DER MITTELSTANDSVERBUND ZGV

DATENSCHUTZGRUNDVERORDNUNG

Praxis-Leitfaden
für
Verbundgruppen und Anschlusshäuser

Version 1.0

Herausgeber:
DER MITTELSTANDSVERBUND – ZGV e.V.
Am Weidendamm 1a
10117 Berlin

Ansprechpartner:
RA Dr. Marc Zgaga, m.zgaga@mittelstandsverbund.de
RA Tim Geier, t.geier@mittelstandsverbund.de

Vorwort

Am 25.05.2018 endet die Übergangsfrist zur Umsetzung des neuen, europaweit und unmittelbar geltenden Datenschutzrechts. Bis dahin muss jedes Unternehmen die Vorgaben der sogenannten EU-Datenschutzgrundverordnung (im Folgenden „DSGVO“) und des neuen Bundesdatenschutzgesetzes (im Folgenden „BDSG neu“) umgesetzt und in den Unternehmensalltag integriert haben.

Die umfangreichen Vorschriften der DSGVO und des BDSG neu bereiten aber gerade kleinen und mittleren Unternehmen Schwierigkeiten:

- „Wo fängt man sinnvollerweise mit der Umsetzung an?“
- „Welche Bereiche und Prozesse im Unternehmen sind überhaupt betroffen?“
- „Muss ich nun einen Datenschutzbeauftragten bestellen?“
- „Wie sieht ein DSGVO-konformes Datenschutzmanagement aus?“

Mit diesen und weiteren Fragen sehen sich mittelständische Unternehmen aktuell konfrontiert.

Vor diesem Hintergrund hat DER MITTELSTANDSVERBUND diesen Praxis-Leitfaden speziell für Verbundgruppen und deren Anschlusshäuser aus Handel, Handwerk und Dienstleistungsgewerbe erarbeitet, um den Einstieg in die Planung zur Umsetzung der DSGVO zu erleichtern und auf die wesentlichen Veränderungen und Neuerungen aufmerksam zu machen. Denn auch wenn die Herausforderungen nicht gering sind, ist es unumgänglich, die unternehmenseigene Datenschutzpraxis zu überprüfen und das Datenschutzmanagement bis zum Stichtag 25.05.2018 nach den Vorgaben der DSGVO anzupassen bzw. weiterzuentwickeln.

Neben diesem Praxis-Leitfaden bietet DER MITTELSTANDSVERBUND seinen Mitgliedern und deren Anschlusshäusern weitere Unterstützungsleistungen im Zusammenhang mit der Umsetzung der DSGVO an, darunter (Inhouse-)Schulungs-Veranstaltungen, Webinare und individuelle Beratung. Sprechen Sie uns an.

RA Dr. Marc Zgaga / RA Tim Geier, DER MITTELSTANDSVERBUND

Berlin/Brüssel, Dezember 2017

Inhaltsverzeichnis

1. Einführung

Das europäische Datenschutzrecht blickt auf eine mehr als zwanzigjährige Geschichte zurück. Den Ursprung dabei bildete die EG-Datenschutzrichtlinie 94/46/EG aus dem Jahr 1995. Als Richtlinie galt dieser Rechtstext allerdings nicht unmittelbar, sondern erforderte zunächst die gesetzgeberische Umsetzung in nationales Recht durch die EU-Mitgliedsstaaten.

Eine uneinheitliche Umsetzung sowie unterschiedliche mitgliedstaatliche Auslegungspraxis der Datenschutzrichtlinie, insbesondere aber die konventionelle Nutzung des Internets durch breite Bevölkerungsschichten und die Wirtschaft (Stichworte „Datenverarbeitung in der Cloud“, „Big Data“, „Smart Home“, „Internet of Things“) erzeugten in den Folgejahren einen steigenden Reformdruck und führten schließlich zur Unterbreitung des ersten Entwurfs der Kommission für ein harmonisiertes europäisches Datenschutzrecht. Am 14.04.2016 verabschiedete das Europaparlament die EU-Datenschutzgrundverordnung - kurz DSGVO. Sie besteht aus 99 Artikeln und annähernd doppelt so vielen Erwägungsgründen, die der weiteren Erläuterung der Verordnungstexte dienen.

Für die Umsetzung der DSGVO ist eine zweijährige Übergangsfrist vorgesehen. Dieser Zeitraum dient den nationalen Gesetzgebern dazu, die bisher geltenden Gesetze, wie z.B. das Bundesdatenschutzgesetz in Deutschland, anzupassen.

Als wesentliche Ziele nennt die DSGVO zum einen den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und hier insbesondere deren Recht auf Schutz personenbezogener Daten, zum anderen die Aufrechterhaltung des freien Verkehrs personenbezogener Daten, der weder eingeschränkt oder verboten werden darf.

2. Normenhierarchie des Datenschutzrechts

Mit Veröffentlichung der DSGVO im Amtsblatt der EU hat sich die Normenhierarchie des Datenschutzrechtes in Europa - und damit auch in Deutschland - grundlegend verändert. Die Regeln der DSGVO werden am 25.05.2018 in Kraft treten. Die DSGVO als europäische Verordnung wird dabei unmittelbar in jedem Mitgliedstaat anwendbar sein und einen großen Teil der Regelungen des bislang geltenden Datenschutzrechtes ablösen. In Deutschland betrifft dies insbesondere das bislang geltende Bundesdatenschutzgesetz (BDSG alt).

Gleichzeitig mit In-Kraft-Treten der Regeln der DSGVO wird ein neues Bundesdatenschutzgesetz (BDSG neu) seine Wirkung entfalten. Diese Parallelität von europäischen und nationalen Vorschriften erschwert die praktische Anwendung des Datenschutzrechtes nicht unerheblich, ist aber den umfangreichen Öffnungsklauseln der DSGVO geschuldet. In vielen Bereichen hat der Europäische Gesetzgeber den EU-Mitgliedstaaten nämlich einen Entscheidungsspielraum überlassen. Von diesem Entscheidungsspielraum hat auch der deutsche Gesetzgeber an verschiedenen Stellen Gebrauch gemacht und dies in Form des BDSG neu konkretisiert.

Die Datenschutzgesetze der Länder stellen besondere Regeln der Datenverarbeitung öffentlicher Stellen auf. Auch hier wird es aufgrund des umfangreichen Regelungsbereichs der DSGVO zu Anpassungen kommen.

3. Aufbau der DSGVO und Funktion der Erwägungsgründe

Die DSGVO wird künftig durch 99 Artikel sowie - diesen vorangestellt - sog. Erwägungsgründen geregelt. Untergliedert wird die DSGVO in 11 Kapitel:

Kapitel I - Allgemeine Bestimmungen: Gegenstand und Ziele der DSGVO, sachlicher und räumlicher Anwendungsbereich, Begriffsbestimmungen

Kapitel II - Grundsätze: Grundsätze der Datenverarbeitung, gesetzliche Erlaubnis, Tatbestände und Einwilligung, Besonderheiten bei der Verarbeitung von besonderen Kategorien personenbezogener Daten

Kapitel III - Betroffenenrechte: Allgemeine Anforderungen im Rahmen der Betroffenenrechte, Informationspflichten, Auskunftsrechte, Recht auf Berichtigung, Löschung und Einschränkungen der Datenverarbeitung, Recht auf Datenübertragbarkeit, Widerspruchsrecht, Rechte bei Maßnahmen der Profilbildung

Kapitel IV - Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter: Pflichten des für die Verarbeitung Verantwortlichen, Datenschutz durch Technik, gemeinsam Verantwortliche, Auftragsdatenverarbeitung, Verzeichnis von Verarbeitungstätigkeiten, Datensicherheit, Meldepflichten bei Datenschutzverletzungen, Datenschutz-Folgenabschätzung, Datenschutzbeauftragter, Verhaltensregeln und Zertifizierungen

Kapitel V - Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen

Kapitel VI - Unabhängigkeit der Aufsichtsbehörden

Kapitel VII - Zusammenarbeit und Kohärenz

Kapitel VIII - Rechtsbehelfe, Haftung und Sanktionen: Recht auf Beschwerde und gerichtlichen Rechtsbehelf, Schadenersatz, Geldbußen, Sanktionen

Kapitel IX - Vorschriften für besondere Datenverarbeitungssituationen: Freiheit der Meinungsäußerung und Informationsfreiheit, Zugang zu amtlichen Dokumenten, Beschäftigtendatenschutz, Wissenschaft, Forschung und Archivzwecke, Kirchendatenschutz

Kapitel X - Delegierte Rechtsakte und Durchführungsrechtsakte

Kapitel XI - Schlussbestimmungen

Den Artikeln der DSGVO sind sog. Erwägungsgründe vorangestellt. Diese haben die Funktion einer amtlichen Kommentierungs- oder Auslegungshilfe. Sie sollen dem Anwender die wichtigsten Artikel in kurzer und knapper Form beschreiben und die darin befindlichen Inhalte begründen und lassen Rückschlüsse auf die hinter den einzelnen Artikeln stehenden Motive des Verordnungs-Gesetzgebers zu. Zum besseren Verständnis einzelner DSGVO-Artikel ist es deshalb geboten, die Gesetzesauslegung in Ansehung der jeweils korrelierenden Erwägungsgründe der DSGVO vorzunehmen. Unmittelbare Rechtsfolgen können allerdings aus Erwägungsgründen in der Regel nicht abgeleitet werden.

4. Zeitlicher Anwendungsbereich

Die DSGVO ist bereits am 25.05.2016, zwanzig Tage nach der Veröffentlichung im EU-Amtsblatt, in Kraft getreten. Nach der darin geregelten Übergangsfrist kommt sie allerdings erst zwei Jahre nach Inkrafttreten zur Anwendung. Das bedeutet, dass die Datenschutzgrundverordnung ab dem 25.05.2018 für alle gilt und deren Einhaltung durch die EU-Datenschutzaufsichts-behörden und Gerichte überprüfbar ist. Zu diesem Datum wird die DSGVO auch die bisherige Datenschutzrichtlinie und die nationalen Vorschriften der Mitgliedsstaaten in weiten Teilen ablösen und ersetzen, um dann europaweit unmittelbar und verbindlich zu gelten.

Die noch verbleibende Übergangsfrist bis zur Geltung der DSGVO sollte von Unternehmen dringend zur Anpassung der internen Workflows und Prozesse genutzt werden, da EU-Datenschutzbehörden ab Geltung im Mai 2018 Sanktionen verhängen können, wenn die Vorgaben der DSGVO nicht oder nicht ausreichend umgesetzt wurden.

5. Sachlicher Anwendungsbereich

Die DSGVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

„Personenbezogene Daten“ in diesem Sinne sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. „Verarbeitung“ meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Erfolgt die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und damit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit, findet die DSGVO keine Anwendung.

6. Grundbegriffe der DSGVO

Mit Einführung der DSGVO werden Unternehmen mit einer Vielzahl neuer Begriffe konfrontiert werden. Zum weiteren Verständnis sollen an dieser Stelle die wichtigsten Begrifflichkeiten kurz beschrieben werden.

a. Personenbezogene Daten

Kernbegriff der DSGVO sowie des gesamten Datenschutzrechts ist der Begriff der personenbezogenen Daten. Dies sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (sogenannte „betroffene Person“) be-

ziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung, wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann.

Praktisch gilt danach, dass alle Informationen, über die irgendwie ein Personenbezug hergestellt werden kann, auch unter den Begriff der personenbezogenen Daten und damit in den Schutzbereich der DSGVO fallen.

Bsp.: Name, Anschrift, Telefonnummer, Kreditkarten- oder Personalnummer, Kontodaten, Kfz-Kennzeichen, Aussehen, Kundennummer.

Achtung: Auch dynamische IP-Adressen und Standortdaten werden regelmäßig als personenbezogene Daten angesehen.

Die Grundsätze des Datenschutzes gelten dagegen nicht für anonyme Informationen. Dies sind Daten, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.

Achtung: Werden Daten zwar anonymisiert, kann diese Anonymisierung jedoch wieder rückgängig gemacht werden, handelt es sich dennoch um personenbezogene Daten und der Schutzbereich der DSGVO ist eröffnet.

b. Besondere Kategorien personenbezogener Daten

Als besondere Kategorien von Daten, oder sensible Daten nach Art. 9 Abs. 1 DSGVO werden Daten bezeichnet, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Bsp.: Jegliche Daten zum Gesundheitszustand einer Person, Fingerabdruck, Irisscan, DNS-Analyse, Krankenakte.

Im Falle der Verarbeitung derartiger besonderer Kategorien personenbezogener Daten hält die DSGVO besondere Prozess- und Informationspflichten bereit (auf diese wird im Folgenden jeweils explizit hingewiesen).

c. Pseudonymisierung

Unter Pseudonymisierung versteht man die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natür-

lichen Person zugewiesen werden. Das Verfahren der Pseudonymisierung wird damit in der DSGVO als Maßnahme des technisch-organisatorischen Datenschutzes weitergeführt.

Achtung: Die Pseudonymisierung kann mithin die Risiken einer Datenverarbeitung senken. Hingegen entbindet sie nicht von den Pflichten der DSGVO. Auch pseudonymisierte Daten unterfallen dem Schutzbereich der DSGVO.

d. Verarbeitung

Der Verarbeitungsbegriff der DSGVO meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Umfasst ist mithin grundsätzlich jeder Verarbeitungsvorgang im Zusammenhang mit personenbezogenen Daten einschließlich deren Erhebung.

Bsp.: Erstellung einer Kundendatei, Aufnahme der Daten zur Erstellung einer Rechnung, Mitarbeiterdatenbank, Marketingaktion, Loyalty-Systeme.

e. Verantwortlicher

Zentraler Adressat der materiellen Regelungen der DSGVO ist der „Verantwortliche“, mithin die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

f. Auftragsverarbeiter

Auftragsverarbeiter (nach früherem Recht „Auftragsdatenverarbeiter“) ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet.

Bsp.: Unternehmer, der Kundendaten zur Erstellung einer Rechnung an den Kunden erfasst, ist „Verantwortlicher“. Der externe Buchhalter, der die Rechnungsdaten zur Bilanzierung erhält und verarbeitet, ist Auftragsverarbeiter.

7. Grundprinzipien der DSGVO

In Art. 5 DSGVO legt der europäische Gesetzgeber allgemein gültige Grundprinzipien für die Verarbeitung personenbezogener Daten fest, die von zentraler Bedeutung sind. Diese Grundprinzipien der Datenverarbeitung muss jeder Verantwortliche einhalten und die Einhaltung im Fall der Fälle auch nachweisen können.

Zwar bleiben viele Grundsätze des bisherigen deutschen Datenschutzrechtes bestehen; diese werden jedoch in vielerlei Hinsicht durch die DSGVO in ihrem Anwendungsbereich erweitert.

Die Grundprinzipien erscheinen zunächst sehr theoretisch, bringen aber für die praktische Anwendung der DSGVO im Unternehmen einen nicht zu unterschätzenden Nutzen. Aufgestellt werden durch die Grundprinzipien sowohl Anforderungen an die Datenqualität, als auch an zu implementierende Verfahren und Prozesse.

Die nachfolgende Auflistung stellt die wichtigsten Grundprinzipien der DSGVO dar.

a. Rechtmäßigkeit

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn sie rechtmäßig ist. Dieser fast schon profane Grundsatz scheint offensichtlich, zwingt den Verarbeiter personenbezogener Daten jedoch immer wieder, die Grundlage der individuellen Datenverarbeitung zu hinterfragen.

b. Treu und Glauben

Eine Ausnahme von dem zuvor aufgestellten Grundsatz der Rechtmäßigkeit der Datenverarbeitung stellt der Grundsatz der Verarbeitung nach Treu und Glauben auf. Dieser sollte indes – zumindest in der ersten Zeit nach In-Kraft-Treten der DSGVO – bei der Anwendung der DSGVO vernachlässigt werden. Aufgrund der durchaus erheblichen Veränderungen des Datenschutzrechts bestehen bis dato keinerlei Fallbeispiele oder Erfahrungswerte, anhand derer sich eine Verarbeitung nach Treu und Glauben bewerten lassen könnte. Zudem liegt auch in einem solchen Fall die Beweislast vollständig beim Verarbeiter der personenbezogenen Daten – wie übrigens auch das Bußgeldrisiko.

c. Transparenz

Nach dem Grundsatz der Transparenz sollen die betroffenen Personen, also z.B. die Kunden, ihre Rechte auch wahrnehmen können. Deshalb stellt die DSGVO an vielen Stellen (die im Weiteren beschrieben werden) Informationspflichten des Verantwortlichen auf.

In Erwägungsgrund 39 DSGVO heißt es hierzu:

„(…) Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. (…)“

d. Zweckbindung

Der Grundsatz der Zweckbindung bestimmt, dass die Zwecke der Datenverarbeitung bereits vor der Erhebung personenbezogener Daten durch den für die Verarbeitung Verantwortlichen festgelegt werden sowie eindeutig und legitim sein müssen. Eine Weiterverarbeitung zu anderen Zwecken ist gleichwohl möglich, sofern die Zwecke der Weiterverarbeitung nicht mit den ursprünglichen Erhebungszwecken unvereinbar sind und eine Rechtsgrundlage hierfür vorliegt (sog. „begrenzte Weiterverarbeitungsbefugnis“)

e. Datenminimierung

Personenbezogene Daten müssen dem Zweck entsprechend angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Im Rahmen einer rechtlich zulässigen Datenverarbeitung soll eine möglichst weitgehende Reduktion des Personenbezugs erreicht werden, nicht dagegen eine Reduktion der Datenquantität an sich. So muss der für die Verarbeitung Verantwortliche bei jeder personenbezogenen Datenerhebung und -verarbeitung prüfen, ob eine solche zur Erreichung des Zwecks erforderlich ist oder alternativ auch eine Verarbeitung anonymisierter Daten ausreichend wäre.

f. Richtigkeit

Nach der DSGVO trifft den Verantwortlichen zukünftig eine „Update-Pflicht“ hinsichtlich der verarbeiteten personenbezogenen Daten. Letztere müssen demnach sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Andernfalls trifft den Verantwortlichen eine Pflicht zur Löschung bzw. Berichtigung – und dies unverzüglich. Realisiert werden kann die Vorgabe über das Vorhalten angemessener Maßnahmen, wie z.B. ein leicht zugängliches Beschwerde- und Korrekturmanagement.

g. Speicherbegrenzung

Mit der in der DSGVO normierten Speicherbegrenzung dürfen personenbezogene Daten nur in einer Form gespeichert werden, die die Identifizierung der Person nur solange ermöglicht, wie es für die Zwecke der Verarbeitung erforderlich ist. Im Umkehrschluss bedeutet das: Sobald die Speicherung personenbezogener Daten für den Verarbeitungszweck also nicht mehr erforderlich ist, müssen die personenbezogenen Daten gelöscht oder die Identifizierung der betroffenen Person aufgehoben werden.

h. Integrität und Vertraulichkeit

Schließlich müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Dies umfasst auch den Schutz vor unbefugter und unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung der personenbezogenen Daten. Hierfür sind geeignete technische und organisatorische Maßnahmen zu treffen.

8. Rechtmäßigkeit der Datenverarbeitung

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten ist in Art. 6 Abs. 1 DSGVO geregelt. Dabei gilt auch in der neuen DSGVO – so wie in Deutschland bislang auch – der Grundsatz vom Verbot mit Erlaubnisvorbehalt. Das bedeutet, dass eine Datenverarbeitung grundsätzlich verboten ist, es sei denn, es liegt eine Einwilligung des Betroffenen oder ein gesetzlicher Erlaubnistatbestand vor.

Erlaubt ist die Verarbeitung personenbezogener Daten nach der DSGVO damit nur

- wenn eine Einwilligung der betroffenen Person vorliegt,
- zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen,
- zur Erfüllung einer rechtlichen Verpflichtung,
- zum Schutze lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person,
- zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde oder
- zur Wahrung berechtigter Interessen im Rahmen einer Interessenabwägung.

Die Datenverarbeitung ist bereits rechtmäßig, wenn einer der genannten Tatbestände vorliegt. Auf die wichtigsten Erlaubnistatbestände wird nun näher eingegangen.

a. Einwilligung des Betroffenen

Wie bereits nach bestehendem, deutschem Recht, ist die Einwilligung des Betroffenen die sicherste und zugleich rechtlich stärkste Möglichkeit, um eine rechtmäßige Verarbeitung personenbezogener Daten zu gewährleisten.

Die Einwilligung des Betroffenen muss dabei wie folgt erklärt werden:

- freiwillig,
- bestimmt,
- in informierter Weise,
- ausdrücklich und unmissverständlich.

Es ist zwingend darauf zu achten, dass die Einwilligung des Betroffenen auf dessen autonomer und ausdrücklich selbstbestimmter Entscheidung zur Weitergabe der entsprechenden Daten beruht. Die Einwilligung ist mithin streng zweckgebunden einzuholen und muss stets die mit der Einwilligung zu rechtfertigenden Verarbeitungszwecke anführen.

Achtung: Eine Generaleinwilligung im Sinne eine unbeschränkten Zusage in die Verarbeitung und Nutzung personenbezogener Daten ist nicht rechtmäßig.

Bsp.: Verwendet ein Onlineshop-Betreiber Klauseln wie: „Der Käufer willigt hiermit in die Verarbeitung seiner personenbezogenen Daten ein.“ liegt keine wirksame Einwilligung vor. Es fehlt an der konkreten Bestimmung, wozu die personenbezogenen Daten verwendet werden sollen.

Im Gegensatz dazu gilt eine einmal erteilte wirksame Einwilligung zur Verarbeitung personenbezogener Daten zu einem bestimmten Zweck für alle daraus folgenden und mit dem Zweck vereinbaren Datenverarbeitungsprozesse.

Die Einwilligung kann auf unterschiedliche Art und Weise erfolgen. Erwägungsgrund 32 der DSGVO führt hierzu aus:

„Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung. Dies könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert.“

Die Einwilligung kann daher erfolgen

- schriftlich,
- elektronisch (in unterschiedlicher Form),
- mündlich oder
- durch schlüssiges Verhalten.

Achtung: Die Einholung einer schriftlichen oder zu dokumentierenden elektronischen Einwilligung erscheint ratsam, muss der Verarbeiter der personenbezogenen Daten doch die Rechtmäßigkeit der Datenverarbeitung nachweisen können, Art. 7 Abs. 1 DSGVO.

Zudem muss das in Art. 7 Abs. 2 DSGVO aufgestellte Transparenzgebot unbedingt beachtet werden. Danach muss die Einwilligung in klarer und verständlicher Sprache erfolgen und insbesondere dann, wenn der Einwilligungstext noch andere Sachverhalte betrifft, die datenschutzrechtliche Relevanz gesondert hervorheben.

Achtung: Der Einwilligungstext sollte im besten Fall gesondert von anderen Informationen dargestellt werden. Ist dies nicht, oder nur unter erheblichem Aufwand möglich, sollte der die Einwilligung betreffende Teil des Textes optisch hervorgehoben werden.

Ein Erklärungsbewusstsein / Einwilligungsbewusstsein sowie eine gewisse Einsichtsfähigkeit werden darüber hinaus ebenfalls vorausgesetzt.

Achtung: Hier zeigt sich die Wichtigkeit eines eindeutigen Erklärungstextes. Ein deutlicher Hinweis, dass der Inhaber der personenbezogenen Daten in deren Verarbeitung einwilligt, spricht für das Bestehen des Erklärungsbewusstseins.

Zudem muss die Erklärung freiwillig erfolgen. Eine Einwilligung entfaltet nur rechtfertigende Wirkung, wenn sie Ausdruck einer selbstbestimmten und ungezwungenen

Entscheidung ist. Jegliche Zwangshandlung (seitens des Datenverarbeitenden) sowie die Ausübung von Druck lassen dagegen ihre Wirksamkeit entfallen.

So entfällt nach Art. 7 Abs. 4 DSGVO die Freiwilligkeit, wenn die Einwilligung in Datenverarbeitungsprozesse als zwingende Bedingung für die Durchführung eines Vertrages formuliert ist, obwohl der Verarbeiter die Daten dafür eigentlich nicht benötigt. Die DSGVO führt damit ein allgemeines Kopplungsverbot ein, dass das bisherige Datenschutzrecht in Deutschland nur in eingeschränkter Form für den Bereich der Werbung kannte.

Bsp. Im Online-Shop wird die Adresse des Kunden bereits mit Anklicken der Internetseite abgefragt. Die Seite baut sich nicht auf, solange die Adresse nicht vollständig angegeben wurde.

Bsp.: Online-Gewinnspiele: Die Teilnahme an einem Online-Gewinnspiel ist von der Einwilligung des Nutzers in die Verarbeitung von Daten zu Werbezwecken abhängig, die für die konkrete Gewinnaktion nicht zwangsweise erforderlich sind. Ein solcher Fall könnte im Zweifel zukünftig keine rechtmäßige Verarbeitung personenbezogener Daten mehr darstellen. Ebenso erscheint die Praxis, dass vor einer Inanspruchnahme eines Gewinns eine Anmeldung für einen Newsletter zwingend erfolgen muss, zukünftig fraglich.

b. Widerrufsrecht

Wie bereits im bisherigen deutschen Datenschutzrecht muss auch nach der DSGVO der Betroffene eine einmal erteilte Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen können. Als neuen Grundsatz stellt die DSGVO dabei ein Simplizitätsgebot auf: Der Widerruf der Einwilligung muss in Zukunft genau so einfach sein wie ihre Erteilung.

Bsp.: Der Verweis auf einen Dritten zur Wirksamkeit eines Widerrufs dürfte regelmäßig unzulässig sein.

Bsp.: Der in Newslettern übliche „Unsubscribe-Link" am Ende jeder Email dürfte hingegen weiterhin zulässig sein.

c. Vertrag und vorvertragliche Maßnahmen

Wie bislang ist die Verarbeitung zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen grundsätzlich rechtmäßig. Zu berücksichtigen ist aber, dass die Verarbeitung personenbezogener Daten nur soweit erfolgt, wie dies objektiv erforderlich ist. Dies gilt – mit Ausnahme der Einwilligung – für alle genannten Tatbestände.

Bsp.: Im Rahmen bestehender Verträge werden regelmäßig die Erfassung von Vertrags-, Stammdaten und Abrechnungsdaten des Vertragspartners notwendig sein, um eine Rechnung zu erstellen oder eine Lieferung korrekt ausführen zu können. Die Speicherung dieser Daten ist dann von diesem Rechtfertigungsgrund gedeckt.

Werden diese Daten jedoch zur Werbung weiterverwendet, entfällt – zumindest für diesen Teil der Datenverarbeitung – die Rechtfertigung aufgrund vertraglicher Notwendigkeit. Andere Rechtfertigungsgründe können aber dennoch greifen.

d. Rechtliche Verpflichtung

Demgegenüber stellt Art. 6 Abs. 1 lit. c) DSGVO die Verarbeitung in den Vordergrund, die durch oder aufgrund von Rechtsvorschriften erforderlich ist. Die Rechtsgrundlage wird dabei durch Unionsrecht oder das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, festgelegt. Etwa aus Rechtsvorschriften des Handels- und Steuerrechts können sich umfassende Dokumentations- und Aufbewahrungspflichten ergeben, die erfüllt werden müssen.

Bsp.: Nach § 257 HGB ist jeder Kaufmann dazu verpflichtet, empfangene Handelsbriefe (§ 257 Abs. 1 Nr. 2 HGB), Wiedergaben von Handelsbriefen (§ 257 Abs. 1 Nr. 3 HGB) und Buchungsbelege (§ 257 Abs. 1 Nr. 4 HGB) aufzubewahren. Die Aufbewahrungsfrist beträgt nach § 257 Abs. 4 HGB für Buchungsbelege zehn Jahre und für Handelsbriefe sechs Jahre.

Ähnliche Aufbewahrungspflichten treffen Unternehmer nach § 147 Abs. 1 Nr. 2-4, Abs. 3 AO.

Achtung: Auch wenn solche Aufbewahrungspflichten gesetzlich vorgeschrieben werden, dürfen diese Daten nach dem Grundsatz der Zweckbindung der Datenverarbeitung nicht für andere Zwecke – wie etwa Werbemaßnahmen – verwendet werden.

e. Abwägung bei berechtigtem Interesse

Darüber hinaus kommt nach Art. 6 Abs. 1 Satz 1 lit. f) DSGVO das berechtigte Interesse des Verantwortlichen oder eines Dritten als Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten in Betracht. Das berechtigte Interesse umfasst das rechtliche, tatsächliche, wirtschaftliche oder ideelle Interesse des Verantwortlichen, wobei eine umfassende Interessenabwägung insbesondere anhand des Zwecks der Datenverarbeitung sowie der Art und des Inhalts der betroffenen Daten erfolgen muss. Dabei dürfen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen. Im Zweifelsfall sollte der Datenschutzbeauftragte beurteilen, ob die Verarbeitung personenbezogener Daten rechtmäßig ist.

Bsp.: Die Sammlung und Weitergabe personenbezogener Daten zum Zwecke des Marketings dürfte daher kein berechtigtes Interesse im Sinne der eben genannten Vorschrift darstellen. Das im alten BDSG aufgestellte Listenprivileg wurde ersatzlos gestrichen. Es bedarf in solchen Fällen also zukünftig wohl einer ausdrücklichen Einwilligung durch den Betroffenen.

Bsp.: Auch eine Datenübermittlung an Auskunfteien sowie die Evaluation von Nutzerverhaltensmuster im Wege des „Scoring“ werden künftig nur noch zulässig sein, wenn Ihnen eine ausdrückliche Einwilligung des Betroffenen vorangegangen ist.

f. Zweckänderung

In Art. 5 Abs. 1 DSGVO ist festgelegt, dass personenbezogene Daten nur für eindeutige und legitime Zwecke erhoben werden dürfen. Wenn eine Erhebung für einen bestimmten Zweck erfolgt, dürfen die Daten nicht außerhalb dieser Zweckbestimmung genutzt werden. Allerdings ist in Ausnahmefällen eine Zweckänderung durchaus möglich. Ausgangspunkt hierbei ist Art. 6 Abs. 4 DSGVO. Bei besonders geschützten personenbezogenen Daten (sensible Daten) sind darüber hinaus die Regelungen in Art. 9 DSGVO zu beachten.

Grundsätzlich ist eine Zweckänderung nur dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind. Die Erhebung kann dabei sowohl von dem Verantwortlichen, dem Auftragsverarbeiter oder einem Dritten erfolgt sein.

Art. 6 Abs. 4 DSGVO listet hierzu verschiedene, nicht abschließende Kriterien auf. Zur Feststellung der Rechtmäßigkeit einer Zweckänderung sind daher zunächst folgende Kriterien in Ansatz zu bringen:

- Bestehen einer Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden und den Zwecken der beabsichtigten Weiterverarbeitung,
- Kontext der Erhebung der personenbezogenen Daten und Verhältnis von betroffener Person und dem Verantwortlichen,
- die Art der personenbezogenen Daten, insbesondere, ob sensible Daten verarbeitet werden,
- die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
- das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Achtung: Das Vorliegen eines Rechtfertigungsgrundes ist in jedem Fall vom Verantwortlichen nachzuweisen. Der Abwägungsprozess sollte also dokumentiert werden.

Die Einwilligung der betroffenen Person – erfolgt diese formell ordnungsgemäß – ist in jedem Fall ein Rechtfertigungsgrund.

Achtung: Zweckänderungen lösen zudem erneute Mitteilungspflichten aus. Siehe dazu die Informationspflichten im nächsten Kapitel.

Im Falle einer Zweckänderung muss schließlich geprüft werden, ob die Zweckänderung auch mit allen Grundsätzen der DSGVO vereinbar ist. Unter Umständen müssen zudem die Risikobewertung überprüft sowie die technisch-organisatorischen Maßnahmen angepasst werden. Gegebenenfalls kann auch eine Datenschutz-Folgeabschätzung nach Art. 35 DSGVO notwendig sein. Soweit die Zweckänderung auch Auswirkungen auf Auftragsdatenverarbeitungen hat, müssen gegebenenfalls Verträge mit Auftragsverarbeitern angepasst werden.

9. Informationspflichten

Der Verantwortliche hat bei der Datenerhebung, -verarbeitung bzw. -nutzung zu jeder Zeit Transparenz gegenüber der betroffenen Person herzustellen. Eine umfassende Information des Betroffenen ist mithin Grundvoraussetzung aller relevanten Prozesse. Nach der DSGVO erfolgt dabei eine Unterscheidung zwischen Informationspflichten bei der Erhebung personenbezogener Daten beim Betroffenen und Informationspflichten in den Fällen, in denen die Erhebung nicht beim Betroffenen erfolgt.

a. Erhebung personenbezogener Daten beim Betroffenen

Werden personenbezogene Daten beim Betroffenen selbst erhoben, muss der Verantwortliche nach Art. 13 Abs. 1 DSGVO folgende Informationen mitteilen:

- Identität des Verantwortlichen,
- Kontaktdaten des Datenschutzbeauftragten,
- Verarbeitungszwecke und Rechtsgrundlage der Datenerhebung und Datenverarbeitung,
- Berechtigtes Interesse,
- Empfänger der personenbezogenen Daten,
- Ggfls. Übermittlung an Drittstaaten.

Zudem muss der Verantwortliche über Folgendes informieren:

- **Dauer der Speicherung**

  Es ist konkret anzugeben, für wie lange die personenbezogene Daten gespeichert werden. Nur ausnahmsweise, wenn die Angabe einer konkreten Zeitspanne dem Verantwortlichen nicht möglich ist, reichen Kriterien für die Festlegung der endgültigen Dauer der Speicherung aus, anhand derer eine Bestimmbarkeit hergestellt wird.

- **Rechte der Betroffenen**

  Der Verantwortliche muss den Betroffenen über seine Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung sowie Datenübertragbarkeit informieren.

- **Widerrufbarkeit von Einwilligungen**

  Beruht die Datenverarbeitung auf einer Einwilligung des Betroffenen ist darauf hinzuweisen, dass die widerruflich ist. Die entsprechende Informationspflicht ist nur erfüllt, wenn gleichzeitig darüber aufgeklärt wird, dass die Einwilligung jederzeit widerrufen werden kann und die Datenverarbeitung bis zum Zeitpunkt des Widerrufs rechtmäßig bleibt.

- **Beschwerderecht bei der Aufsichtsbehörde**

  Der Betroffene ist darüber aufzuklären, dass er sich gemäß Art. 7 DSGVO bei einer Aufsichtsbehörde beschweren kann, wenn er der Ansicht ist, dass die Verarbeitung seiner personenbezogenen Daten rechtswidrig erfolgt.

- **Verpflichtung zur Bereitstellung personenbezogener Daten**

  Besteht für den Betroffenen eine Pflicht, die entsprechenden personenbezogenen Daten bereitzustellen, ist über die gesetzliche oder vertragliche Grundlage sowie der eventuellen Folgen der Nicht-Bereitstellung zu informieren.

- **Automatisierte Entscheidungsfindung und Profiling**

  Sobald der Verantwortliche Verfahren der automatisierten Entscheidung oder andere Profiling-Maßnahmen durchführt, muss der Betroffene über die besondere Tragweite und die angestrebten Auswirkungen solcher Verfahren informiert werden. Diese Informationspflicht erstreckt sich auf Angaben zu der dazu verwendeten Logik oder des Algorithmus.

b. Erhebung von personenbezogenen Daten bei Dritten

Werden personenbezogene Daten nicht unmittelbar beim Betroffenen, sondern bei oder über einen Dritten erhoben, bestehen nach Art. 14 DSGVO für den Verantwortlichen nahezu identische Informationspflichten, wie bei der Erhebung direkt beim Betroffenen. Zudem muss der Verantwortliche über die Quelle die personenbezogenen Daten informieren.

Achtung: In vielen Fällen müssen zukünftig kombinierte Datenschutzerklärungen bereitgestellt werden, wenn die Daten teils beim Betroffenen selbst und teils von Dritten stammen. Dies kann beispielsweise bei der Verarbeitung personenbezogener Daten zum Zwecke des Abschlusses von Finanzierungsverträgen im Bankenbereich erheblich sein. Auch der letzte Schritt eines Kaufabschlusses im Online-Handel, bei dem die vom Kunden eingegebenen Daten mit denen von Auskunfteien übermittelten Daten zur Bestimmung der Zahlungsmethode ergänzt werden, ist in diesem Zusammenhang zu nennen.

c. Form der Information

Hinsichtlich der Form der Datenschutzinformationen sind die Vorgaben in Art. 12 DSGVO zu beachten. Danach sind die Informationen der betroffenen Person „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln“.

d. Zeitpunkt und Art der Bereitstellung

Ebenfalls relevant ist die Frage, zu welchem Zeitpunkt die Datenschutzinformationen der betroffenen Person bereitgestellt werden müssen. Werden personenbezogene Daten direkt beim Betroffenen erhoben, sind die Informationen der betroffenen Person zum Zeitpunkt der Erhebung mitzuteilen.

Achtung: Im Online-Bereich kann dies - wie aktuell bereits regelmäßig der Fall - dadurch erfüllt werden, dass auf der Webseite ein Link zur Datenschutzerklärung mit den spezifischen Informationen aufgenommen wird. Im Print-Bereich sieht dies anders aus: hier dürfte ein sogenannter Medienbruch, bei dem im

Fall einer Print-Direktwerbung auf einen Web-Link zu einer ausschließlichen online verfügbaren Datenschutzerklärung verwiesen wird, regelmäßig unzulässig sein. Die Informationen müssen vielmehr im Print-Mailing zur Verfügung gestellt werden.

Wichtig ist hierbei die Dokumentation der Datenschutzinformation, da den Verantwortlichen insoweit eine Nachweispflicht trifft.

10. Rechte des Betroffenen

Neben den zuletzt besprochenen Auskunftsrechten hat der Betroffene weitere Rechte gegenüber dem Verantwortlichen.

a. Auskunftsrecht

Art. 15 DSGVO statuiert ein umfassendes Auskunftsrecht des Betroffenen. Der Verantwortliche hat – allerdings nur auf Nachfrage - über Folgendes zu informieren:

- Zweck der Datenverarbeitung,
- Kategorien der Daten,
- Empfänger oder Kategorien von Empfängern,
- Dauer der Speicherung,
- Recht auf Berichtigung, Löschung und Widerspruch,
- Beschwerderecht bei einer Aufsichtsbehörde,
- Herkunft der Daten (wenn nicht bei Betroffenen erhoben),
- Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling,
- Übermittlung in Drittland oder an internationale Organisation.

Der Verantwortliche muss dem Betroffenen auf Anfrage eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung stellen. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

Das Auskunftsrecht besteht nur in angemessenen Abständen. Eine tägliche Abfrage der Daten durch den Betroffenen ist mithin nicht möglich.

b. Recht auf Berichtigung

Sind die erhobenen personenbezogenen Daten falsch oder unvollständig, kann der Betroffenen vom Verantwortlichen eine Berichtigung seiner personenbezogenen Daten verlangen. Die Berichtigung hat unverzüglich zu erfolgen.

Achtung: Die betroffene Person muss ihre Identität nur dann nachweisen, wenn der Verantwortliche berechtigte Zweifel daran hat.

Die Pflicht zur Berichtigung, Löschung oder Einschränkung der Daten trifft ausschließlich den Verantwortlichen. Wird ein Antrag irrtümlich an einen Auftragsverarbeiter gerichtet, trifft diesen zwar keine ausdrückliche Pflicht, den Antrag an den Verantwortlichen weiterzuleiten. Der Auftragsverarbeiter hat jedoch eine Unterstützungspflicht dem Verantwortlichen gegenüber.

Der Antrag kann formlos gestellt werden.

c. Recht auf Löschung (Recht auf Vergessenwerden)

Der Betroffene hat einen Löschungsanspruch gegenüber dem Verantwortlichen:

- wenn die Speicherung der Daten nicht mehr notwendig ist,
- wenn der Betroffene seine Einwilligung zur Datenverarbeitung widerrufen hat,
- wenn die Daten unrechtmäßig verarbeitet wurden und
- wenn eine Rechtspflicht zum Löschen nach EU- oder nationalem Recht besteht.

Der Löschungsanspruch ist in folgenden Fällen ausgeschlossen:

- wenn das Recht auf freie Meinungsäußerung bzw. die Informationsfreiheit überwiegen,
- wenn die Datenspeicherung der Erfüllung einer rechtlichen Verpflichtung dient,
- wenn das öffentliche Interesse im Bereich der öffentlichen Gesundheit überwiegt,
- wenn Archivzwecke oder wissenschaftliche und historische Forschungszwecke entgegenstehen oder
- wenn die Speicherung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Bei Bestehen eines Löschungsanspruchs trifft den für die Veröffentlichung der Daten Verantwortlichen eine umfassende Mitwirkungspflicht bei der Löschung der Daten. So muss dieser - unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten - angemessene Maßnahmen treffen, um die Verantwortlichen, die die Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt hat.

d. Recht auf Einschränkung

Unter Geltendmachung seines Rechts auf Einschränkung der Verarbeitung kann der Betroffene verlangen, dass alle erhobenen personenbezogenen Daten ab dem Zeitpunkt der Geltendmachung grundsätzlich nur mit individueller Einwilligung verarbeitet werden dürfen. Voraussetzung für das Recht auf Einschränkung ist das Zutreffen einer der folgenden Gründe:

- Die betroffene Person hat die Richtigkeit der personenbezogenen Daten bestritten.

- Die Verarbeitung ist unrechtmäßig und die betroffene Person hat die Löschung der personenbezogenen Daten abgelehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt.
- Der Verantwortliche benötigt die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger, die betroffene Person jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
- Die betroffene Person hat Widerspruch gegen die Verarbeitung eingelegt.

Auch hier muss eine Mitteilung an die die Daten Verarbeitende durch den für die Veröffentlichung der Daten Verantwortlichen.

e. Recht auf Datenübertragbarkeit

Der Betroffene hat das Recht, die von ihm zur Verfügung gestellten Daten von einer automatisierten Anwendung, etwa einem sozialen Netzwerk, auf eine andere Anwendung zu übertragen.

Demnach hat die betroffene Person „das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln“. Dies soll immer dann gelten, wenn die Grundlage der Datenverarbeitung die Einwilligung oder ein Vertrag ist und die Daten automatisiert verarbeitet werden.

Achtung: Für nur in Papierform vorgehaltene Daten gilt dies demnach nicht. Den direkten Transfer von einem Anbieter zu einem anderen Anbieter können die Verantwortlichen mit der Begründung ablehnen, dass dies aus technischen Gründen nicht machbar ist.

11. Technischer Datenschutz

Wer personenbezogene Daten verarbeitet, muss diese mittels technischer und organisatorischer Maßnahmen (kurz TOMs) schützen. Nach Art. 32 DSGVO müssen dazu, „geeignete technische und organisatorische Maßnahmen [getroffen werden], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“.

Weitere Konkretisierungen erfolgen nicht. Im Rahmen einer Arbeitsgruppe zu Verzeichnissen für Verarbeitungstätigkeiten nach Art. 30 DSGVO wurde eine Mustervorlage zur Beschreibung der „technischen und organisatorischen Maßnahmen“ durch die deutschen Aufsichtsbehörden herausgegeben. Darin werden folgende Aspekte zur Gewährleistung des technischen Datenschutzes aufgeführt:

- Pseudonymisierung,
- Verschlüsselung,
- Gewährleistung der Vertraulichkeit,
- Gewährleistung der Integrität,
- Gewährleistung der Verfügbarkeit,
- Gewährleistung der Belastbarkeit der Systeme,

- Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall,
- Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Es ist folgende Herangehensweise anzuraten:

- Etablieren eines Managements für Datensicherheit oder Informationssicherheit,
- Feststellen des Schutzbedarfes,
- Bewertung von Risiken,
- Treffen und Umsetzen der jeweiligen Maßnahmen,
- Führen von Dokumentationen und Nachweisen.

12. Auftragsverarbeitung

Auftragsdatenverarbeitung bezeichnet das Erheben, Verarbeiten oder Nutzen personenbezogener Daten durch einen Dienstleister (Auftragnehmer). Der Dienstleister ist an die Weisungen des Auftragsgebers gebunden.

Auftragsverarbeiter können beispielsweise externe Personalagenturen, Gehaltsabrechnungsbüros, Steuerberater, Marketingagenturen, Call-Center und Cloud-Computing-Anbieter sowie externe IT-Administratoren sein. Erbringt die Verbundgruppe gegenüber ihren Anschlusshäusern eigens Dienstleistungen (E-Shop-Lösungen, Web-Lösungen, Portal-Lösungen, CRM-Systeme, PIM-Systeme, Warenwirtschafts-Systeme, Marketing-Lösungen, Newsletter-Lösungen etc.), kann auch sie Auftragsverarbeiter sein.

a. Allgemeine Pflichten

Der Verantwortliche (Auftraggeber) muss den Auftragsverarbeiter sorgfältig und unter besonderer Berücksichtigung der technischen und organisatorischen Maßnahmen (TOMs) auswählen. Dies kann bspw. Durch eine Zertifizierung des Auftragsverarbeiters nach Art. 42 DSGVO nachgewiesen werden.

Den Auftragsverarbeiter trifft insbesondere die Pflicht, die Daten nur auf Weisung des für die Verarbeitung Verantwortlichen zu verarbeiten.

b. Pflicht zur vertraglichen Vereinbarung (ADV-Vertrag)

Auch nach dem In-Kraft-Treten der DSGVO wird die Pflicht zur Vereinbarung von Verträgen zur Auftragsdatenverarbeitung (ADV) bestehen bleiben.

Achtung: Alt-ADV-Verträge behalten weiterhin ihre Gültigkeit. Die ADV-Verträge müssen jedoch gegebenenfalls an das neue Datenschutzrecht nach In-Kraft-Treten der DSGVO angepasst werden.

Wesentlicher Inhalt eines ADV-Vertrags sind folgende Punkte:

- der für die Datenverarbeitung Verantwortliche,
- Gegenstand und Dauer der Verarbeitung,
- Art und Zweck der Verarbeitung,
- Art der personenbezogenen Daten und Kategorien von betroffenen Personen,
- Umfang der Weisungsbefugnisse,
- Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit,
- Sicherstellung von technischen und organisatorischen Maßnahmen für den Datenschutz,
- Etwaige Hinzuziehung von Subunternehmern,
- Unterstützung des Auftraggebers (für die Verarbeitung Verantwortlichen) durch den Auftragsverarbeiter, wenn es um die größtmögliche Sicherheit der Verarbeitung personenbezogener Daten geht,
- Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsdatenverarbeitung,
- Kontrollrechte des für die Verarbeitung Verantwortlichen und Duldungspflichten des Auftragsverarbeiters,
- Pflicht des Auftragsverarbeiters, den Verantwortlichen zu informieren, falls eine Weisung gegen Datenschutzrecht verstößt.
- Je klarer Sie im ADV-Vertrag die Vereinbarungen zur Auftragsverarbeitung treffen und je präziser darin die Pflichten definiert werden, desto mehr Rechtssicherheit können sowohl Sie als auch der Auftragsverarbeiter erwarten.

Zur Vermeidung von Rechtsunsicherheit empfiehlt es sich, die Pflichten des Auftragsdatenverarbeiters klar und präzise in dem ADV-Vertrag zu definieren.

Achtung: ADV-Verträge können zukünftig schriftlich oder – und das ist neu - elektronisch abgeschlossen werden. Dies erleichtert den Abschluss von ADV erheblich.

c. Joint Control – gemeinsam für die Verarbeitung Verantwortliche

Ein Novum nach deutschem Datenschutzrecht stellt Art. 26 DSGVO mit der sogenannten Joint Control auf. Dabei erfolgt die Datenverarbeitung im Auftrag als gemeinsame, gleichberechtigte Verantwortungsaufgabe von Auftraggeber und Auftragnehmer. Zwei oder mehrere Verantwortliche legen danach die Zwecke und Mittel zur Verarbeitung personenbezogener Daten transparent fest.

Achtung: Der Betroffene kann seine Ansprüche zukünftig gegenüber jedem für die Verarbeitung Verantwortlichen geltend machen – also sowohl gegenüber dem Auftragsnehmer, als auch dem Auftragsverarbeiter. Es ist jedoch zu erwarten, dass sich der Betroffene primär auch bei der Datenverarbeitung an den Verantwortlichen als ersten Ansprechpartner halten wird.

d. Wartung/Fernzugriff durch IT-Dienstleister

Der Status der technischen Wartung durch externe IT-Dienstleister ist momentan noch ungeklärt. Ein Kriterium zur Abgrenzung – und damit zur Bestimmung der Pflichten nach der DSGVO - kann die Frage darstellen, inwieweit der IT-Dienstleister durch die Wartung Zugriff auf personenbezogene Daten erhält – letzteres wäre auch im Falle einer Fernwartung als Auftragsdatenverarbeitung zu werten.

Achtung: Es empfiehlt sich daher, auch bei „einfachen“ IT-Dienstleistungsverträgen eine Verschwiegenheitsverpflichtung zu vereinbaren.

e. Einsatz von Subunternehmen

Die Beauftragung eines Subunternehmers aufseiten des Auftragsverarbeiters bedarf einer schriftlichen oder elektronischen Zustimmung des Verantwortlichen. Außerdem muss der ADV-Vertrag zwischen Auftragsverarbeiter und Subunternehmer die gleichen Pflichten enthalten wie der ADV-Vertrag zwischen Verantwortlichen und Auftragsverarbeiter.

Achtung: Die Beauftragung eines Subunternehmers entbindet den Auftragsverarbeiter nicht von seinen Pflichten nach der DSGVO; der Auftragsverarbeiter haftet dem Verantwortlichen gegenüber weiterhin uneingeschränkt.

f. Gemeinsame Haftung/Verantwortlichkeit

Nach den neuen Regeln der DSGVO haften sowohl Verantwortlicher (Auftraggeber), als auch Auftragsverarbeiter künftig direkt gegenüber dem Betroffenen. Letzterer jedoch nur, wenn und soweit er gegen seine Pflicht zur weisungsgebundenen Verarbeitung verstößt.

Bsp.: *Ein „klassischer“ Verstoß dürfte in der Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter für eigene Zwecke oder Zwecke Dritter liegen; in einem solchen Fall wird er nach der DSGVO nämlich selbst als Verantwortlicher behandelt - mit allen rechtlichen Folgen.*

Auch bei Datenpannen haftet - im Gegensatz zur bisherigen Rechtslage - nicht nur der Verantwortliche, sondern auch der Auftragsverarbeiter.

13. Verarbeitungsverzeichnis

Durch das Inkrafttreten der DSGVO und der Anwendbarkeit der neuen Regeln ab Mai 2018 werden die bisherigen Regelungen des deutschen BDSG zur Führung eines Verfahrensverzeichnisses durch EU-weit geltende Vorgaben der Verordnung ersetzt.

Dabei wird auch der Begriff „Verfahrensverzeichnis“ durch den Begriff „Verzeichnis der Verarbeitungstätigkeiten“ (oder kurz Verarbeitungsverzeichnis) abgelöst. Es entfällt die bisher bestehende allgemeine Meldepflicht nach § 4d Abs. 1 BDSG, während eine allgemeine Nachweis- und Dokumentationspflicht für die Rechtmäßigkeit der Verarbeitung bei der verantwortlichen Stelle verankert wird (Art. 24 Abs. 1 DSGVO). Ebenfalls findet sich in der Verordnung die ausdrückliche Verpflichtung der verantwortlichen Stelle sowie (neu) der Auftragsverarbeiter zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten (Art. 30 DSGVO).
Jeder Verantwortliche und Auftragsverarbeiter ist verpflichtet, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.

Mit dem Verarbeitungsverzeichnis soll Transparenz über die Verarbeitung personenbezogener Daten geschaffen werden. Zudem dient es der rechtlichen Absicherung des Unternehmens. Der betriebliche Datenschutzbeauftragte sowie die Aufsichtsbehörden können aufgrund des Verarbeitungsverzeichnisses die Rechtmäßigkeit der Datenverarbeitung durch das Unternehmen bewerten.

a. Verpflichteter

Grundsätzlich gilt: Jeder hat ein Verzeichnis der Kategorien zu führen, die er verarbeitet. Dies führt im Zweifel zu einer Verpflichtung sowohl des Verantwortlichen als auch des Auftragsverarbeiters.

- Der **Auftragsverarbeiter** muss ein Verzeichnis über auf alle Kategorien führen, die im Auftrag des Verantwortlichen verarbeitet werden. Der Auftragsverarbeiter hat das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung stellen.

- Der **beauftragende Verantwortliche** muss parallel hierzu ein Verzeichnis aller Verarbeitungstätigkeiten führen, die seiner Zuständigkeit unterliegen.

Im Fall einer Datenverarbeitung im Auftrag als gemeinsame, gleichberechtigte Verantwortungsaufgabe von Auftraggeber und Auftragnehmer (Joint Control), sind grundsätzlich beide (oder alle) Beteiligten gleichermaßen zur Erstellung eines Verarbeitungsverzeichnisses verpflichtet. Vertragliche Vereinbarungen können jedoch regeln, wer das Verzeichnis erstellt.

Zwar besteht für Unternehmen mit weniger als 250 Mitarbeitern dem Grunde nach eine Ausnahme von der Pflicht zum Führen eines Verzeichnisses.

Achtung: Allerdings entfällt die Pflicht nur unter der Voraussetzung, dass die Verarbeitungen nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder eine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 DSGVO bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 DSGVO eingeschlossen wird.

Diese sehr kompliziert formulierte Ausnahme von der Ausnahme führt in der heutigen digitalen Welt vermutlich dazu, dass kaum Unternehmen von der Pflicht zur Führung eines Verarbeitungsverzeichnisses ausgenommen sein dürften. Normale Handels-, Handwerks- und Dienstleistungsunternehmen jedenfalls fallen in aller Regel NICHT unter die Ausnahme und sind damit zum Führen eines Verzeichnisses verpflichtet.

b. Vorlagepflicht

Der Verantwortliche und/oder der Auftragsverarbeiter, sowie gegebenenfalls deren Vertreter, stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung. Eine Meldepflicht, wie nach dem bisherigen BDSG, stellt die DSGVO nicht auf. Die Verzeichnisse sind regelmäßig in deutscher Sprache zu führen. Zumindest muss das

Unternehmen in der Lage sein, von der Aufsichtsbehörde angeforderte Verzeichnisse unverzüglich in deutscher Sprache vorzulegen.

Bsp.: Lohnabrechnungen – als eines der typischen Tätigkeiten von Unternehmen – dürften damit regelmäßig eine Pflicht zum Führen eines Verzeichnisses auslösen. Dies ändert sich ggf. nur, wenn die Tätigkeit vollständig von einem Steuerberater übernommen wird.

Weitere Verarbeitungstätigkeiten, die zum Führen eines Verzeichnisses verpflichten:

- *Marketing und Vertrieb, z.B. Kundendateien*
- *Leistungserbringung, z.B. Auftragsabwicklung*
- *Rechnungslegung*
- *Kundenbetreuung*
- *Beschaffung*
- *HR-Maßnahmen, z.B. Bewerbungsverfahren online/offline*

c. Inhalt des Verarbeitungsverzeichnisses

Der Verantwortliche (Auftraggeber) hat ein Verzeichnis mit folgendem Inhalt zu führen:

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten,
- die Zwecke der Verarbeitung,
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen,
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen,
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen,
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 Abs. 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien,
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien,
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO.

Der Auftragsverarbeiter hat ein Verzeichnis mit folgendem Inhalt zu führen:

- den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten,
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden,
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien,
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO.

Ausgehend von den soeben aufgeführten Mindestanforderungen werden Inhalt und Umfang des Verzeichnisses je nach Art und Größenordnung der Stelle eines Verantwortlichen oder Auftragsverarbeiters zu differenzieren sein.

d. Form

Das Verzeichnis ist schriftlich zu führen. Dies beinhaltet jedoch die Möglichkeit, eine entsprechende Datei anzulegen. Auch der Einsatz einer speziellen Software ist möglich. Nach allgemeinen verwaltungsrechtlichen Grundsätzen kann die Aufsichtsbehörde jedoch das Format der Vorlage eigenständig festlegen und daher auch bei einem im elektronischen Format geführten Verzeichnis den Ausdruck verlangen.

14. Meldepflicht von Datenpannen

Die Erfahrung gerade der letzten Jahre zeigt: Datenlecks, also die unfreiwillige Preisgabe von Daten, gehören bedauerlicherweise zum Alltag vieler Unternehmen. Die DSGVO spricht in diesem Zusammenhang von Datenpannen. Dies sind Verstöße gegen die Datensicherheit und den Datenschutz, bei denen personenbezogene Daten Unberechtigten vermutlich oder erwiesenermaßen bekannt werden. Ursachen dafür sind vielfältig und können z.B. in einem Hackerangriff, dem Verlust eines USB-Sticks, dem Diebstahl eines Smartphones oder in einem unbefugten Weitergeben durch Mitarbeiter – gleichgültig ob bewusst oder unbewusst – liegen.

Die DSGVO sieht für diese Fälle von Datenpannen ab Mai 2018 eine deutlich verschärftere Meldepflicht vor. Wann eine solche Verpflichtung besteht, richtet sich nach Art. 33 DSGVO für Meldungen an die Aufsichtsbehörde und Art. 34 DSGVO für Meldungen an die Betroffenen.

a. Meldungen an die Aufsichtsbehörde

Künftig muss grundsätzlich jede Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde gemeldet werden. Eine Beschränkung auf die oben bezeichneten Risikodaten kennt die DSGVO nicht. Eine Ausnahme besteht

nach Art. 33 Abs. 1 DSGVO nur dann, wenn die Datenpanne voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Es ist also stets eine Risikoabwägung durchzuführen. Diese Abwägung ist zu dokumentieren.

b. Meldungen an die Betroffenen

Ergibt die durchzuführende Risikoabwägung, dass durch die Datenpanne voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen besteht, sind diese - neben der Aufsichtsbehörde - nach Art. 34 DSGVO zu benachrichtigen.

Ausnahmen von der Pflicht zur Benachrichtigung der Betroffenen bestehen nach Art. 34 Abs. 3 DSGVO, wenn:

- geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen wurden, durch die die betroffenen Daten für Unbefugte nicht zugänglich sind (z.B. Verschlüsselung),
- durch nachfolgende Maßnahmen sichergestellt wurde, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht,
- die direkte Information der Betroffenen mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall ist jedoch eine öffentliche Bekanntmachung gefordert.

Auch hier empfiehlt es sich, das Bestehen von Ausnahmen sowie die Meldung als solche zu dokumentieren.

c. Umfang und Zeitpunkt der Meldung

Die Datenpanne muss innerhalb von 72 Stunden bei der zuständigen Aufsichtsbehörde gemeldet werden. Eine Überschreitung der Frist ist gesondert zu begründen.

Die Meldung muss dabei folgende Punkte enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze,
- der Name und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Die letzten drei Punkte sind auch bei der Benachrichtigung der Betroffenen zu berücksichtigen. Zudem ist in diesen Fällen die Meldung in einer klaren und einfachen Sprache zu verfassen.

15. Datenschutzbeauftragter

Ein betrieblicher Datenschutzbeauftragter muss mit dem in Kraft treten der DSGVO europaweit spätestens bis Mai 2018 von Unternehmen bestellt werden, deren Tätigkeit einer besonderen Kontrolle bedarf. Darüber hinaus kann jedes Unternehmen einen Datenschutzbeauftragten freiwillig bestellen.

a. Pflicht zur Bestellung

Nach Art. 37 Abs. 1 DSGVO ist ein betrieblicher Datenschutzbeauftragter in jedem Fall zu bestellen, 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 gemäß Art. 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO besteht (besondere Kategorien der Datenverarbeitung).

Unter dem Begriff „Kerntätigkeit“ ist jede Tätigkeit zu verstehen, die essentiell für die Erreichung der Ziele des Unternehmens sind.

Bsp.: Gesundheitsdaten in einem Krankenhaus, Handel mit personenbezogenen Daten (Auskunfteien, Adresshändler)

Bei der Bewertung einer „umfangreiche Verarbeitung“ sollten folgende Faktoren berücksichtigt werden:

- die Anzahl der Betroffenen,
- die Menge der betroffenen Daten und/oder die Vielzahl der verschiedenen Datensätze
- die Dauer der Datenverarbeitung
- die geographische Reichweite der Datenverarbeitung.

Achtung: Die Prüfung der vorgenannten Voraussetzungen für eine Pflicht-Bestellung nach den Regeln der DSGVO kann in den meisten Fällen dahinstehen, denn der deutsche Gesetzgeber hat die Pflicht zur Bestellung eines Datenschutzbeauftragten weiter konkretisiert. Danach muss - wie bislang - ein Datenschutzbeauftragter bereits dann bestellt werden, wenn in dem Unternehmen in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung unterliegen (siehe vorheriges Kapitel), oder

verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

b. Auswahlkriterien

Unabhängig davon, ob sich ein Unternehmen für einen internen oder externen Datenschutzbeauftragten entschieden hat, muss die ausgewählte Person gewisse Anforderungen erfüllen, um das Unternehmen bei der Umsetzung etwaiger Datenschutzregelungen gezielt unterstützen zu können. Insbesondere muss ein Interessenkonflikt unbedingt vermieden werden.

Nach Art. 37 Abs. 5 DSGVO muss der Datenschutzbeauftragte folgende Kriterien erfüllen:

- eine gewisse berufliche Qualifikation,
- das Fachwissen auf dem Gebiet des Datenschutzes und der Datenschutzpraxis und
- die Fähigkeiten zur Erfüllung der gesetzlich definierten Aufgaben.

Im Rahmen der beruflichen Qualifikation sollte der eingesetzte Datenschutzbeauftragte über ausreichende Kenntnisse und/oder Berufserfahrung im betreffenden Wirtschaftsbereich verfügen und im Stande sein, die verschiedenen Verarbeitungsprozesse zu erfassen. Das erforderliche Niveau des Fachwissens richtet sich insbesondere nach den durchgeführten Verarbeitungsvorgängen und dem erforderlichen Schutz für die personenbezogenen Daten, die der Verantwortliche oder der Auftragsverarbeiter verarbeiten.

Der Datenschutzbeauftragte sollte darüber hinaus ein solides Fachwissen in Bezug auf das IT-System und IT-Sicherheitsmaßnahmen verfügen und die damit einhergehenden datenschutzrechtlichen Bedürfnisse erkennen und im Arbeitsalltag berücksichtigen können.

Achtung: Spätestens mit der Anwendbarkeit der noch komplexeren DSGVO sollte der Faktor der juristischen Qualifikation eines betrieblichen Datenschutzbeauftragten eine Rolle spielen. Gerade vor diesem Hintergrund sollte der Einsatz eines externen Datenschutzbeauftragten geprüft werden.

c. Bestellung des Datenschutzbeauftragten

Weder die DSGVO, noch die deutschen Regeln zum Datenschutz bestimmen zukünftig eine bestimmte Form der Bestellung des Datenschutzbeauftragten.

Achtung: Aus Beweisgründen und zur Rechtsklarheit ist eine schriftliche Benennung eines Datenschutzbeauftragten jedoch empfehlenswert. Zudem sollten die Aufgaben des Datenschutzbeauftragten durch den Verantwortlichen im Vertrag explizit festgehalten werden, damit sich der Verantwortliche und der Datenschutzbeauftragte über seine Aufgaben im Klaren sind.

d. Publizität der Bestellung

Im Vergleich zum bisherigen nationalen Recht sieht die DSGVO eine verstärkte Publizität des Datenschutzbeauftragten und seiner Bestellung vor Nach Art. 37 Abs. 7 DSGVO müssen Verantwortliche und Auftragsverarbeiter die

- Kontaktdaten ihres Datenschutzbeauftragten veröffentlichen und
- diese der zuständigen Aufsichtsbehörde mitteilen.

Daher sind die Kontaktdaten des Datenschutzbeauftragten sowohl innerhalb der Organisation des Verantwortlichen (Intranet, Organisationspläne), als auch nach außen, z.B. auf der Homepage, zu veröffentlichen.

Achtung: Wie ein Vergleich mit Art. 13 Abs. 1 Buchst. a) DSGVO zeigt, wo von „Name und Kontaktdaten“ die Rede ist, setzt die Angabe der bloßen Kontaktdaten, z.B. auf der Homepage, nicht zwingend voraus, dass auch der Name des Datenschutzbeauftragten genannt wird. Im Verhältnis zur Aufsichtsbehörde ist die namentliche Nennung des Beauftragten aber gleichwohl sinnvoll.

e. Position des Datenschutzbeauftragten im Betrieb

Der betriebliche Datenschutzbeauftragte berichtet der Geschäftsleitung direkt und ist unmittelbar der höchsten Managementebene unterstellt, Art. 38 Abs. 3 S. 3 DSGVO. Der Datenschutzbeauftragte hat auch weiterhin keine Entscheidungsbefugnis, sondern berät das Unternehmen lediglich im Rahmen seiner Aufgaben.

f. Datenschutzbeauftragter – Benachteiligungsverbot

Der Datenschutzbeauftragte kann wegen der Erfüllung seiner Aufgaben nicht abberufen oder in sonstiger Weise benachteiligt werden, Art. 38 Abs. 3 S. 2 DSGVO. Anders, als nach bestehenden Datenschutzrecht ist ein besonderer Kündigungsschutz des Datenschutzbeauftragten nach den neuen Vorschriften nicht mehr vorgesehen.

g. Aufgaben und Pflichten des Datenschutzbeauftragten

Die Aufgaben und Pflichten eines betrieblichen Datenschutzbeauftragten umfassen nach Art. 39 DSGVO:

- Unterrichtung und Beratung der Verantwortlichen, der Auftragsverarbeiter und der Beschäftigten,
- Überwachung der Einhaltung der DSGVO und nationalen Sonderregelungen (BDSG neu)
- Sensibilisierung und Schulung der Mitarbeiter,
- Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung,
- Zusammenarbeit mit der Aufsichtsbehörde.

Um diesen Aufgaben und Pflichten nachkommen zu können, bestimmt Art. 38 Abs.1 DSGVO explizit, dass der Datenschutzbeauftragte „ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen“ einzubinden ist.

Grundsätzlich bleibt für die Einhaltung der datenschutzrechtlichen Vorschriften das Unternehmen selbst verantwortlich; der betriebliche Datenschutzbeauftragte wirkt insofern weiterhin in ausreichendem Maße auf die Einhaltung hin. Dennoch geht die bislang herrschende Auffassung von einer Haftung des Datenschutzbeauftragen für Verstöße gegen das Datenschutzrecht in seinem Bereich aus.

16. Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung (DSFA) ist eigentlich nichts anderes, als die bisher im deutschen Datenschutzrecht schon bekannte Vorabkontrolle. Die Folgenabschätzung bleibt - wie bislang auch - eine strukturierte Risikoanalyse.

Nach der DSGVO ist eine Folgenabschätzung immer dann durchzuführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge hat.

Darüber bestimmt Art. 35 Abs. 3 DSGVO eine Folgenabschätzung 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 ähnlicher Weise erheblich beeinträchtigen,
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10,
- systematische weiträumige Überwachung öffentlich zugänglicher Bereiche.

Die Aufsichtsbehörden sind nach Art. 35 Abs. 4 DSGVO gehalten, die eben genannten Kriterien in Listen zu konkretisieren. Diese noch zu erstellenden Listen (sogenannte Whitepaper) sollen die Fälle beschreiben, in denen eine Folgenabschätzung in jedem Fall erforderlich ist.

a. Inhalt der Folgenabschätzung

Nach Art. 35 Abs. 7 DSGVO muss eine Datenschutz-Folgenabschätzung mindestens folgende Inhalte haben:

- exakte Beschreibung der geplanten Verarbeitungsvorgänge und der jeweiligen Verarbeitungszwecke sowie etwaiger berechtigter Interessen des Verantwortlichen,
- Evaluierung von Notwendigkeit und Verhältnismäßigkeit der Erhebung personenbezogener Daten bezogen auf den jeweiligen Zweck,

- Evaluierung von Risiken für die Freiheiten sowie Rechte der Betroffenen,
- geplante Abhilfemaßnahmen, mit deren Hilfe die Risiken bewältigt werden können (Garantien, Sicherheitsvorkehrungen, Verfahren)

b. Verantwortlichkeiten

Es ist Aufgabe des Verantwortlichen, und nicht des Datenschutzbeauftragten, eine Datenschutz-Folgenabschätzung durchzuführen, falls sie erforderlich ist. Der Datenschutzbeauftragte berät und überwacht bei der Folgenabschätzung.

Der Verantwortliche sollte zu folgenden Gesichtspunkten den Rat des Datenschutzbeauftragten einholen:

- Erforderlichkeit einer Folgenabschätzung,
- Strategie bei Durchführung der Folgenabschätzung,
- Entscheidung für eine interne oder ausgelagerte Folgenabschätzung,
- Sicherheitsvorkehrungen (inklusive technischer und organisatorischer Maßnahmen), um die Risiken in Bezug auf die Rechte der Betroffenen zu minimieren ,
- Prüfung, ob die Durchführung der Folgenabschätzung richtig vorgenommen wurde und ob die Schlussfolgerungen daraus dem Datenschutzrecht übereinstimmen.

Achtung: Den Rat des Datenschutzbeauftragten einzuholen, bedeutet nicht, dass der Verantwortliche in jedem Fall dem Rat des Datenschutzbeauftragten zu folgen hat. Falls der Verantwortliche sich dazu entscheiden sollte, vom Rat des Datenschutzbeauftragten abzuweichen, sollte er gewährleisten, die Gründe für die Abweichung schriftlich zu dokumentieren, um seine Rechenschaftspflicht zu erfüllen.

17. Beschäftigtendatenschutz

Der Beschäftigtendatenschutz (oder auch Arbeitnehmerdatenschutz) ist in der DSGVO nicht eigenständig geregelt. Vielmehr wurde die Regelungsbefugnis durch eine Öffnungsklausel an die Mitgliedsstaaten zurückgespielt. Von dieser Möglichkeit hat auch der deutsche Gesetzgeber gebrauch gemacht und den Beschäftigtendatenschutz im BDSG neu geregelt.

a. Vorgaben zum Arbeitnehmerdatenschutz im neuen BDSG

Der deutsche Gesetzgeber hat von der ihm eingeräumten Kompetenz Gebrauch gemacht und mit § 26 BDSG neu eine Regelung zum Arbeitnehmerdatenschutz in das überarbeitete Bundesdatenschutzgesetz aufgenommen.

Eine Datenverarbeitung von Daten der Beschäftigten durch den Arbeitgeber ist demnach zulässig:

- wenn der Beschäftigte in die Datenverarbeitung eingewilligt hat,

- wenn die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung, Durchführung oder Beendigung eines Beschäftigtenverhältnisses erforderlich ist,
- zur Aufdeckung von Straftaten, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind,
- wenn personenbezogene Daten von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen,
- wenn dies zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist,
- wenn der Beschäftigte in die Datenverarbeitung eingewilligt hat.

b. Freiwilligkeit der Einwilligung

Für die Beurteilung der Freiwilligkeit der Einwilligung in die Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis sind insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen.

Freiwilligkeit kann insbesondere dann vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung ist grundsätzlich schriftlich einzuholen. Außerdem hat der Beschäftigte einen Auskunftsanspruch sowie ein Widerrufsrecht. Der Arbeitgeber muss den Beschäftigten über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht in Textform aufklären.

c. Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses ist zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Soweit die Verarbeitung auf der Grundlage einer Einwilligung erfolgt, ist zusätzlich zu beachten, dass sich die Einwilligung ausdrücklich auf diese Daten beziehen muss.

d. Verarbeitung auf der Grundlage von Kollektivvereinbarungen

Eine Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis kann auch auf der Grundlage von Kollektivvereinbarungen erfolgen.

e. Einhaltung der Grundsätze der DSGVO

Der Verantwortliche muss geeignete Maßnahmen ergreifen um sicherzustellen, dass die Grundsätze der Datenschutz-Grundverordnung, insbesondere diejenigen des Art. 5 DSGVO, eingehalten werden.

f. Beschäftigte im Sinne des Gesetzes

Beschäftigte im Sinne des § 26 BDSG neu sind:

- Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,
- zu ihrer Berufsbildung Beschäftigte,
- Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
- in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
- Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten,
- Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
- Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte.

18. Sanktionen

Auch wenn die beschriebenen Regeln des zukünftigen Datenschutzrechtes auf den ersten – und auch auf den zweiten – Blick verwirrend erscheinen, muss jedes Unternehmen eine Tatsachengrundlage schaffen, welche Regeln greifen. Denn: auch nach der DSGVO kann die Einhaltung der rechtlichen Vorgaben durch verschiedene Stellen nachgehalten und einer – im Zweifel auch gerichtlichen – Überprüfung zugeführt werden. Bei Verstößen gegen das Datenschutzrecht drohen empfindliche Bußgelder, im schlimmsten Fall bis zu 20 Mio. EUR bzw. 4% des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist. Außerdem stehen den Aufsichtsbehörden Untersuchungs-, Abhilfe- und Genehmigungsbefugnisse zu.

Eine unmittelbare Kontrolle durch die Aufsichtsbehörden gerade in mittelständischen Betrieben bereits am 26.05.2018 scheint unrealistisch, wenn auch nicht ausgeschlossen. Dennoch sollte sich jedes Unternehmen auf den stetigen Anstieg der Kontrollen der Datenschutzaufsichtsbehörden einstellen. Eine Auseinandersetzung mit den neuen Datenschutzvorschriften ist damit unerlässlich.

Bußgeldbewährt ist nach Art. 83 DSGVO zunächst ein Verstoß gegen die Pflichten, die bei der Verarbeitung personenbezogener Daten entstehen – die Pflicht zur Erstellung eines Verzeichnis der Verarbeitungstätigkeiten, die Pflicht zur Bestellung eines

Datenschutzbeauftragten oder die Pflicht zur Erstellung einer Datenschutz-Folgenabschätzung seien in diesem Zusammenhang nur beispielhaft erwähnt.

Weiterhin können Verstöße gegen die in den Art. 5, 6, 7, 9 DSGVO aufgestellten Grundprinzipien geahndet werden. Eine Verarbeitung personenbezogener Daten muss damit zu jedem Zeitpunkt rechtmäßig und die ggf. erteilte Einwilligung des Betroffenen zur Verarbeitung seiner personenbezogenen Daten formell einwandfrei erfolgt sein. Zudem sind die Sondervorschriften im Zusammenhang mit der Verarbeitung besonderer Kategorien von Daten nach Art. 9 DSGVO zu beachten.

Achtung: In jedem Fall müssen auch die Regeln des BDSG neu beachtet werden, denn auch ein Verstoß gegen nationale Vorschriften kann ein Bußgeld nach Art. 83 Abs. 5 d) DSGVO zur Folge haben.

Zudem müssen die Anweisungen der Datenschutzbehörden befolgt werden, da auch eine Zuwiderhandlung bzw. Nichtbeachtung dieser eine Bußgeld auslösen kann, Art. 83 Abs. 5 e), Abs. 6 DSGVO.

Schließlich müssen die Betroffenenrechte eingehalten werden (Informations-, Löschungs- oder Berichtigungspflichten), da auch hier ein Bußgeld nach Art. 83 Abs. 5 b) DSGVO verhängt werden kann.

Achtung: Hier zeigt sich die Wichtigkeit einer gründlichen Dokumentation interner Datenverarbeitungsvorgänge. Dies auch in den Fällen, in denen ein Unternehmen nicht direkt zur Dokumentation verpflichtet ist. Nur so lassen sich bspw. rechtmäßig erteilte Einwilligungen oder auf Anfrage des Betroffenen veranlasste Lösch- oder Berichtigungsvorgänge einwandfrei gegenüber der Datenschutzbehörde nachweisen und somit Bußgelder vermeiden.

In den meisten Fällen dürften Aktennotizen bzw. ein Eintrag in elektronische Dokumente ausreichend sein. In umfassenderen Fällen empfehlen sich spezielle Datenschutzprogramme.