Keller Steuerberater

Mathias Keller, Steuerberater
Glarnerstraße 4
79713 Bad Säckingen

Tel. +49 7761 2552
Fax +49 7761 4074

www.steuerberaterkeller.de
info@steuerberaterkeller.de

USt-IdNr. DE 294 54 65 06

Merkblatt

Das neue Datenschutzrecht: Was es für Unternehmer bedeutet

Inhalt

Das Datenschutzrecht wird in der Praxis immer noch häufig vernachlässigt oder bleibt gar unberücksichtigt. Angesichts wachsender Sensibilität und entsprechender Sachzwänge auf Unternehmensseite, zunehmender Prüfungsdichte und Sanktionshäufigkeit von Seiten der Aufsichtsbehörden sowie nicht zuletzt der mit moderner Datenverarbeitungs- und Informationstechnik steigenden Verletzlichkeit gehören Datenschutzlücken jedoch zu den nicht (mehr) vernachlässigbaren **Geschäftsrisiken**. Hierauf reagierte der europäische Verordnungsgeber mit der Datenschutz-Grundverordnung (**DSGVO**), die **seit dem 25.05.2018 uneingeschränkt** in allen Staaten der Europäischen Union (EU) für grundsätzlich **gleiche Standards** sorgt. Zugleich wird mit der DSGVO das Ziel verfolgt, das **Datenschutzrecht** zu **modernisieren**, um bessere Antworten auf die Globalisierung und datenschutzrechtliche Herausforderungen zu geben, die die zunehmende Digitalisierung und das Internetzeitalter mit sich bringen.
Die neuen Regelungen sollen zu **gleichen Wettbewerbsbedingungen** für alle Unternehmen auf dem europäischen Markt beitragen.

Aus der DSGVO ergeben sich im Vergleich zum Bundesdatenschutzgesetz (**BDSG**) einige Änderungen, wenngleich die bisherigen datenschutzrechtlichen **Grundprinzipien fortbestehen**. Auch seit Inkrafttreten der DSGVO gilt das (novellierte) BDSG weiter, weshalb **beide Regelwerke zu beachten** sind. Allerdings wirkt die DSGVO unmittelbar und direkt: Sofern sie keine ausdrücklichen Möglichkeiten für einzelstaatliche Regelungen vorsieht, **verdrängt** sie die **Vorschriften der einzelnen EU-Mitgliedstaaten** zur Datenverarbeitung.

Im Folgenden wird ein Überblick über das **verbindlich geltende Datenschutzrecht** für private Unternehmen gegeben.

1 Die zentralen Begriffe

1.1 Personenbezogene Daten

Personenbezogene Daten sind **Einzelangaben über** persönliche oder sachliche **Verhältnisse einer** bestimmten oder bestimmbaren natürlichen **Person** (dem Betroffenen), wie zum Beispiel Alter, Anschrift, Vermögen, Äußerungen, Überzeugungen.

1.2 Anwendungsbereich und Marktortprinzip

Unternehmen unterliegen dem Datenschutzrecht nur dann, wenn

- sie personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder
- personenbezogene Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben.

Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten gilt dabei als **automatisiert**, wenn Datenverarbeitungsanlagen zum Einsatz kommen.

> **Hinweis**
>
> **Ausgenommen** ist die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten für **ausschließlich persönliche oder familiäre Tätigkeiten**.

Die DSGVO gilt nach dem sogenannten **Marktortprinzip** nicht nur für in der EU niedergelassene Unternehmen, sondern auch für solche, deren Angebot sich an einen bestimmten nationalen Markt innerhalb der EU richtet. Der **Anwendungsbereich** erstreckt sich damit **auch** auf **außereuropäische Unternehmen**, die auf dem europäischen Markt tätig sind. So sollen **gleiche Wettbewerbsbedingungen** für alle Unternehmen gelten, die Waren und Dienstleistungen in der EU anbieten.

> **Hinweis**
>
> Insbesondere erhalten auch ausländische Unternehmen nur dann Zugang zum EU-Binnenmarkt, wenn sie sich an die dort geltenden Regelungen halten.

1.3 One-Stop-Shop

Eine **echte Neuerung** der DSGVO ist der „One-Stop-Shop-Mechanismus“: Für Unternehmen mit Niederlassungen in mehreren EU-Mitgliedstaaten, in denen sie Datenverarbeitung betreiben, ist nur die **Aufsichtsbehörde an** ihrem **Hauptsitz zuständig**. Damit ist unerheblich, an welchem Standort sich der Server befindet.

Sobald **mehrere Mitgliedstaaten betroffen** sind, werden deren Datenschutzaufsichtsbehörden in den Abstimmungsmechanismus eingebunden. Einigen sich die federführende und die übrigen betroffenen Aufsichtsbehörden auf eine **einheitliche Vorgehensweise**, ergeht ein entsprechender **Beschluss an die Hauptniederlassung** des Unternehmens. Diese hat dann die erforderlichen Maßnahmen zu treffen, um die Verarbeitungstätigkeiten aller Niederlassungen innerhalb der EU mit dem Beschluss in Einklang zu bringen. Die federführende Aufsichtsbehörde ist über die Maßnahmen zu unterrichten und unterrichtet ihrerseits wiederum die übrigen betroffenen Aufsichtsbehörden.

Wird **kein Konsens** zwischen der federführenden Aufsichtsbehörde und den mitbetroffenen Aufsichtsbehörden erzielt, sieht die DSGVO das „**Kohärenzverfahren**“ mit der Befugnis des **Europäischen Datenschutzausschusses** vor, **verbindliche Beschlüsse** zu treffen, um die ordnungsgemäße und einheitliche Anwendung der Verordnung in Einzelfällen sicherzustellen. Die federführende Aufsichtsbehörde trifft dann den **endgültigen Beschluss** auf der Grundlage eines solchen Beschlusses gegenüber der Hauptniederlassung des Unternehmens, das ihr EU-weit Folge zu leisten hat.

Hinweis

Um zur einheitlichen Anwendung der DSGVO beizutragen, werden im Kohärenzverfahren über die Klärung von Einzelfragen hinaus aber auch gemeinsame Positionen, Stellungnahmen und Richtlinien bestimmt.

Wird bei einer Aufsichtsbehörde eine **Beschwerde** hierzu **eingereicht**, unterrichtet sie den Beschwerdeführer über den Beschluss. Wird die Beschwerde **abgewiesen oder abgelehnt**, ergeht der Beschluss gegenüber dem Beschwerdeführer durch die angerufene Aufsichtsbehörde; das Unternehmen wird lediglich darüber informiert. Wird einer Beschwerde nur **teilweise stattgegeben**, ergehen zwei Beschlüsse: einer durch die federführende Aufsichtsbehörde gegenüber dem Unternehmen und einer durch die angerufene Aufsichtsbehörde gegenüber dem Betroffenen.

Hinweis

Zeitgleich mit dem Erlass des endgültigen Beschlusses gegenüber dem Unternehmen oder dem Beschwerdeführer wird ein etwaiger Beschluss des Europäischen Datenschutzausschusses auf dessen Website veröffentlicht.

In „Marktortfällen“ – wenn also keine Niederlassung in der EU existiert, die DSGVO aber dennoch anwendbar ist (z.B. weil sich das Angebot an EU-Bürger richtet) – gibt es diesen Kooperationsmechanismus nicht. Stattdessen ist **jede Aufsichtsbehörde** im Hoheitsgebiet ihres Mitgliedstaats **zuständig** und kann Entscheidungen erlassen. Daher können hier auch divergierende Entscheidungen ergehen.

1.4 Verbot mit Erlaubnisvorbehalt

Auch nach der DSGVO gilt für die Verarbeitung personenbezogener Daten der allgemeine Grundsatz des Verbots mit Erlaubnisvorbehalt: Es ist **grundsätzlich verboten, was nicht ausdrücklich erlaubt** ist. Das bedeutet konkret, dass die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten verboten sind, es sei denn,

- sie sind durch eine Rechtsvorschrift ausdrücklich erlaubt oder angeordnet oder
- der Betroffene hat seine Einwilligung dazu erklärt.

Hinweis

Sollte der Betroffene aus gesundheitlichen Gründen nicht mehr in der Lage sein, Inhalte, Tragweite und Bedeutung einer Einwilligung über seine Rechte nach der DSGVO zu erfassen, kann sein Betreuer als gesetzlicher Vertreter die Einwilligung abgeben.

Soll eine **Einwilligung** Grundlage für eine Erhebung, Verarbeitung oder Nutzung sein, ist zu beachten, dass

- sie **freiwillig** erfolgen muss,
- der **Betroffene vorher** über die Tragweite seiner Einwilligung **aufgeklärt** werden muss,
- sie grundsätzlich der **Schriftform** bedarf (es sei denn, wegen besonderer Umstände ist eine andere Form angemessen) und
- der **Betroffene** auch darüber zu **informieren** ist, was geschieht, wenn er nicht einwilligt.

Ausdrücklich auf diese Daten beziehen muss sich die Einwilligung bei der Verarbeitung **besonderer Arten personenbezogener Daten**, also bei Angaben über

- rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder politische Überzeugungen,
- Gewerkschaftszugehörigkeit,
- Gesundheit oder
- Sexualleben.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten unterliegen einer **Vielzahl von Einschränkungen**. Bereits bei der Erhebung personenbezogener Daten sind die **Zwecke**, für die die Daten verarbeitet oder genutzt werden sollen, **konkret festzulegen**. Dies gilt auch für die geschäftsmäßige Datenverarbeitung. Dabei besteht eine grundsätzliche **Zweckbindung**, von der nicht ohne weiteres abgewichen werden darf. **Änderungen des Verarbeitungszwecks** sind grundsätzlich nur erlaubt, wenn sie mit dem ursprünglichen Erhebungszweck vereinbar sind. Als Kriterien zur **Beurteilung der Vereinbarkeit** einer Zweckänderung sieht die DSGVO unter anderem vor:

- die **Verbindung** zwischen den Zwecken,
- den **Gesamtkontext**, in dem die Daten erhoben wurden,
- die **Art** der personenbezogenen Daten,
- mögliche **Konsequenzen** der zweckändernden Verarbeitung für den Betroffenen und
- das Vorhandensein von angemessenen **Sicherheitsmaßnahmen** (z.B. eine Verschlüsselung).

Hinweis

Eine **strikte Zweckbindung** besteht für Daten, die ausschließlich zur Datenschutzkontrolle, Datensicherung, Sicherung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage oder zur wissenschaftlichen Forschung gespeichert werden.

Stets muss zwischen einander entgegenstehenden Interessen an der **Zweckänderung** und schutzwürdigen Interessen des Betroffenen abgewogen werden. Eine Verwendung für andere als die zuvor festgelegten Zwecke kommt **als Ausnahme** unter anderem in Betracht

- zur **Wahrung berechtigter Interessen** der verantwortlichen Stelle oder eines Dritten oder,
- wenn die **Daten allgemein zugänglich** sind oder veröffentlicht werden dürfen.

Hinweis

Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Auf der anderen Seite liegt **keine Zweckänderung** vor, soweit die Daten verwendet werden für

- die Rechnungsprüfung,
- die Wahrnehmung von Aufsichts- und Kontrollbefugnissen,
- Organisationsuntersuchungen sowie
- Ausbildungs- und Prüfungszwecke der speichernden Stelle.

Hinweis

In Unternehmen wird der größte Teil der personenbezogenen Daten (u.a. Kundendaten) zur Erfüllung eigener Geschäftszwecke verwendet.

2 Die zentralen Schritte

2.1 Datenerhebung

Auch nach der DSGVO gilt das **Prinzip der Datensparsamkeit**: Die Erhebung und Verarbeitung personenbezogener Daten muss dem Zweck angemessen und sachlich relevant sowie auf das für den Zweck der Datenverarbeitung notwendige Maß beschränkt sein.

Die Daten sind grundsätzlich **beim Betroffenen** zu erheben. Es ist ihm mitzuteilen, zu welchem Zweck dies geschieht. Er hat **Anspruch** darauf **zu erfahren**,

- welche **verantwortliche** Stelle die Daten erhoben hat und
- welche **Zweckbestimmung** der Datenerhebung zugrunde liegt.

Nur so ist gewährleistet, dass der Betroffene seine **Datenschutzrechte wahrnehmen** kann.

Ohne Mitwirkung des Betroffenen dürfen Daten **nur** erhoben werden, **wenn**

- eine **Rechtsvorschrift** dies vorsieht oder zwingend voraussetzt **oder**
- die Erhebung beim Betroffenen einen unverhältnismäßig **hohen Aufwand zur Folge** hätte und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Hinweis

Ob die dafür befragte Stelle die erbetenen Daten übermitteln darf, muss besonders geprüft werden.

2.2 Datenübermittlung

2.2.1 Das Recht auf Datenübertragbarkeit

Neu eingeführt wurde durch die DSGVO das Recht auf Datenübertragbarkeit. Es räumt betroffenen Personen unter bestimmten Voraussetzungen den Anspruch ein, eine **Kopie der** sie betreffenden personenbezogenen **Daten** in einem üblichen und maschinenlesbaren Dateiformat **zu erhalten**. Der Nutzer hat das Recht, Daten von einem Anbieter zu einem anderen „mitzunehmen“.

Die Regelung kann damit insbesondere bei Social Networks den **Wechsel zu** einem **anderen Anbieter** erleichtern. Sie gilt aber letztlich bei jeder automatisierten Verarbeitung personenbezogener Daten auf Basis einer Einwilligung oder Vertragsbeziehung mit dem Betroffenen. Allerdings ist das Recht auf Datenübertragbarkeit **auf** die **Daten beschränkt**, die **die betroffene Person** dem Verarbeiter **zur Verfügung gestellt** hat.

2.2.2 Datenübermittlung in Drittstaaten

Eine Übermittlung von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation ist **nur zulässig, wenn** der Verantwortliche und der Auftragsverarbeiter die zur Datenübermittlung in Drittländer und an internationale Organisationen geltenden Bedingungen erfüllen und auch die sonstigen Bestimmungen der DSGVO beachtet werden. Eine Übermittlung ist danach zulässig, wenn die Europäische Kommission entschieden hat, dass ein **angemessenes Schutzniveau besteht**. Andernfalls darf eine entsprechende Übermittlung nur stattfinden, wenn der Verantwortliche oder Auftragsverarbeiter **geeignete Garantien** vorgesehen hat und **durchsetzbare Rechte** sowie **wirksame Rechtsbehelfe** zur Verfügung stehen. Hierzu gehören

- unternehmensinterne Datenschutzvorschriften (sog. Binding Corporate Rules) und
- Standarddatenschutzklauseln,

die von der Kommission oder der Aufsichtsbehörde in einem speziellen Verfahren akzeptiert werden müssen.

Ob in einem Land ein **angemessenes Datenschutzniveau** besteht, kann **festgestellt** werden **durch**

- die verantwortliche Stelle selbst, die Daten übermitteln will (Kriterien: Art der Daten, Zweckbestimmung, Dauer der geplanten Verarbeitung, Herkunft und Bestimmungsland, für den Empfänger geltende Rechtsnormen, Standesregeln und Sicherheitsmaßnahmen), und
- die Europäische Kommission.

Hinweis

Darüber hinaus kommt eine Übermittlung von Daten an einen Drittstaat auch im Rahmen **weitreichender Ausnahmeregelungen** in Betracht.

2.3 Vorabkontrolle

Für automatisierte Verarbeitungen, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, sieht das BDSG eine Prüfung vor Beginn der Verarbeitung vor. Beispielhaft – nicht abschließend – nennt das Gesetz zwei Fallgestaltungen, in denen die Vorabkontrolle notwendig ist:

- bei der Verarbeitung von personenbezogenen **Daten besonderer Art**,
- bei **Verfahren zur Bewertung** von Persönlichkeit, Fähigkeit, Leistung oder Verhalten des Betroffenen.

Eine **Vorabkontrolle entfällt**, wenn

- eine gesetzliche Verpflichtung zur Durchführung der Datenverarbeitung besteht,
- die Einwilligung des Betroffenen vorliegt,
- die Erhebung, Verarbeitung oder Nutzung im Rahmen der Zweckbestimmung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erfolgt.

Zuständig für die Durchführung der Vorabkontrolle ist der **Datenschutzbeauftragte**. Ihm sind von der verantwortlichen Stelle für die Datenverarbeitung vor der Durchführung der Vorabkontrolle bestimmte Informationen zur Verfügung zu stellen.

2.4 Datensicherheit

2.4.1 Maßnahmen zur Datensicherheit

Als **zentrales Prinzip des Datenschutzes** wurde in der DSGVO auch die Gewährleistung von Datensicherheit verankert. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, der Umstände und des Zwecks der Datenverarbeitung, aber auch der unterschiedlichen Schwere und Eintrittswahrscheinlichkeit des Risikos für die persönlichen Rechte und Freiheiten, haben der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen** umzusetzen. Dabei muss das Sicherheitslevel im Verhältnis zum Risiko angemessen sein.

Schon bei der Konzeption von IT-Systemen muss der Datenschutz berücksichtigt werden **(„Privacy by Design“**). Dabei geht es in erster Linie darum, den Umfang der erhobenen und verarbeiteten personenbezogenen Daten auf ein Minimum zu beschränken.

Zu einer datenschutzgerechten Technikgestaltung gehören auch entsprechende Voreinstellungen von IT-Systemen und elektronischen Diensten (**„Privacy by Default“**). So sollte etwa ein WLAN-Router nur mit voreingestellter Verschlüsselung ausgeliefert werden.

Mit einem „**Datenschutzaudit**“ können sowohl Anbieter von Datenverarbeitungssystemen und -programmen als auch verantwortliche Stellen ihre Datenschutzkonzepte sowie ihre technischen Einrichtungen mit einem datenschutzrechtlichen Gütesiegel versehen lassen und damit werben. Die Prüfung sollte durch unabhängige und zugelassene Gutachter erfolgen.

Besondere Bedeutung kommt auch der Pflicht zur Information bei **Datenschutzpannen** zu. Unternehmen, Vereine und Verbände, die personenbezogene Daten erheben, verarbeiten oder nutzen, müssen ebenso wie jedes ihnen gleichgestellte öffentlich-rechtliche Wettbewerbsunternehmen **bei Verlust** von als besonders gefährdet eingestuften Daten die **Betroffenen** sowie die Aufsichtsbehörde **informieren**. Unterbleibt diese Information oder ist sie nicht richtig, nicht vollständig oder nicht rechtzeitig, **droht** ein **Bußgeld**.

Die DSGVO sieht für Verantwortliche und Auftragsverarbeiter **deutlich erweiterte Nachweispflichten** vor („accountability“): Der für die Verarbeitung Verantwortliche muss nachweisen können, dass er die Datenschutzgrundsätze der DSGVO einhält. Auftragsverarbeiter müssen ihm dazu alle erforderlichen Informationen zur Verfügung stellen.

Folgende Prozesse und Dokumente sollte ein Unternehmen **prüfen bzw. vorhalten**:

- Dokumentation der Datenverarbeitungsprozesse im Unternehmen,
- Datenschutzerklärungen (Erweiterung der Informationspflichten),
- Einwilligungserklärungen (Verschärfung der formalen Vorgaben),
- Prozess für den Widerruf der Einwilligung,
- an die DSGVO angepasste Version der Betriebsvereinbarungen,
- Prozesse zur Umsetzung von Widersprüchen,
- Vereinbarungen zur Auftragsverarbeitung (Haftungsregelung, Dokumentation),
- Prozess bei Datenpannen (neue Vorgaben),
- Verfahren, um Daten in gängigem elektronischen Format übertragen zu können,
- zielgruppengerechte Schulungen (Neuerungen der DSGVO und eigener Prozesse),
- Risk Assessment (Festlegung geeigneter technisch-organisatorischer Maßnahmen),
- Privacy Impact Assessment (als Methode der Datenschutz-Folgenabschätzung; vgl. Punkt 2.4.2),
- Monitoring nationaler Gesetzgebung,
- Fortbildungen.

Hinweis

Jedes Unternehmen sollte ein effektives Datenschutzmanagementsystem mit den oben aufgeführten Prozessen integrieren und vor allem die einzelnen Schritte dokumentie-

ren, so dass auch gegenüber einer Aufsichtsbehörde der Nachweis geführt werden kann, dass geeignete Strategien erarbeitet und Maßnahmen ergriffen wurden.

2.4.2 Datenschutz-Folgenabschätzung

Mit der Vorabkontrolle (siehe Punkt 2.3) eng verwandt ist die mit der DSGVO **neu eingeführte** Datenschutz-Folgenabschätzung. Sie sieht vor, dass **Risiken und** deren **mögliche Folgen** für die persönlichen Rechte und Freiheiten der Betroffenen vorab **bewertet werden** – und hierbei vor allem **Eintrittswahrscheinlichkeit und Schwere** eines möglichen Risikos.

Überdies soll das Unternehmen auch **systematisch** die verfolgten **Zwecke** der Datenverarbeitung **beschreiben**. Ebenso sollen **Maßnahmen, Garantien und Verfahren formuliert** bzw. geprüft werden, mit denen bestehende Risiken eingedämmt und die sonstigen Vorgaben der Verordnung eingehalten werden können.

Hinweis

Wurde ein solcher bestellt, ist der Datenschutzbeauftragte bei der Datenschutz-Folgenabschätzung zu beteiligen.

Ergibt die Datenschutz-Folgenabschätzung, dass die geplante Datenverarbeitung tatsächlich ein **hohes Risiko** zur Folge hätte, muss der Verantwortliche die zuständige **Aufsichtsbehörde konsultieren**, sofern er keine Maßnahmen zur Eindämmung des Risikos trifft.

Hinweis

Die Datenschutz-Folgenabschätzung ist ein wichtiges Mittel für Unternehmen, um ihre Dokumentationspflichten zu erfüllen. Allein aus diesem Grund sollten Unternehmen zeitnah Strukturen und Prozesse schaffen, um die detaillierten Anforderungen an den Datenschutz zu erfüllen.

Die nachfolgende Tabelle liefert einen Überblick über die verschiedenen Schutzbedarfskategorien und die jeweilige Schadensschwere mitsamt Beispielen.

Schutzbedarf	Schadensschwere: Beeinträchtigung des Persönlichkeitsrechts der Betroffenen	Beispiele
normal (gering oder mittel)	Tolerabel. Bei Datenmissbrauch bestünden nur geringfügige (wirtschaftliche oder gesellschaftspolitische) Auswirkungen auf Betroffene. Es geht also um nicht zur Veröffentlichung bestimmte Daten, deren Veröffentlichung oder Verfälschung nur geringfügige Schäden für die Betroffenen nach sich ziehen können.	**Gering:** Öffentliche Register; Anschrift; Kontaktdaten **Mittel:** Daten über Geschäfts- und Vertragsbeziehungen; Kontostände; Prüfungsergebnisse; Personaldaten (soweit nicht von hohem Schutzbedarf); Kreditauskünfte
hoch	Erheblich. Bei Datenmissbrauch bestünden erhebliche (wirtschaftliche oder gesellschaftspolitische) Auswirkungen auf Betroffene bis hin zur Beeinträchtigung von deren persönlicher Unversehrtheit. Es geht also um sensible Daten, deren Veröffentlichung oder Verfälschung hohe Folgeschäden für die Betroffenen nach sich ziehen können.	Steuerdaten; Daten über strafbare Handlungen; Daten, die einem Berufs-, Geschäfts-, Fernmelde- oder Mandantengeheimnis unterliegen; Personaldaten (soweit nicht von normalem Schutzbedarf) wie Beurteilungen, berufliche Laufbahn, Angaben über Behinderung etc.
sehr hoch	Besonders bedeutsam und nicht tolerabel. Datenmissbrauch würde für Betroffene den wirtschaftlichen oder gesellschaftspolitischen Ruin bedeuten oder ihre persönliche Unversehrtheit gravierend beeinträchtigen. Es geht also um hochsensible Daten, deren Veröffentlichung oder Verfälschung die Persönlichkeitsrechte der Betroffenen verletzt oder Schaden an deren Leib, Leben oder Ansehen verursacht.	Adressen von polizeilichen V-Leuten, Adressen von Zeugen in bestimmten Strafverfahren

3 Die zentrale Position: Der Datenschutzbeauftragte

3.1 Notwendigkeit einer Bestellung

Laut DSGVO müssen Unternehmen einen Datenschutzbeauftragten bestellen, **wenn** die **Kerntätigkeit** des Unternehmens oder desjenigen, der die Daten im Auftrag verarbeitet, in einer Datenverarbeitung besteht,

- die aufgrund ihres Zwecks oder Umfangs eine umfangreiche, regelmäßige und systematische **Beobachtung** von betroffenen Personen **erfordert oder**
- eine umfangreiche Verarbeitung von **besonders schutzwürdigen Daten umfasst**.

Hinweis

Als Kerntätigkeit versteht die DSGVO dabei die Hauptaktivität des Unternehmens.

Zudem sieht die DSGVO **zwei Öffnungsklauseln** vor:

- Unternehmen oder Auftragsverarbeiter können auch **freiwillig** einen Datenschutzbeauftragten bestellen.
- Die EU-Mitgliedstaaten können im nationalen Recht für **weitere Fälle** die Bestellung eines Datenschutzbeauftragten **vorschreiben**.

Der Bundesgesetzgeber hat von letzterer Möglichkeit Gebrauch gemacht: **Unternehmen in Deutschland** müssen wie bisher einen Datenschutzbeauftragten bestellen, wenn **mehr als neun Personen** mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. **Auskunfteien, Adresshändler** sowie **Markt- und Meinungsforschungsinstitute** müssen in jedem Fall einen Datenschutzbeauftragten bestellen.

Damit **bleibt** es bei der **bisher geltenden Rechtslage**.

3.2 Stellung im Unternehmen

Der Datenschutzbeauftragte ist **unmittelbar dem Geschäftsführer** des Unternehmens **zu unterstellen** und in der Ausübung seiner Aufgaben **weisungsfrei**. Außerdem genießt er einen **besonderen Kündigungsschutz**: Während der Bestellung bzw. bis ein Jahr nach Beendigung der Bestellung darf ihm nur aus wichtigem Grund (z.B. Arbeitsverweigerung) gekündigt werden.

Hinweis

Der besondere Kündigungsschutz gilt jedoch nicht für freiwillig bestellte Datenschutzbeauftragte.

Der Geschäftsführer eines Unternehmens ist nicht an das Votum des Datenschutzbeauftragten gebunden. Die **Letztverantwortung** für die Datenverarbeitung **verbleibt** damit bei der **Unternehmensleitung**.

Zum Datenschutzbeauftragten darf nur bestellt werden, wer die **erforderliche „Fachkunde und Zuverlässigkeit**“ besitzt. Die verantwortliche Stelle ist verpflichtet, dem Datenschutzbeauftragten zum Erhalt seiner Fachkunde die **Teilnahme an Schulungs- und Fortbildungsveranstaltungen** zu ermöglichen und hierfür die Kosten zu übernehmen.

Hinweis

Um Interessenkonflikte zu vermeiden, sollten Unternehmen IT- und Personalverantwortliche sowie IT-Systemadministratoren nicht als Datenschutzbeauftragte bestellen.

3.3 Aufgaben

Die Aufgaben des Datenschutzbeauftragten umfassen

- die **datenschutzrechtliche Unterrichtung** und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten,
- die **Überwachung der Einhaltung** der datenschutzrechtlichen Vorschriften sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters zum Schutz personenbezogener Daten,
- auf Anfrage die **Beratung hinsichtlich der Datenschutz-Folgenabschätzung** und die Überwachung ihrer Durchführung,
- die **Zusammenarbeit mit der Aufsichtsbehörde**,
- Tätigkeiten als **Anlaufstelle für die Aufsichtsbehörde** in Fragen der Datenverarbeitung und gegebenenfalls Beratung zu allen sonstigen Fragen.

Hinweis

Anders als das bisherige Recht sieht die DSGVO **umfassende Überwachungspflichten** für den Datenschutzbeauftragten vor. Es bleibt daher abzuwarten, ob und in welchem Umfang Gerichte und Behörden Datenschutzbeauftragte künftig als „Überwachergaranten“ im Rahmen einer straf- und ordnungswidrigkeitenrechtlichen Verantwortlichkeit einordnen werden.

4 Besondere Schritte im Umgang mit Daten

4.1 Datenverarbeitung im Auftrag

Entschließt sich ein Unternehmen zum **Outsourcing** einzelner Tätigkeiten (z.B. der Personalbuchhaltung), müssen dabei verschiedene rechtliche, technische und organisatorische **Voraussetzungen** erfüllt werden.

Werden dem Auftragnehmer zu einem solchen Zweck personenbezogene **Daten überlassen**, findet datenschutzrechtlich gesehen **keine Übermittlung** statt, da der Auftragnehmer nicht Dritter ist. Gegenüber Geschäftspartnern und Kunden bleibt das Unternehmen als Auftraggeber der Datenverarbeitung voll dafür verantwortlich, dass mit den personenbezogenen Daten rechtmäßig umgegangen wird.

Der **Auftraggeber** muss

- einen schriftlichen Auftrag erteilen und
- die erforderlichen Maßnahmen zur Datensicherheit vorgeben.

Überdies muss er sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen und das Ergebnis dieser Überprüfung dokumentieren.

Hinweis

Es ist möglich, diese Aufgaben an vertrauenswürdige Dritte (z.B. unabhängige Sachverständige) zu delegieren, welche die Einhaltung der Vorgaben mittels Zertifikat bescheinigen.

Der **Auftragnehmer** darf und muss im Rahmen der Weisungen des Auftraggebers tätig werden.

4.2 Werbung und Adresshandel

Personenbezogene Daten dürfen grundsätzlich **nur mit Einwilligung** des Betroffenen zu Zwecken der Werbung und des Adresshandels weitergegeben werden.

Von diesem Grundsatz gibt es – bezogen auf postalische Direktwerbung – jedoch **zahlreiche Ausnahmen.** So dürfen personenbezogene Daten zu Zwecken der Werbung oder des Adresshandels **ohne Einwilligung** verarbeitet oder genutzt werden, **wenn**

- der Betroffene anhand der Werbung erkennen kann, welches Unternehmen seine Adressdaten hierfür weitergegeben hat, oder
- Unternehmen ihre eigenen Kunden bewerben.

Hinweis

Der Betroffene hat das Recht, der Zusendung einer Werbung zu widersprechen. Auf dieses Recht muss er hingewiesen werden, wenn er Werbung zugesandt bekommt. Der **Widerspruch** kann auch bei den Stellen eingelegt werden, denen die Daten übermittelt worden sind.

4.3 Auskunfteien

Ein Unternehmen darf unter bestimmten Voraussetzungen **geschäftsmäßig** personenbezogene **Daten** erheben und verarbeiten, um diese **Dritten** zu **übermitteln**.

Dies geschieht insbesondere bei Auskunfteien, die anderen Unternehmen **Angaben zur Kreditwürdigkeit** von Privatpersonen verkaufen. Dazu erheben und speichern Auskunfteien Angaben zu vertragsgemäßem wie nicht vertragsgemäßem Verhalten.

Folgende personenbezogene **Daten dürfen** an eine Auskunftei **übermittelt werden**:

- Forderungen, die durch rechtskräftige Urteile festgestellt worden sind,
- Forderungen im Rahmen von Insolvenzverfahren,
- ausdrücklich anerkannte Forderungen,
- jede Art der unbestrittenen Forderung, wenn sie mindestens zweimal schriftlich angemahnt wurde und auf die Einmeldung hingewiesen wurde,
- jede Art von Forderung, die den Vertragspartner zur fristlosen Kündigung berechtigt, wenn vorher über die Einmeldung bei einer Auskunftei informiert wurde.

Zusätzlich dürfen Auskunfteien von Banken und anderen Kreditinstituten **weitere Informationen anfordern** (u.a. Angaben über Girokontenverträge, laufende Kredite, beantragte Hypotheken und andere Bankgeschäfte).

4.4 Videoüberwachung

Da die DSGVO **keine explizite Regelung** zur Videoüberwachung trifft, greift der grundsätzliche Anwendungsvorrang der DSGVO hier nicht. In der Praxis müssen sich Unternehmen **am** beibehaltenen oder neu geregelten **nationalen Datenschutzgesetz und** der **Rechtsprechung orientieren**.

Videoüberwachung ist in Unternehmen weit verbreitet. Primär soll sie dem Schutz von Objekten (u.a. vor Diebstahl) oder Personen dienen. Auch wenn hierbei in den meisten Fällen keine gezielte Beobachtung und Kontrolle der Mitarbeiter beabsichtigt ist, können deren Datenschutz- und Persönlichkeitsrechte von der Videoüberwachung berührt sein.

Beispiel

In Kreditinstituten und Parkhäusern sind ebenso wie in Kassenbereichen von Warenhäusern und Museen häufig Videokameras angebracht, mit denen zwangsläufig auch die dort Beschäftigten überwacht werden.

Die **Zulässigkeit** einer Videoüberwachung von Beschäftigten richtet sich nach **unterschiedlichen Vorschriften** – je nachdem, ob der überwachte Bereich öffentlich zugänglich ist (z.B. Straße, Warenhaus) oder nicht (z.B. Räumlichkeiten des Unternehmens).

Hinweis

Der **Begriff „öffentlich zugänglich“** charakterisiert hier einen Raum, in dem sich jedermann berechtigt aufhalten kann, ohne in irgendwelche Rechtsbeziehungen zum Inhaber des Hausrechts dieses Raums treten zu müssen.

Eine **Videoüberwachung darf grundsätzlich eingesetzt werden** zur Aufgabenerfüllung, zur Wahrnehmung des Hausrechts und zur Wahrnehmung berechtigter Interessen.

Sind aber **Beschäftigte** von der Überwachung **betroffen**, so ist die **Überwachung** nur **eingeschränkt** zulässig. Etwa rechtfertigt allein das Hausrecht nicht die Videoüberwachung von Beschäftigten, da sich diese der Überwachung nicht durch Verlassen der Räumlichkeiten entziehen können. Wenn Beschäftigte von den Überwachungskameras dauerhaft erfasst werden, müssen deshalb **zusätzliche Abwägungskriterien** herangezogen werden.

Beispiel

Erfolgt die Überwachung zur Beobachtung von Besuchern, muss gewährleistet sein, dass sie nicht auch zu **Leistungskontrollen** der miterfassten Beschäftigten verwendet wird.

In jedem Fall ist eine Videoüberwachung durch geeignete Maßnahmen kenntlich zu machen. Diese **Hinweispflicht** schließt heimliche Videoüberwachungen grundsätzlich aus. Dazu hat das Bundesarbeitsgericht (BAG) festgestellt, dass eine **verdeckte Videoüberwachung im öffentlichen Bereich** nur dann zulässig ist, wenn sie das einzige Mittel zur Überführung eines Beschäftigten ist, gegen den der konkrete Verdacht vorliegt, eine Straftat begangen zu haben.

Hinweis

Da die DSGVO keine Unterscheidung zwischen öffentlichem und nicht öffentlichem Raum trifft, ist es denkbar, dass in bestimmten (weiteren) Fällen auch eine verdeckte Überwachung des öffentlichen Raums zulässig sein kann. Davon, dass damit die Kennzeichnungspflicht gänzlich entfallen könnte, kann man nicht ausgehen.

Handelt es sich um einen **nicht öffentlichen Raum**, etwa einen Arbeitsplatz, so richtet sich die **Zulässigkeit** der Videoüberwachung **nach** den **strengeren Vorgaben** des nationalen Beschäftigtendatenschutzes. Bei der Bewertung der Zulässigkeit ist danach eine umfassende Verhältnismäßigkeitsprüfung durchzuführen. Da der Eingriff in die Persönlichkeitsrechte der Betroffenen bei der Videoüberwachung am Arbeitsplatz sehr intensiv ist, ist die Rechtfertigungsschwelle besonders hoch. Aus Sicht des BAG ist eine **Videoüberwachung von Arbeitsplätzen** nur ausnahmsweise durch besondere Sicherheitsinteressen des Arbeitgebers oder zur Aufklärung von Straftaten eines Beschäftigten gerechtfertigt.

Generell ist von den folgenden **Grundsätzen** auszugehen, die sich in der **Rechtsprechung** entwickelt haben:

- Es müssen überwiegende schutzwürdige Interessen des Arbeitgebers vorliegen (z.B. Schutz von Firmeneigentum), die vor Beginn der Videoüberwachung **durch konkrete Anhaltspunkte und Verdachtsmomente belegt** sind (keine vage Vermutung und kein pauschaler Verdacht gegen alle Beschäftigten),
- Die Durchführung der Videoüberwachung erfolgt mittels einer offen sichtbaren Anlage nach vorheriger Information der Belegschaft.
- Der Einsatz von verdeckten Kameras ist nur zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind sowie die verdeckte Videoüberwachung praktisch das einzig verbleibende Mittel darstellt und insgesamt nicht unverhältnismäßig ist.
- Der Betriebsrat oder die Personalvertretung sind involviert worden.
- Es wurde eine strenge, einzelfallbezogene Verhältnismäßigkeitsprüfung durchgeführt.

Die **weitere Verarbeitung oder Nutzung** von Videoaufnahmen ist nur zulässig, soweit sie erforderlich ist. Kontrollfrage: Genügt nicht die einfache Beobachtung? Wenn die durch Videoüberwachung erhobenen Daten einer **bestimmten Person zugeordnet** werden, muss diese Person über die Verarbeitung oder Nutzung benachrichtigt werden. Nur so kann gewährleistet werden, dass sie von der Überwachung und der anschließenden Auswertung Kenntnis erhält und selbst für die Wahrung ihrer Rechte eintreten kann.

Daten, die **nicht mehr** für den angestrebten Zweck der Überwachung **benötigt** werden, müssen **unverzüglich gelöscht** werden. Dasselbe gilt, wenn schutzwürdige Interessen des Betroffenen der weiteren Speicherung entgegenstehen.

5 Die Rechte Betroffener

5.1 Die Regelungen im Detail

5.1.1 Das Recht auf Auskunft

Jeder Betroffene hat das Recht auf Auskunft über die zu seiner Person gespeicherten Daten. Hierzu gehören

- die zur eigenen Person gespeicherten Daten einschließlich der Angabe, woher sie stammen und an wen sie weitergegeben werden, sowie
- die Angabe über den Zweck der Speicherung.

Hinweis

Es empfiehlt sich, die Auskunft schriftlich anzufordern. Zur Legitimation genügt es in der Regel, die Kopie eines Personaldokuments beizulegen.

Ansprechpartner ist die **verantwortliche Stelle**. Außerdem können die Datenschutz-Kontrollinstitutionen weiterhelfen. Grundsätzlich ist die Auskunft kostenfrei.

Auskunfteien und andere Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung speichern, müssen bei Anforderung **einmal im Kalenderjahr kostenlos** Auskunft erteilen. Für jede weitere Auskunft kann jedoch ein Entgelt verlangt werden, wenn die Auskunft gegenüber Dritten wirtschaftlich genutzt werden kann (z.B. zum Nachweis der Bonität). Diese Stellen **müssen auch mitteilen**, woher sie die Daten haben und an wen sie die Daten weitergeben – es sei denn, sie können geltend machen, dass ihr Interesse an der Wahrung des Geschäftsgeheimnisses das Auskunftsinteresse des Betroffenen überwiegt.

Alle **Stellen, die** sogenannte **Scorewerte verwenden**, unterliegen bei Anfrage der **Mitteilungspflicht** darüber, welche Scorewerte zu einer Person gespeichert und an Dritte übermittelt wurden und wie diese Scorewerte zustande gekommen sind. Jeder Scorewert muss dem Betroffenen verständlich, einzelfallbezogen und nachvollziehbar erklärt werden. Die **Geltendmachung** des Auskunftsanspruchs darf sich **nicht negativ** auf den Scorewert des Betroffenen **auswirken**.

Unternehmen dürfen eine **Auskunft** nur in Fällen **ablehnen**, in denen auch keine Benachrichtigungspflicht besteht. Der Betroffene hat grundsätzlich Anspruch auf eine vollständige Auskunft. Alle Angaben, für die nach dem Gesetz grundsätzlich eine Auskunftsverpflichtung besteht, müssen mitgeteilt werden. Wenn die auskunftspflichtige Stelle nicht oder **nur teilweise Auskunft** erteilt, muss sie auf die Unvollständigkeit der Auskunft ausdrücklich hinweisen, damit der Betroffene eine Überprüfung verlangen kann. Im Allgemeinen ist die verantwortliche Stelle auch verpflichtet zu begründen, aufgrund welcher gesetzlichen Bestimmung oder Tatsache sie eine **Auskunft verweigert oder beschränkt**. Eine solche Begründung ist nur entbehrlich, wenn sonst der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.

Hinweis

Bei Zweifeln an der Korrektheit einer Auskunft hat der Betroffene die Möglichkeit, sich an die zuständige Datenschutz-Kontrollinstitution zu wenden oder eine gerichtliche Klage einzureichen.

Also Achtung, denn wie mittlerweile gerichtlich bestätigt wurde, sind unterlassene oder nicht vollständige Auskunftserteilungen mit einer hohen Geldbuße bedroht.

5.1.2 Das Recht auf Einsicht

Unternehmen haben eine **Übersicht** über ihre automatisierten Verarbeitungen personenbezogener Daten zu führen. Diese Übersicht kann von jedermann **unentgeltlich eingesehen** werden.

Hinweis

Es ist Aufgabe des Datenschutzbeauftragten, die Angaben in diesem Verfahrensverzeichnis etwaigen Antragstellern in geeigneter Weise verfügbar zu machen.

Diese Regelung gilt entsprechend **auch** für **Unternehmen ohne betrieblichen Datenschutzbeauftragten**.

Bis auf die allgemeine Beschreibung, die es ermöglicht, die Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu beurteilen, sind **alle Angaben öffentlich**. Es geht dabei vor allem um folgende Angaben:

- Name oder Firma der verantwortlichen Stelle,
- Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
- Anschrift der verantwortlichen Stelle,
- Zwecke der Erhebung, Verarbeitung und Nutzung der Daten,
- Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten,
- Empfänger der Daten,
- Regelfristen für die Löschung der Daten,
- etwaige geplante Datenübermittlung in Drittstaaten.

5.1.3 Das Recht auf Benachrichtigung

Jede verantwortliche Stelle ist verpflichtet, alle Betroffenen individuell zu benachrichtigen, über die sie **Daten ohne deren Kenntnis erhoben** hat und deren Daten sie speichern oder verarbeiten möchte. Unternehmen müssen Betroffene bereits bei der ersten Datenspeicherung informieren. Die Benachrichtigung muss umfassen:

- Kontaktdaten des Verantwortlichen und seines Datenschutzbeauftragten,
- Zwecke der Datenverarbeitung, gegebenenfalls berechtigte Interessen des Verantwortlichen oder eines Dritten an der Datenverarbeitung,
- Empfänger oder Kategorien von Empfängern personenbezogener Daten,
- Meldung der Übermittlung von Daten in ein Drittland,
- Speicherdauer,
- Auskunftsrechte, Rechte auf Berichtigung, Löschung, Einschränkung, Widerspruch und Datenübertragbarkeit sowie Beschwerderechte bei Aufsichtsbehörden.

Hinweis

In bestimmten gesetzlich geregelten Fällen muss **keine Benachrichtigung** erfolgen, zum Beispiel bei Bestehen einer überwiegenden Geheimhaltungspflicht oder wenn der Betroffene bereits Kenntnis besitzt.

5.1.4 Das Recht auf Berichtigung

Unternehmen sind verpflichtet, unrichtige Daten zu berichtigen. Es liegt aber auch am Betroffenen selbst, darauf hinzuweisen, wenn Daten unrichtig oder überholt sind. Geschätzte Daten müssen als solche deutlich gekennzeichnet werden.

5.1.5 Das Recht auf Löschung

Daten sind von Unternehmen zu löschen, wenn

- die **Speicherung unzulässig** ist,
- die erteilte **Einwilligung** zur Datenspeicherung **widerrufen** wurde,
- es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit, das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre **Richtigkeit** von der verantwortlichen Stelle **nicht bewiesen** werden kann,
- für eigene Zwecke verarbeitete Daten **für** die Erfüllung des **Speicherungszwecks nicht mehr erforderlich** sind oder
- geschäftsmäßig zum Zweck der Übermittlung verarbeitete Daten **aufgrund** einer am Ende des vierten Kalenderjahres nach der ersten Speicherung vorzunehmenden **Prüfung nicht mehr erforderlich** sind; soweit es sich um Daten über erledigte Sachverhalte handelt, muss bereits zum Ende des dritten Kalenderjahres nach der ersten Speicherung die Löschverpflichtung überprüft werden.

Eine **Löschung** ist **nur vorgesehen für** personenbezogene Daten, die entweder aus automatisierter Datenverarbeitung oder aus einer manuellen, also ohne Automationsunterstützung geführten Datei stammen. Sie ist **nicht vorgesehen für** einzelne Daten, die in nicht dateimäßig strukturierten Akten festgehalten sind.

Hinweis

Sind allerdings komplette Akten unzulässig angelegt, so sind sie ebenfalls zu vernichten. Ebenso ist im Allgemeinen mit nicht mehr erforderlichen Akten zu verfahren.

Als besondere Ausformung des Löschungsanspruchs wurde mit der DSGVO ein **„Recht auf Vergessenwerden“** eingeführt. Dieses Recht greift, wenn die verantwortliche Stelle die zu löschenden Daten öffentlich gemacht hat (z.B. im Internet). Dann muss sie vertretbare Schritte unternehmen, um die Stellen, die diese Daten verarbeiten, darüber zu informieren, dass die betroffene Person von ihnen die Löschung aller Links zu diesen Daten oder die Löschung aller Kopien oder Replikationen dieser Daten verlangt.

Hinweis

Unternehmen sollten die **veränderten Anforderungen** bei den Löschpflichten in ihren Löschkonzepten **präzise abbilden**, um nachweisen zu können, dass sie die Vorgaben der DSGVO einhalten.

5.1.6 Das Recht auf Sperrung

Personenbezogene Daten sind immer dann zu sperren, wenn einer fälligen Löschung besondere Gründe entgegenstehen.

Derartige besondere Gründe sind unter anderem

- gesetzlich, satzungsmäßig oder vertraglich festgelegte **Aufbewahrungsfristen**,
- **schutzwürdige Interessen** des Betroffenen, etwa wenn ihm Beweismittel verlorengingen, und
- ein **unverhältnismäßig hoher Aufwand** wegen der besonderen Art der Speicherung.

Personenbezogene **Daten** sind zu **sperren**, **wenn** der Betroffene ihre Richtigkeit bestreitet und **sich weder** deren **Richtigkeit noch** deren **Unrichtigkeit feststellen lässt**. Die Tatsache dieser Sperrung darf dann ebenfalls nicht übermittelt werden.

Gesperrte Daten dürfen **ohne Einwilligung** des Betroffenen **nur übermittelt** oder genutzt werden, **wenn** es

- zu wissenschaftlichen Zwecken,
- zur Behebung einer bestehenden Beweisnot oder
- aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen

unerlässlich ist. Zudem schreibt das Gesetz vor, dass gesperrte Daten nur ausnahmsweise und nur dann für die genannten Zwecke übermittelt oder genutzt werden dürfen, wenn dies auch ohne Sperrung erlaubt wäre.

5.2 Das allgemeine Widerspruchsrecht

Betroffene haben das Recht, unter bestimmten Voraussetzungen **sogar** einer **rechtmäßigen Datenverarbeitung** zu widersprechen. Begründet ist dies, sofern

- besondere Umstände in der Person des Betroffenen vorliegen und deswegen
- das schutzwürdige Interesse des Betroffenen das Interesse der verantwortlichen Stelle an der Erhebung, Verarbeitung oder Nutzung der entsprechenden personenbezogenen Daten überwiegt.

Das **Widerspruchsrecht besteht nicht, wenn** eine Rechtsvorschrift die Erhebung, Verarbeitung oder Nutzung vorschreibt. Es kann für den Betroffenen **dennoch sinnvoll** sein, **Widerspruch einzulegen**, um die eigenen berechtigten Interessen geltend zu machen. Die verantwortliche Stelle hat den Widerspruch in den Abwägungsprozess einzubeziehen.

5.3 Einschränkung der Betroffenenrechte

Sämtliche Betroffenenrechte können **durch nationale Gesetze** beschränkt werden, wenn dies zur Wahrung bestimmter öffentlicher Interessen erforderlich ist. Dabei sind der Verhältnismäßigkeitsgrundsatz und der Wesensgehalt der Grundrechte zu beachten. Der Bundesgesetzgeber hat von dieser Möglichkeit Gebrauch gemacht und **im novellierten BDSG Einschränkungen der Betroffenenrechte** vorgesehen.

6 Die Folgen einer Datenschutzverletzung

6.1 Meldepflicht

Verletzungen des Schutzes personenbezogener Daten müssen unverzüglich, nach Möglichkeit innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls, an die zuständige Aufsichtsbehörde **gemeldet werden**. Eine **Ausnahme** besteht, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen führt (etwa aufgrund einer geeigneten Verschlüsselung).

Stellt die Verletzung des Schutzes personenbezogener Daten ein **hohes Risiko** für die persönlichen Rechte und Freiheiten dar, muss der Verantwortliche **auch die betroffene Person** ohne unangemessene Verzögerung **benachrichtigen** – es sei denn, er hat technisch-organisatorische Maßnahmen getroffen, die eine Kenntnisnahme durch Dritte verhindern oder sicherstellen, dass aller Wahrscheinlichkeit nach kein hohes Risiko mehr für die Rechte und Freiheiten der betroffenen Person besteht.

Hinweis

Fehler bei der Umsetzung der Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen werden mit Bußgeldern von bis zu 2 % des Umsatzes geahndet.

6.2 Rechtliche Konsequenzen

Verstöße gegen den Datenschutz können ernsthafte rechtliche Folgen haben. Die DSGVO hat die bisher geltenden **Regelungen deutlich verschärft**, und zwar sowohl im Hinblick auf Geldbußen als auch im Hinblick auf Schadenersatz einschließlich Schmerzensgeld.

Hinweis

Bereits kurz nach Inkrafttreten der DSGVO kam es zu ersten Abmahnungen mit der Vorlage von Unterlassungserklärungen wegen Datenschutzverletzungen. Es bleibt jedoch abzuwarten, wie deutsche Gerichte damit umgehen. In jedem Fall sollten betroffene Unternehmen eine Abmahnung ernst nehmen und die oftmals nachteilig vorformulierten Unterlassungserklärungen wie auch die zugleich geforderten Rechtsanwaltskosten überprüfen lassen.

6.2.1 Bußgeld

Die DSGVO sieht eine maximale Geldbuße von bis zu **20 Mio. € oder 4 % des gesamten** weltweit erzielten **Jahresumsatzes** im vorangegangenen Geschäftsjahr vor (je nachdem, welcher Wert der höhere ist). Es gilt der Jahresumsatz des gesamten Unternehmens, nicht der der einzelnen juristischen Person. Für die **Bemessung des Bußgelds** steht ein Katalog mit Kriterien zur Verfügung. Entscheidend sind:

- Art, Schwere und Dauer des Verstoßes,
- Vorsätzlichkeit oder Fahrlässigkeit,
- die vorgenommenen Maßnahmen zur Minderung des entstandenen Schadens,
- der Verantwortungsgrad unter Berücksichtigung aller getroffenen Maßnahmen,
- etwaige einschlägige frühere Verstöße,
- der Umfang der Zusammenarbeit mit der Aufsichtsbehörde,
- die Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind,
- die Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere Selbstanzeige,
- die Einhaltung früher angeordneter Maßnahmen,
- die Einhaltung genehmigter Verhaltensregeln und
- alle anderen Umstände des Einzelfalls (u.a. finanzielle Vorteile).

6.2.2 Schadenersatz

Wenn eine verantwortliche Stelle einem Betroffenen durch eine unzulässige oder unrichtige Datenverarbeitung einen Schaden zufügt, besteht eine **Schadenersatzpflicht** und in schweren Fällen auch ein Anspruch auf **Schmerzensgeld**. Zudem sind die zivilrechtlichen **Haftungsrisiken** wegen Datenschutzverstößen für Unternehmen durch die DSGVO **gestiegen**. So sind nunmehr materielle und immaterielle Schäden zu erstatten, die auf Verstößen gegen die Verordnung beruhen. Die ausdrückliche Nennung **immaterieller Schäden** wird in der Praxis zu einer **erheblichen Veränderung** gegenüber **der bisherigen Rechtslage** führen. Eine weitere Neuerung ist die ausdrückliche **Erweiterung** der Haftung auch **auf Auftragsverarbeiter**.

Hinweis

Eine Exkulpierung ist nur möglich, wenn durch einen Dienstleister nachgewiesen werden kann, dass das Unternehmen für den Verstoß nicht verantwortlich ist.

Gerade vor dem Hintergrund der erweiterten Haftung ist es für Unternehmen und Auftragsverarbeiter umso wichtiger, Datenschutzmaßnahmen umfassend zu dokumentieren. Nur so können sich Unternehmen angesichts der massiv erweiterten Beweislast nach der DSGVO effektiv **gegen Schadenersatzforderungen verteidigen**.

7 Muster und Checklisten

7.1 Muster einer Einwilligungserklärung von Kunden

Unser Unternehmen nimmt den Schutz der Kundendaten ernst. Der Schutz der individuellen Privatsphäre bei der Verarbeitung personenbezogener Daten ist für uns ein wichtiges Anliegen, das wir bei unseren Geschäftsprozessen mit hoher Aufmerksamkeit berücksichtigen.

A.

Datenverarbeitung zur Vertragsabwicklung

Die Verarbeitung der von Ihnen angegebenen personenbezogenen Daten durch uns (oder einen von uns beauftragten Dienstleister) ist zur ordnungsgemäßen Abwicklung des zugrundeliegenden Vertragsverhältnisses, und soweit wir zu deren Erhebung gesetzlich verpflichtet sind, erforderlich.

Die Daten werden gelöscht, sobald sie für die vorgenannten Zwecke nicht mehr erforderlich sind.

Eine darüber hinausgehende, unter Abschnitt B. beschriebene Verarbeitung Ihrer personenbezogenen Daten erfolgt nur mit Ihrer freiwilligen Einwilligung.

B.

Einwilligung in die Datenverarbeitung

[ ] Ja, ich bin damit einverstanden, dass das Unternehmen *[Platzhalter]* (ggf. unter Einschaltung eines beauftragten Dienstleisters) meine personenbezogenen Daten zum Zweck der Erfüllung der zwischen uns bestehenden vertraglichen Verpflichtungen bis auf Widerruf verwendet.

Zu den konkreten Verwendungszwecken meiner personenbezogenen Daten möchte ich per

[ ] Post,

[ ] E-Mail,

[ ] Telefon,

[ ] Fax,

[ ] SMS

kontaktiert zu werden (Zutreffendes bitte ankreuzen; Mehrfachnennungen sind möglich).

Mir ist bewusst, dass diese Einwilligung freiwillig erfolgt und jederzeit widerruflich ist. Meine in Abschnitt C. dargestellten Datenschutzrechte habe ich zur Kenntnis genommen.

_____

(Ort, Datum, Unterschrift des Kunden)

C.

Datenschutzrechte des Kunden und Kontaktdaten

Sie können von uns jederzeit Auskunft über Ihre gespeicherten personenbezogenen Daten erhalten, deren Berichtigung, Löschung oder Einschränkung der Verarbeitung verlangen sowie Ihr Recht auf Datenübertragbarkeit geltend machen.

Außerdem können Sie Ihre Einwilligungserklärung jederzeit ohne Angabe von Gründen mit Wirkung für die Zukunft ändern oder widerrufen. Bitte beachten Sie, dass Datenverarbeitungen, die vor dem Widerruf erfolgt sind, hiervon nicht betroffen sind.

Zu den vorgenannten Zwecken wenden Sie sich bitte an eine der nachfolgenden Kontaktadressen.

Sie erreichen unseren Datenschutzbeauftragten unter:

Musterunternehmen, Musterstraße 1, 12345 Musterstadt, Tel.: 0123/5678, E-Mail: datenschutz@musterunternehmen.de

Für die Datenverarbeitung verantwortlich:

Musterunternehmen, Geschäftsführer: Max Mustermann, Musterstraße 1, 12345 Musterstadt, Tel.: 01234/56789, E-Mail: Mustermann@musterunternehmen.de

Ihnen steht des Weiteren ein Beschwerderecht bei einer Aufsichtsbehörde zu.

Das Original dieser Erklärung verbleibt beim Unternehmen *[Platzhalter]*. Als Kunde erhalten Sie eine Kopie.

7.2 Datenschutz-Checkliste für KMU

Die DSGVO betrifft maßgeblich auch kleine und mittlere Unternehmen (KMU), denn bei groben Verstößen droht die persönliche Haftung der Geschäftsführer, was die Vornahme von Schutzmaßnahmen daher zwingend erforderlich macht. Die folgende Checkliste informiert KMU-Geschäftsführer, damit sie ihre Organisation und Prozesse an die neue Rechtslage anpassen können.

Hinweis

Die Checkliste ersetzt nicht die individuelle Beratung. Kommen Sie im Zweifel gerne jederzeit auf uns zu.

Maßnahmen	Umgesetzt	
	Ja	Nein
Sie haben in Ihrem Unternehmen geregelt, wer für Datenschutzthemen zuständig ist, bzw. Sie haben einen **Datenschutzbeauftragten** bestellt?		
Sie haben Ihren **Datenschutzbeauftragten** (falls vorhanden) mit den entsprechenden Kontaktdaten an die Aufsichtsbehörde **gemeldet**?		
Sie haben sich und Ihre **Mitarbeiter** über die neuen Datenschutzregelungen **informiert** oder geschult?		
Sie haben sämtliche Geschäftsabläufe, bei denen personenbezogene Daten wie • Mandantendaten, • Beschäftigtendaten und • Daten über Dritte (Geschäftspartner, Auftragsverarbeiter etc.) verarbeitet werden, in ein **Verzeichnis von Verarbeitungstätigkeiten** aufgenommen?		
In Ihrem Unternehmen existiert eine klare Zuständigkeit für die Erstellung und **regelmäßige Aktualisierung des Verarbeitungsverzeichnisses**?		
Sie können für alle Verarbeitungen in Ihrem Unternehmen eine dokumentierte **Rechtsgrundlage oder** eine **schriftliche Einwilligung** der Betroffenen vorweisen?		
Sie haben Ihre **Muster für Einwilligungserklärungen** für Mandanten, Mitarbeiter und andere an die Anforderungen der DSGVO im Hinblick auf • Freiwilligkeit, • Informiertheit, • Ausdrücklichkeit und • Widerrufbarkeit (für die Zukunft) angepasst?		
Sie haben die **datenschutzkonforme Information** von Mandanten, Mitarbeitern und anderen durch Zuständigkeiten und festgelegte Abläufe sichergestellt?		
Sie haben die **weiteren Rechte der betroffenen Personen** wie • das Recht auf Benachrichtigung, • das Recht auf Auskunft, • das Recht auf Einsichtnahme, • das Recht auf Berichtigung, • das Recht auf fristgemäße Löschung der verarbeiteten Daten, • das Recht auf Einschränkung der Verarbeitung (Sperrung), • das Recht auf Datenübertragbarkeit, • das Recht auf Widerspruch der Datenverarbeitung und • das Recht, keiner automatisierten Entscheidung unterworfen zu werden, sichergestellt?		
Sie oder Ihre Dienstleister setzen **technische und organisatorische Maßnahmen** (TOM) wie • Vorgaben für die physikalische Sicherheit und Zugangskontrolle (Einbruchs-, Alarm- und Brandmelder, gesicherte Stromversorgung, kontrollierter Personenzugang, sichere Aufbewahrung von Dokumenten, stabile Telekommunikation), • die Verwendung und Überwachung eines aktuellen Betriebssystems auf dem Server, • die Beachtung von Sicherheitsstandards (u.a. ausreichende Länge und Unterschiedlichkeit von Passwörtern, Änderung der Passwörter alle 90 Tage, aktueller Virenscanner, keine Anschlussmöglichkeit für USB-Geräte, Nutzerabmeldung bei Nichtnutzung des PC bzw. Laptops, fachgerechte Entsorgung von Altgeräten nach vorheriger Datenlöschung), • die passwortgeschützte Nutzung aktueller Software, • die Nutzung einer aktuellen Firewall, • regelmäßige Backups, • Pseudonymisierungsverfahren, • Anonymisierungsverfahren, • Verschlüsselungsverfahren, • Verhaltensvorschriften für Mitarbeiter im Umgang mit Anhängen und Links in E-Mails sowie auch mit den eigenen Zugangsdaten und für die Nutzung des Internets sowie von Browsern und • das Vorhalten eines Notfallplans (mit Dokumentation aller Maßnahmen und Passwörter, Ansprechpartner und Adressen) ein, um ein angemessenes Schutzniveau zu gewährleisten?		
Sie haben sichergestellt, dass in Ihrem Unternehmen **Datenschutzanforderungen** bei jedem Geschäftsvorfall **von Anfang an mit berücksichtigt** werden?		

Sie haben Ihre bestehenden **Verträge mit Auftragsverarbeitern**, das heißt mit Unternehmen, die in Ihrem Auftrag personenbezogene Daten verarbeiten, hinsichtlich folgender Kriterien überprüft: • Vorliegen eines Vertrages, • Gegenstand und Dauer des Auftrags, • Art und Zweck der Datenverarbeitung, • Kategorien betroffener Personen, • Einhaltung der TOM im Sinne der DSGVO, • Rechte des Verantwortlichen (Kontrollen) und • Weisungsbefugnisse des Verantwortlichen.		
Sie haben in Ihrem Unternehmen einen Prozess und die Zuständigkeit für die **Meldung von Datenschutzverstößen** binnen 72 Stunden an die Aufsichtsbehörde geregelt?		
Sie erfüllen nachweislich Ihre **Dokumentationspflichten** im Hinblick auf die Einhaltung aller hier aufgeführten Pflichten und Anforderungen?		
Sie haben sichergestellt, dass sich Ihre **datenschutzrechtliche Dokumentation** aller Maßnahmen und Prozesse in Ihrem Unternehmen immer auf dem neuesten Stand befindet (**Überprüfungszyklus**)?		

Wir stehen Ihnen gerne für weitere Fragen zur Verfügung.

Rechtsstand: September 2018

Alle Informationen und Angaben in diesem Mandanten-Merkblatt haben wir nach bestem Wissen zusammengestellt. Sie erfolgen jedoch ohne Gewähr. Diese Information kann eine individuelle Beratung im Einzelfall nicht ersetzen.