetreiber** eine Datenschutzerklärung bereithalten, damit die Datenerhebung für die Besucher deutlich wird, welche Daten wie und wozu erhoben werden. Hier erfahren Sie alles über das Thema Datenschutzerklärung.

Mit Geltung der DSGVO müssen Webseitenbetreiber aber neue Anforderungen an diese Datenschutzerklärung beachten. Sie müssen:

- die **Rechtsgrundlage** angeben, auf der die Datenverarbeitung beruht (Art. 13 Abs. 1 c)).
- alle in Art. 13 genannten, verpflichtenden **Informationen** bereithalten (s.o.)
- in **klarer und einfacher Sprache** formuliert sowie **transparent und verständlich strukturiert** sein
- **leicht zugänglich** sein, sodass Betroffene sie mit nur einem Klick erreichen können

Daher entspricht eigentlich keine der bislang verwendeten Datenschutzerklärungen den Anforderungen der DSGVO. Aus diesem Grund muss sich jeder, der eine Webseite betreibt, seine Datenschutzerklärung **dringend an die DSGVO anpassen.**

Diese können Sie aber auch mit unserem kostenfreien Generator schnell und einfach DSGVO-konform umsetzen.

Verbot automatisierter Einzelfallentscheidungen

Nach Art. 22 DSGVO haben betroffene Personen das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Die Norm regelt also wie bisher das BDSG a.F. ein grundsätzliches Verbot, Entscheidungen nur von Maschinen treffen zu lassen.

Zu automatisierten Einzelfallentscheidungen zählen alle rechtlich relevanten oder sonst erheblich einschränkenden Entscheidungen, die **nicht von einem Mensch getroffen** wurden. Das können z.B. die automatische Ablehnung eines Online-Kreditantrags, ein Online-Einstellungsverfahren oder andere Maßnahmen sein, bei denen persönlichen Aspekte lediglich elektronisch ausgewertet werden. Dazu zählt vor allem auch das Profiling (z. B. für die Werbung), bei dem Daten zur Analyse oder Prognose für Persönlichkeitsmerkmale verwendet werden wie etwa die Arbeitsleistung, die wirtschaftliche Lage, die Gesundheit, persönlichen Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten. Allerdings wird hiernach nicht die Tätigkeit des Profilings selbst verboten, sondern nur die Entscheidungen, die auf dieser Grundlage getroffen werden. Somit ist das Sammeln und Bewerten von Daten zum Profiling selbst nicht von Art. 22 DSGVO erfasst.

Das Verbot, Entscheidungen auf diese Art treffen zu lassen, gilt nach Abs. 2 ausnahmsweise nicht, wenn eine automatisierte Entscheidung z. B. für den Abschluss oder die Erfüllung eines Vertrages mit dem Betroffenen erforderlich ist oder mit ausdrücklicher Einwilligung des Betroffenen erfolgt. Außerdem enthält das deutsche BDSG n.F. in § 37 weitere Ausnahmen vor – u. a. wenn dem Begehren des Betroffenen uneingeschränkt stattgegeben wird sowie und für Krankenversicherer im Rahmen der Leistungsprüfung. Dem Betroffenen ist in diesen Fällen aber die Möglichkeit zu eröffnen, die automatisierte Entscheidung überprüfen zu lassen.

Weiterhin in der Regel verboten bleiben solche Entscheidungen aber bei den bereits beschriebenen besonders sensiblen Daten (Art. 22 Abs. 4, Art. 9 DSGVO).

Vorgaben für Unternehmen

Technischer und organisatorischer Datenschutz

Verantwortliche müssen **geeignete technische und organisatorische Maßnahmen (TOM)** treffen, um Datenschutz und Datensicherheit zu gewährleisten (Art. 24, 25 DSGVO). Welche Maßnahmen konkret erforderlich sind, hängt u.a. vom Stand der Technik sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken für die persönlichen Rechte und Freiheiten ab. Daten sollen danach z.B. so wenige Daten wie möglich erhoben werden; diese sollen so schnell wie möglich pseudonymisiert werden. Außerdem müssen technische Geräte und IT-Anwendungen zukünftig so voreingestellt werden, dass nur solche Daten erhoben werden, die für den Zweck der Verarbeitung notwendig sind. Die DSGVO und das neue BDSG beschreiben im Einzelnen die erforderlichen Kontrollmaßnahmen (Art. 32 DSGVO und §§ 64 ff. und 71 bis 74 BDSG n.F.).

Gemeinsame Datenverarbeitung

Nach Art. 26 DSGVO ist es zukünftig auch zulässig, dass **mehrere verantwortliche Stellen** die erlaubte Datenverarbeitung gemeinsam durchführen können. Erforderlich ist hierzu eine transparente Vereinbarung, die die jeweiligen Zwecke und Verantwortlichkeiten sowie die Handhabung hinsichtlich der Betroffenenrechte festlegt. Betroffene können ihre Rechte aber weiterhin gegenüber jedem einzelnen Verantwortlichen geltend machen.

Auftragsverarbeitung

Die Auftragsverarbeitung (früher: Auftragsdatenverarbeitung) ist auch in Art. 28 und 29 DSGVO zukünftig erlaubt. Darunter versteht man die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen Auftragsverarbeiter gemäß den Weisungen des für die Verarbeitung Verantwortlichen auf Grundlage eines schriftlichen Vertrags. Darunter fallen z.B. Unternehmen, die ihre Daten bei einem externen Rechenzentrum speichern oder die eine externe Stelle mit der Erstellung etwa von Rechnungen beauftragen.

Die neuen Regelungen ähneln den Vorgaben des § 11 BDSG, enthalten aber weiter gehende Pflichten für beide Seiten. Die Auftragsverarbeitung ist nur zulässig, wenn der Auftragsverarbeiter hinreichende Garantien für eine ordnungsgemäße Datenverarbeitung bietet. Art. 28 DSGVO enthält eine umfangreiche Aufzählung von Regelungsinhalten sowie Rechte und Pflichten, die in dem Vertrag zwingend vereinbart werden müssen. Vieles ist ähnlich geregelt wie in § 11 BDSG. **Neu ist allerdings, dass auch der Auftragsverarbeiter ein „Verzeichnis der Verarbeitungstätigkeiten" führen muss** (s.u.).

Datenverarbeitung und auch Auftragsverarbeitung ist in Drittstaaten – wie bisher – nur zulässig, wenn dort ein angemessenes Datenschutzniveau gewährleistet ist. Die bisherige deutsche Restriktion, dass in Drittstaaten – auch bei angemessenem Datenschutzniveau – keine Daten der besonderen Art (z. B. Gesundheitsdaten) verarbeitet werden dürfen, entfällt nach der DSGVO.

Verzeichnis der Verarbeitungstätigkeiten

In Art. 30 DSGVO ist vorgeschrieben, dass der Verantwortliche bzw. der Auftragsverarbeiter ein „Verzeichnis der Verarbeitungstätigkeiten" führen müssen. Ähnlich dem bisherigen Verfahrensverzeichnis nach § 4g Abs. 2 in Verbindung mit § 4e BDSG handelt es sich dabei um eine **Dokumentation und Übersicht aller Verfahren, bei denen personenbezogene Daten verarbeitet werden**. Unter bestimmten Voraussetzungen können Unternehmen mit weniger als 250 Beschäftigten nach Art. 30 Abs. 5 DSGVO von dieser Pflicht ausgenommen sein.

Die neue Verordnung sieht im Vergleich zur bisherigen Rechtslage zusätzliche Angaben vor, wie z. B. Name und Kontaktdaten des ggf. bestellten Datenschutzbeauftragten, Löschfristen und die TOM. Unternehmen müssen dieses Verzeichnis außerdem auf Anfrage der Aufsichtsbehörde zur Verfügung stellen. Allerdings fällt die noch im BDSG geregelte Pflicht weg, das Verzeichnis jedermann auf Anforderung zur Verfügung zu stellen.

Datenschutzfolgenabschätzung

Gänzlich neu für Unternehmen ist die in Art. 35 DSGVO geregelte Datenschutzfolgenabschätzung. Diese erfolgt in **3 Stufen** und ist **schriftlich zu dokumentieren.**

1. In der ersten Stufe findet eine **systematische Risikobewertung (Schwellwertanalyse)** statt. Hier müssen Sie Ihre einzelnen Prozesse daraufhin überprüfen, ob im Einzelfall voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Für mehrere ähnliche Verarbeitungsvorgänge mit ähnlichem Risiko reicht eine gemeinsame Abschätzung. Ein solches Risiko besteht nach Abs. 3 insbesondere bei der Verwendung neuer Technologien, die automatisiert, systematisch und umfassend Daten erfassen, verarbeiten und bewerten. Auch kann aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ein solches Risiko bestehen. Schließlich kann die Verarbeitung besonderer Kategorien von Daten (z.B. Gesundheitsdaten oder Religionszugehörigkeit i.S.d. Art. 9 DSGVO) eine weitere Prüfung notwendig machen. Doch auch, wenn Ihr Unternehmen besonders schützenswerte Daten verarbeitet, bedeutet das nicht zwangsweise, dass auch ein hohes

Risiko besteht – dies hängt von Ihrem Sicherheitskonzept ab. Letztlich gibt es an diesem Punkt noch keine Rechtssicherheit. Als weitere Hilfestellung für die Einschätzung dienen die ersten „Leitlinien zu DSFA der Art.-29-Datenschutzgruppe“, die aber noch durch eine sog. Blacklist der deutschen Aufsichtsbehörden präzisiert werden (Art. 35 Abs. 4 DSGVO).
2. Wenn ein solches Risiko im Hinblick auf den Prozess besteht, müssen Sie in einer 2. Stufe eine **Bewertung** dahingehend vornehmen, ob die geplanten Abhilfemaßnahmen und Sicherheitsvorkehren ausreichen, um den **Schutz der Daten** zu gewährleisten. Außerdem müssen Sie den Nachweis erbringen, dass Sie die DSGVO eingehalten haben und den Interessen der Betroffenen Rechnung getragen wird.
3. Kommt Ihre Bewertung zu dem Ergebnis, dass trotz möglicher Maßnahmen ein hohes Risiko besteht, müssen Sie in einer 3. Stufe die Aufsichtsbehörde konsultieren (Art. 36DSGVO). Diese kann dann innerhalb von 8 Wochen Empfehlungen aussprechen. Diese Frist kann je nach Komplexität von der Aufsichtsbehörde verlängert werden. Zuständige Behörde ist in Deutschland der Bundesbeauftragte nach § 69Abs. 1 BDSG n.F..

Ist in dem Unternehmen ein Datenschutzbeauftragter bestellt, wird dieser auf Anfrage beratend in die Durchführung einer Datenschutz-Folgenabschätzung eingebunden (Art. 35 Abs. 2 und Art. 39 Abs. 1 c) DSGVO).

Melde- und Informationspflichten bei Datenpannen

Für die bisher in § 42a BDSG vorgeschrieben **Melde- und Informationspflichten bei Datenpannen/Incidents** gelten zukünftig die Vorgaben des Art. 33 DSGVO. Danach müssen grds. alle Verletzungen des Schutzes personenbezogener Daten gemeldet werden, es sei denn, das Risiko für persönliche Rechte und Freiheiten ist unwahrscheinlich.

Unternehmen müssen solche Incidents der Aufsichtsbehörde **binnen 72 Stunden** nach Bekanntwerden der Verletzung erfolgen und **folgende Informationen übermitteln**:

- Beschreibung des Incidents, Angabe der Kategorie der betroffenen Daten, Anzahl der Betroffenen und betroffenen Datensätze,
- Name und Kontaktdaten des Datenschutzbeauftragten oder eines anderen informierten Ansprechpartners,
- Beschreibung der Folgen der Datenschutzverletzung,
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

In Deutschland ist der Bundesbeauftragte für Datenschutz die zuständige Aufsichtsbehörde (§ 65 BDSG n.F.).

Außerdem müssen die von einer Verletzung **Betroffenen grds. selbst benachrichtigt** werden (Art. 34 DSGVO und § 66 BDSG n.F.). Die Benachrichtigungspflicht **entfällt** aber, wenn:

- der Verantwortliche Vorkehrungen getroffen hat, die Daten Unbefugten unzugänglich zumachen, etwa durch Verschlüsselung,
- der Verantwortliche nachträglich Maßnahmen ergriffen hat, durch die das hohe Risiko für die Rechte und Freiheiten der Betroffenen aller Wahrscheinlichkeit nach nicht mehr bestehen,
- sie einen unverhältnismäßig hohen Aufwand erfordern würde – dann muss allerdings eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme erfolgen.

Datenschutzbeauftragter

Nach Art. 37 DSGVO müssen Unternehmen immer dann **einen betrieblichen Datenschutzbeauftragten** benennen, wenn ihre Kerntätigkeit bzw. die ihres Auftragsverarbeiters:

- aus Verarbeitungsvorgängen besteht, die nach Art, Umfang und/oder Zweck eine systematische Überwachung erfordern
- die Verarbeitung besonders sensibler Daten nach Art. 9 und 10 DSGVO betrifft

§ 38 BDSG n.F. erweitert die Gründe für die Benennung eines Datenschutzbeauftragten. Sie ist danach auch dann erforderlich, wenn der Verantwortliche oder Auftragsverarbeiter:

- in der Regel mindestens 10 Personen ständig mit der Datenverarbeitung beschäftigt
- Verarbeitungen vornimmt, die der Datenschutzfolgenabschätzung unterliegen (dies ist insbesondere relevant bei Gesundheitsdaten)
- personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet

Der Datenschutzbeauftragte muss entsprechend beruflich und fachlich qualifiziert sein. Er kann Mitarbeiter des datenverarbeitenden Unternehmens sein, es können aber auch ein externer eingesetzt werden. Hat ein Konzern mehrere Gesellschaften, können diese auch einen gemeinsamen Beauftragten benennen (Konzerndatenschutzbeauftragter). Ohne wichtigen Grund gem. § 626 BGB darf er weder abberufen noch gekündigt werden (§ 38 in Verbindung mit § 6 Abs. 4 BDSG n.F.).

Nach Art. 38 DSGVO ist der Datenschutzbeauftragte frühzeitig einzubinden, fachlich weisungsfrei und berichtet unmittelbar der höchsten Managementebene. Seine Aufgaben umfassen nach Art. 39 DSGVO die:

- Unterrichtung und Beratung des Verantwortlichen bzw. Auftragsverarbeiters sowie deren Beschäftigten,
- Überwachung der Einhaltung der rechtlichen Regelungen sowie der Strategien des Verantwortlichen bzw. Auftragsverarbeiters einschließlich der Zuweisung von Zuständigkeiten und die Sensibilisierung und Schulung der relevanten Mitarbeiter
- Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung gem. Art. 35 DSGVO
- Zusammenarbeit mit der Aufsichtsbehörde
- Tätigkeit als Anlaufstelle der Aufsichtsbehörde

Er kann im Unternehmen auch zusätzlich andere Aufgaben wahrnehmen, sofern sichergestellt ist, dass daraus keine Interessenkonflikte erwachsen.

Welche Risiken drohen bei einer verspäteten Umsetzung der neuen Vorgaben?

Die zuständigen Aufsichtsbehörden können zunächst nach Art. 83 DSGVO **Bußgelder** verhängen. Diese können – je nach Verstoß und dessen Schwere – bis zu 20 Millionen Euro oder bis zu 4 Prozent des weltweiten Jahresumsatzes eines Unternehmens betragen. Es gilt immer der jeweils höhere Betrag.

Daneben besteht auch weiterhin die Möglichkeit, wegen bestimmten Datenschutzrechtsverstößen **wettbewerbsrechtlich abgemahnt** zu werden, was – je nach Ausmaß und Zahl der Verstöße – hohe Abmahnkosten verursachen kann.

Neu ist auch, dass Betroffene wegen der Verletzung des Datenschutzrechts im Rahmen ihrer **Schadensersatzansprüche** nun auch ihren immateriellen Schaden geltend machen können. Nach außen **haftet immer die Unternehmensleitung**, auch für Mitarbeiter-Fehlverhalten.

Fazit: Was kommt auf Unternehmen zu?

Die DSGVO erweitert für Unternehmen die bereits bekannten Pflichten und erhöht die rechtlichen, betrieblichen und technisch-organisatorischen Anforderungen an den Datenschutz.

Neu sind insbesondere die **umfassenden Informationspflichten** und die Pflicht zur **Datenschutz-Folgenabschätzung** bei besonderen Risiken für die erhobenen Daten. Außerdem wird neu eingeführt, dass auch der **Auftragsverarbeiter** ein „**Verzeichnis der Verarbeitungstätigkeiten**“ führen muss. Das deutsche Umsetzungsgesetz erweitert außerdem die Gründe für die Benennung eines **Datenschutzbeauftragten**. Schließlich müssen Unternehmen auch erweiterten Ansprüchen von Betroffenen gerecht werden.

Vor diesem Kontext wird deutlich, dass die rechtskonforme Umsetzung der DSGVO eine intensive Prüfung und einen gewissen Aufwand erfordert. Dabei ist die Umsetzungsfrist bis Mai 2018 relativ gering, während die Risiken einer

mangelhaften Umsetzung aufgrund der Anhebung der Bußgelder sehr hoch sind. Den exemplarischen Ablauf einer DSGVO-Anpassung können Sie unserer Grafik entnehmen. Die Grafik finden Sie am Ende unseres Beitrages.

Beratung im Einzelfall

Wir raten daher dringend, sich **so bald wie möglich** rechtlich umfassend durch einen Rechtsanwalt oder externen Datenschutzbeauftragten beraten zu lassen, um die erforderlichen neuen Prozesse rechtzeitig zu etablieren.

Unsere auf das Datenschutz **spezialisierten Rechtsanwälte, insbesondere unser Datenschutzbeauftragter Peter Mainzer** mit seiner jahrzehntelangen Erfahrung auf dem Gebiet des Datenschutzes in Unternehmen, können sie umfassend und rechtssicher beraten.

Rufen Sie uns unter der Rufnummer 0221 / 9688 8154 43 (Beratung bundesweit) an!

ANHANG Grafik „Exemplarischer Ablauf einer DSGVO-Anpassung“