HERTING OBERBECK
DATENSCHUTZKANZLEI

Das neue Datenschutzrecht

55 Antworten zur Datenschutz-Grundverordnung

und zum Bundesdatenschutzgesetz 2018

November 2017
Version 1.4

Kontakt

DATENSCHUTZKANZLEI
Herting Oberbeck Rechtsanwälte Partnerschaft
Sillemstraße 60a, 20257 Hamburg

Telefon	+49 (0)40 228 691 140
E-Mail	info@datenschutzkanzlei.de
Twitter	@hertingoberbeck
Web	https://www.datenschutzkanzlei.de

Vorwort

Liebe Leserin, lieber Leser,

am 24.05.2016 ist die Europäische Datenschutz-Grundverordnung in Kraft getreten - seitdem tickt die Uhr. Am 30.06.2017 wurde nun auch das neue Bundesdatenschutzgesetz veröffentlicht, das für deutsche Unternehmen parallel anzuwenden ist. Wir befinden uns bereits in der „heißen Phase“, in der sich Unternehmen auf das neue Datenschutzrecht vorbereiten müssen. Denn am 25.05.2018 werden die neuen Gesetze schlagartig zur Anwendung kommen und dann sollten Sie vorbereitet sein. Auch wenn nicht alles neu ist und viele Unternehmen bereits auf etablierte Datenschutzkonzepte zurückgreifen können, ist die verbleibende Zeit knapp.

Mit den vorliegenden 55 Antworten (genau genommen sind es ca. 60) möchten wir Ihnen einen ersten Einstieg und Überblick in das neue Datenschutzrecht ermöglichen. Wir haben unsere Erfahrungen aus der anwaltlichen Beratung im Datenschutzrecht und aus der Tätigkeit als externe betriebliche Datenschutzbeauftragte einfließen lassen. Mit Risikoeinschätzungen und wertvollen Praxis-Tipps ordnen wir die Neuerungen für Sie ein.

Ein großer Dank gilt unseren juristischen Mitarbeitern Hanno Dormagen und Phillip Malinowski, die an der Erstellung der „55 Antworten“ mitgewirkt haben.

Es ist unser Ziel, dieses Whitepaper regelmäßig zu aktualisieren und sukzessive auszubauen. Die erste Version haben wir im Oktober 2016 veröffentlicht. In der hier vorliegenden vierten Überarbeitung haben wir die Anforderungen des neuen Bundesdatenschutzgesetzes aufgenommen und die Darstellung um nützliche weiterführende Informationen der Datenschutz-Aufsichtsbehörden, Datenschutzgremien und Fachverbände ergänzt.

Die aktuellste Version finden Sie stets im Internet unter www.datenschutzkanzlei.de/dsgvo.Dort können Sie sich auch für unseren Newsletter „Datenschutz-Update“ anmelden und so sicherstellen, dass Ihnen keine neue Version und keine wesentliche Entwicklung im Datenschutz entgehen. Wir freuen uns auf Ihren Besuch!

Hamburg im November 2017

Ihr Team der Datenschutzkanzlei

Inhaltsverzeichnis

Kontakt 1
Vorwort 2
Grundsatzfragen 6
Was ist die DSGVO? 6
Was ist das BDSG-neu? 6
DSGVO oder BDSG-neu - was gilt ab dem 25. Mai 2018? 6
Herrscht jetzt einheitlicher Datenschutz in Europa? 6
Für wen gelten die neuen Bestimmungen? 7
Wer ist „Verantwortlicher“ 8
Was bedeutet „Verarbeitung“ von Daten? 8
Was sind personenbezogene Daten? 8
Welche Grundsätze liegen der Verordnung zugrunde? 9
Was bedeutet die „Rechenschaftspflicht“ für die Praxis? 10
Verarbeitung von personenbezogenen Daten 11
Wann dürfen personenbezogene Daten verarbeitet werden? 11
Welche Besonderheiten gelten bei der Einwilligung eines Betroffenen? 12
Was gilt bei Einwilligungen von Kindern? 12
Wann ist eine Datenverarbeitung für die Erfüllung eines Vertrags „erforderlich“? 13
Wann liegt ein „berechtigtes Interesse“ zur Datenspeicherung vor? 13
Was gilt bei besonders sensiblen Daten? 14
Wann haben Betroffene ein Widerrufsrecht? 15
Wann haben Betroffene ein Widerspruchsrecht? 15
Was ändert sich bei der Datenverarbeitung im Gegensatz zur alten Rechtslage? 15
Auftragsverarbeitung 16
Wann liegt eine Auftragsverarbeitung vor? 16
Unter welchen Voraussetzungen ist Auftragsverarbeitung zulässig? 16
Welche Form muss der Vertrag mit einem Auftragsverarbeiter haben? 17
Welche Pflichten treffen den Auftraggeber? 17
Welche Pflichten treffen den Auftragsverarbeiter? 17
Was bedeuten die neuen Regelungen für die Praxis? 18
Betroffenenrechte 20
Welche Informationspflichten müssen beachtet werden? 20
Was gilt, wenn Daten nicht direkt erhoben werden? 21

Gibt es Ausnahmen von der Informationspflicht? 21
Was müssen Unternehmen formell beachten? 21
Welche Auskunftsrechte haben Betroffene nach DSGVO? 22
Wann müssen Informationen dauerhaft gelöscht werden? 23
Was ist mit Daten, die (noch) nicht gelöscht werden können? 24
Was bedeutet das Recht auf Datenübertragbarkeit? 25
Was bedeuten die Neuerungen für die Praxis? 26
Dokumentationspflicht 27
Welche Informationen muss das Verzeichnis enthalten? 27
Welche Form muss das Verzeichnis haben? 28
Wer ist für die Führung des Verzeichnisses verantwortlich? 29
Gibt es Ausnahmen für kleine und mittlere Unternehmen? 29
Was bedeuten die neuen Regelungen für die Praxis? 29
Datenschutz-Folgenabschätzung 31
Wann ist eine Datenschutz-Folgenabschätzung vorzunehmen? 31
Wie ist die Datenschutz-Folgenabschätzung konkret umzusetzen? 32
Was ist zu tun, wenn ein erhöhtes Risiko festgestellt wird? 33
Was bedeuten die neuen Regelungen für die Praxis? 33
Technischer Datenschutz 35
Was müssen Unternehmen bei „Privacy by Design/Default“ beachten? 35
Welche technischen Sicherheitsvorkehrungen müssen beachtet werden? 35
Was bedeuten die neuen Regelungen für die Praxis? 36
Pflichten bei Datenpannen 38
Wann liegt eine Datenpanne vor? 38
Welche Informationen sind der Aufsichtsbehörde zu übermitteln? 38
In welchen Fällen müssen auch die Betroffenen benachrichtigt werden? 39
Welche Informationen müssen in diesen Fällen an Betroffene übermittelt werden? 40
Inwieweit müssen Datenpannen dokumentiert werden? 40
Was bedeuten die neuen Regelungen für die Praxis? 41
Datenschutzbeauftragter 42
Wann muss ein Datenschutzbeauftragter benannt werden? 42
Was gilt für Konzerne und Unternehmensgruppen? 44
Was sind die Aufgaben des Datenschutzbeauftragten? 44
Welche Voraussetzungen muss der Datenschutzbeauftragte erfüllen? 45
Interner und externer Datenschutzbeauftragter? 45

Wie läuft die Zusammenarbeit mit dem Datenschutzbeauftragten? 46
Was bedeuten die neuen Regelungen für die Praxis? 47
Datenübermittlung in Drittstaaten 48
Wann ist eine Datenübermittlung in Drittstaaten gerechtfertigt? 48
Was bedeuten die neuen Regelungen für die Praxis? 50
Gesetzestexte (Links) 51
Unsere Leistungen im Datenschutzrecht 52

Grundsatzfragen

Was ist die DSGVO?

Die EU-Datenschutz-Grundverordnung (DSGVO) soll den Datenschutz, also den Umgang mit personenbezogenen Daten durch öffentliche Stellen und private Unternehmen, vereinheitlichen und den freien Datenverkehr innerhalb des europäischen Binnenmarkts gewährleisten.

Die DSGVO ist bereits am 24. Mai 2016 in Kraft getreten. Sie gilt allerdings erst ab dem 25. Mai 2018 und löst zu diesem Zeitpunkt die EU-Datenschutzrichtlinie (95/46/EG) ab, auf der das bisherige Bundesdatenschutzgesetz (BDSG-alt) beruht.

Was ist das BDSG-neu?

Das neue Bundesdatenschutzgesetz (BDSG-neu) greift die Vorgaben der DSGVO auf und erweitert diese im Rahmen sogenannter „Öffnungsklauseln".

Das BDSG-neu wurde am 27. April 2017 als Artikel 1 des Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (DSAnpUGEU) vom deutschen Bundestag beschlossen, hat am 12. Mai 2017 vom Bundesrat Zustimmung erhalten und wurde am 30. Juni 2017 im Bundesgesetzblatt veröffentlicht. Das BDSG-neu entfaltet zeitgleich mit der DSGVO seine Wirkung, also ab dem 25. Mai 2018.

Das BDSG-neu besteht aus vier Teilen. Für die Konkretisierung der DSGVO sind lediglich Teil 1 und Teil 2 interessant. Teil 1 enthält allgemeine Bestimmungen und Grundlagen. Teil 2 umfasst die tatsächliche Ergänzung der DSGVO und ist in der Struktur der DSGVO angepasst.

DSGVO oder BDSG-neu - was gilt ab dem 25. Mai 2018?

Kurz gesagt: beides! Grundlage bildet die DSGVO. Diese wirkt unmittelbar in allen europäischen Mitgliedstaaten und genießt als Unionsrecht den Anwendungsvorrang vor nationalem Recht. Dies folgt aus der Rechtsprechung des Europäischen Gerichtshofs (EuGH) und ergibt sich auch aus § 1 Abs. 5 BDSG-neu. Darüber hinaus regelt das BDSG-neu spezielle Vorschriften für Deutschland, welche durch die DSGVO im Rahmen sog. „Öffnungsklauseln" bewusst offengelassen oder nicht abschließend geregelt wurden.

Herrscht jetzt einheitlicher Datenschutz in Europa?

Leider nicht ganz. Trotz der Intention der DSGVO, das europäische Datenschutzrecht weitgehend zu vereinheitlichen, bestehen immer noch eine Reihe von Möglichkeiten für die Mitgliedstaaten, eigene Vorschriften zu erlassen.

Die ergänzenden Regelungen in Deutschland machen es in der Praxis nicht gerade einfacher. Das BDSG-neu enthält z.B. detaillierte Regelungen zum Beschäftigtendatenschutz, zur Videoüberwachung und zum Profiling. Zudem wurden die Vorgaben für den betrieblichen Datenschutzbeauftragten aus dem BDSG-alt übernommen, so dass Unternehmen in Deutschland in der Regel weiterhin ab 10 Beschäftigten einen Datenschutzbeauftragten benennen müssen.

Die Datenschutzaufsichtsbehörden und einige Datenschutzexperten vertreten die Meinung, dass das BDSG-neu den Handlungsspielraum der Öffnungsklauseln überschritten habe und damit EU-rechtswidrig sei. Für Unternehmen führt das zu erheblicher Rechtsunsicherheit bei der Umsetzung der neuen Bestimmungen.

Der Gesetzgeber wird sich wohl als nächstes mit weiteren Datenschutzbestimmungen in Spezialgesetzen beschäftigen (z.B. TMG).

Zudem gibt es Gremien wie die Datenschutzkonferenz und den Düsseldorfer Kreis, über den sich die deutschen Aufsichtsbehörden abstimmen und praktische Orientierungshilfen veröffentlichen. Ein ähnliches Gremium auf europäischer Ebene stellen die Artikel-29-Gruppe bzw. der Europäische Datenschutzausschuss dar, über den sich die Aufsichtsbehörden der Mitgliedstaaten abstimmen und ebenfalls Orientierungshilfen sowie Leitlinien und Vorlagen zu gewissen Instrumenten der DSGVO erlassen. Letztlich ist auch immer mit dem Europäischen Gerichtshof (EuGH) zu rechnen, der in der Vergangenheit bereits das europäische Datenschutzrecht maßgeblich geprägt hat.

> **Praxis-Tipp**
> Nutzen Sie die Leitlinien, Praxishilfen, Kurzpapiere und Vorlagen der Datenschutzbehörden, Datenschutzgremien und Fachverbände. Links und Fundstellen finden Sie in diesem Whitepaper.

Für wen gelten die neuen Bestimmungen?

Die DSGVO und das BDSG-neu gelten zum einen für Verantwortliche und Auftragsverarbeiter, die im Rahmen der Tätigkeit einer Niederlassung in der Union Daten verarbeiten, Art. 3 Abs. 1 DSGVO / § 1 Abs. 4 Nr. 1, 2 BDSG-neu (Niederlassungsprinzip). In Deutschland ansässige Unternehmen sind daher nahezu vollständig vom Geltungsbereich der DSGVO und des BDSG-neu erfasst.

Darüber hinaus gilt aber auch das sogenannte „Marktortprinzip“: Auch für Verantwortliche und Auftragsverarbeiter, die keine Niederlassung in der EU betreiben, gilt die DSGVO, wenn sie ihre Waren und Dienstleistungen Betroffenen in der Union anbieten (Art. 3 Abs. 2 lit. a) DSGVO / § 1 Abs. 4 Nr. 3 BDSG-neu).

Kurzpapier der Datenschutzkonferenz zum Marktortprinzip:
https://www.lda.bayern.de/media/dsk_kpnr_7_marktortprinzip.pdf

Wer ist „Verantwortlicher“

Adressat der DSGVO und des BDSG-neu ist hauptsächlich der „Verantwortliche“. Das ist gemäß Art. 4 Nr. 7 DSGVO diejenige natürliche oder juristische Person, Behörde oder Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Was bedeutet „Verarbeitung“ von Daten?

Der Begriff der Verarbeitung ist denkbar weit gefasst. Jeder irgendwie geartete Umgang mit den Daten eröffnet den Anwendungsbereich der Verordnung. Gemäß Art. 4 Nr. 2 DSGVO ist eine Verarbeitung:

> *„jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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 Weitergabe durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Vergleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“.*

Ausreichend wäre damit bereits das Zwischenspeichern im Cache eines Browsers. Einzig unstrukturierte Akten oder Aktensammlungen fallen aus dem Anwendungsbereich, sind für die betriebliche Praxis aber kaum spielentscheidend.

Was sind personenbezogene Daten?

„Personenbezogenen Daten“ sind gemäß Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Identifizierbar ist eine natürliche Person,

> *„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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.“*

Es liegen somit in der Regel auch dann personenbezogene Daten vor, wenn die Informationen unter Zuhilfenahme weiterer verfügbarer Daten und technischer Mittel einer bestimmten Person zugeordnet werden können. Dies ist etwa bei Telefonnummern, KFZ-Kennzeichen, Kundennummern und auch IP-Adressen der Fall. Der Anwendungsbereich der DSGVO und des

BDSG-neu endet erst da, wo eine solche Zuordnung auch mit größtmöglichem Aufwand nicht möglich ist.

> Unterschied zum BDSG-alt
> Der Begriff der personenbezogenen Daten ist damit weiter gefasst als im bisherigen deutschen Recht. Denn gemäß § 3 BDSG-alt liegen bereits dann keine personenbezogenen Daten vor, wenn eine Verknüpfung nur mit „unverhältnismäßig großem Aufwand“ möglich wäre. Eine entsprechende Regelung sieht die DSGVO nicht vor. Da eine absolute Anonymisierung selten ist (selbst komplexe Verschlüsselungsalgorithmen können theoretisch geknackt werden), wird ein Herausfallen aus dem Regelungsbereich wohl seltener werden.

Welche Grundsätze liegen der Verordnung zugrunde?

Die Speicherung und Nutzung personenbezogener Daten muss sich gemäß Art. 5 Abs. 1 DSGVO an folgenden Grundsätzen orientieren:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
  Daten müssen rechtmäßig erhoben und nachvollziehbar für betroffene Person verarbeitet werden.

- Zweckbindung
  Daten wurden für festgelegte, eindeutige und legitime Zwecke erhoben und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

- Datenminimierung
  Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.
- Richtigkeit
  Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Andernfalls sind sie zu löschen.

- Speicherbegrenzung
  Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

- Integrität und Vertraulichkeit
  Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter

Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Risiko-Radar
Die Grundsätze der Datenverarbeitung sind mehr als bloße Programmsätze. Bei Verletzung drohen Geldbußen von bis zu 20.000.000 EUR oder bis zu 4% des gesamten weltweit erzielten Vorjahresumsatzes Ihres Unternehmens, je nachdem, was höher ist.

Was bedeutet die „Rechenschaftspflicht" für die Praxis?

Verantwortliche sind gemäß Art. 5 Abs. 2 DSGVO für die Einhaltung der dargestellten Grundsätze zur Verarbeitung personenbezogener Daten verantwortlich und müssen dessen Einhaltung nachweisen können (**Rechenschaftspflicht/Accountability**). Nach Ansicht der Datenschutzkonferenz soll die Rechenschaftspflicht das Vorliegen von Einwilligungen, den ordnungsgemäßen Ablauf der Verarbeitung und das Ergebnis der Datenschutz-Folgenabschätzung beinhalten und konkret darstellen.

Es sind daher umfangreiche Dokumentationen erforderlich, unter anderem über die Verarbeitungen personenbezogener Daten, den Zweck und die Rechtsgrundlage der einzelnen Verarbeitungen, die Schaffung wesentlicher Datenschutz-Prozesse und Entscheidungsgrundlagen. Unternehmen kommen also nicht daran vorbei, den Datenschutz zukünftig aktiv zu managen und wirksame Datenschutzkonzepte/ Datenschutz-Managementsysteme (DSMS) einzuführen.

Praxis-Tipp
Unternehmen sind gut beraten, ein wirksames Datenschutz-Managementsystem (DSMS) einzuführen, welches sich an den Risiken der im Unternehmen verarbeiteten personenbezogenen Daten ausrichtet. Ein rein reaktiver Umgang mit Datenschutz-Themen dürfte der Vergangenheit angehören. Zukünftig ist aktives Datenschutz-Management gefragt, um Haftungsrisiken zu minimieren.

Praxishilfe des GDD zur Accountability:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_9.pdf

Verarbeitung von personenbezogenen Daten

Art. 6 DSGVO, §§ 22ff. BDSG-neu

Zentraler Anknüpfungspunkt der DSGVO sind die „personenbezogenen Daten“. Wenn Informationen demnach Rückschluss auf eine natürliche Person zulassen, dürfen diese nicht verarbeitet werden. Dieses Verbot wird aber sogleich entschärft, indem eine Reihe von Fällen aufgelistet wird, in denen eine Verarbeitung ausnahmsweise zulässig ist. Man spricht daher von einem „Verbot mit Erlaubnisvorbehalt“, welches aus § 4 BDSG-alt bekannt ist. Für Unternehmen relevant sind vor allem die Datenverarbeitungen auf Grundlage einer **Einwilligung**, zur **Erfüllung eines Vertrages** und auf Grundlage eines **berechtigten Interesses**.

Risiko-Radar

Als Unternehmen müssen sie beachten, dass bei rechtswidriger Verarbeitung personenbezogener Daten Geldbußen von bis zu 20.000.000 EUR oder bis zu 4% des gesamten weltweit erzielten Vorjahresumsatzes ihres Unternehmens drohen, je nachdem, was höher ist.

Wann dürfen personenbezogene Daten verarbeitet werden?

Eine Verarbeitung ist gemäß Art. 6 DSGVO nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Welche Besonderheiten gelten bei der Einwilligung eines Betroffenen?

Für die Wirksamkeit einer Einwilligung eines Betroffenen in eine Datenverarbeitung sieht Art. 7 DSGVO besondere Voraussetzungen vor. Danach besteht im Falle einer Einwilligung des Betroffenen eine Nachweispflicht des Verantwortlichen. Weiterhin ist auf Transparenz (verständliche und einfache Sprache, klare Unterscheidbarkeit von anderen Sachverhalten) zu achten.

Eine Erleichterung für Unternehmen besteht zukünftig darin, dass sich die DSGVO von der Schriftform verabschiedet. Im BDSG war die Schriftform in den meisten Fällen vorgesehen, mit Ausnahmen beispielsweise für die elektronische Einwilligung im E-Commerce. Durch den Wegfall des generellen Schriftformerfordernisses könnten zukünftig auch im Offline-Bereich alternative Einwilligungserklärungen eingeholt werden. Allerdings liegt die Beweislast für das Vorliegen der Einwilligung weiterhin bei den Unternehmen.

Eine Neuerung ist das ausdrücklich erwähnte **Kopplungsverbot**: Eine Einwilligung kann demnach als nicht freiwillig erfolgt gelten, wenn sie in Hinsicht auf solche personenbezogenen Daten erfolgt, die für die eigentliche Vertragserfüllung nicht erforderlich sind.

> **Praxis-Tipp**
> Das „Kopplungsverbot“ ist zwar bereits im BDSG erwähnt, erlangt aber durch die schärfere Formulierung in Art. 7 Abs. 4 DSGVO eine neue Bedeutung. Gerade in den Fällen, in denen für eine Online-Dienstleistung als „Gegenleistung“ eine Einwilligung zu einer Verarbeitung von Daten ohne direkten inhaltlichen Bezug gefordert wird, könnten zukünftig Zweifel an der Wirksamkeit entstehen.

Kurzpapier des BayLDA zur Einwilligung nach der DSGVO:
https://www.lda.bayern.de/media/baylda_ds-gvo_9_consent.pdf

Was gilt bei Einwilligungen von Kindern?

Weitere Einschränkungen nimmt Art. 8 Abs. 1 DSGVO bei Diensten der Informationsgesellschaft an Kinder vor. Bei diesen muss eine Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt werden. Zugleich müssen unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen unternommen werden, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde.

Die vorgesehene Altersgrenze liegt bei 16 Jahren, kann aber von den nationalen Gesetzgebern der Mitgliedstaaten auf bis zu 13 Jahre herabgesetzt werden (Öffnungsklausel). Der deutsche Gesetzgeber hat keine Herabsetzung vorgenommen, so dass die Altersgrenze von 16 Jahren

gilt. Für Unternehmen, die in mehreren EU-Ländern aktiv sind, stellt sich nun die Herausforderung, für jeden Markt die dort geltende Altersgrenze zu prüfen und einzuhalten.

Kurzpapier des BayLDA zur Einwilligung eines Kindes:
https://www.lda.bayern.de/media/baylda_ds-gvo_15_childs_consent.pdf

Wann ist eine Datenverarbeitung für die Erfüllung eines Vertrags „erforderlich“?

Eine Datenverarbeitung ist beispielsweise zur Erfüllung eines Vertrages erforderlich, wenn die Speicherung und Verarbeitung von Kundendaten zur Durchführung einer Warenbestellung benötigt wird. Denn ohne diese Form der Verarbeitung kann die Ware weder verschickt werden noch können mögliche Nachfragen des Kunden beantwortet werden. Selbst wenn ein Kunde nur Informationen zu der Ware anfordert, ohne aber eine Bestellung aufzugeben, kann eine Speicherung seiner Daten erforderlich sein (Datenverarbeitung zur Durchführung vorvertraglicher Maßnahmen). In beiden Fällen ist jedoch auch hier das Zweckbindungsgebot zu beachten: Eine Verarbeitung, die über den Zweck der Versendung der Ware bzw. Kontaktaufnahme zum Kunden herausgeht, bedarf einer eigenen Rechtfertigung, da sie für den ursprünglichen Zweck nicht erforderlich ist. Über den Zweck der Datenspeicherung muss der Unternehmer zudem ausdrücklich informieren.

Wann liegt ein „berechtigtes Interesse“ zur Datenspeicherung vor?

Die Mehrzahl der Datenverarbeitungen von Unternehmen wird in Zukunft wohl über die Klausel des „berechtigten Interesses“ vorgenommen werden. Bei dieser Auffangregelung soll eine Abwägung zwischen legitimen Zwecken des Verarbeitenden einerseits und dem Interesse des Betroffenen am Erhalt seiner Privatsphäre andererseits erfolgen. Bei der Abwägung ist zu berücksichtigen, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Eine Interessenabwägung dieser Art ist bereits aus dem deutschen Recht bekannt, § 28 Abs. 1 S. 1 Nr. 2 BDSG-alt. Vorerst kann sich deshalb auch an der entsprechenden Rechtsprechung orientiert werden.

Ein überwiegendes berechtigtes Interesse liegt zum Beispiel dann vor, wenn ein Unternehmen in Folge einer nicht bezahlten Rechnung den Hinweis speichert, an einen Kunden in Zukunft nur gegen Vorkasse zu versenden. Besonders relevant für Unternehmen ist zudem, dass Erwägungsgrund 47 der DSGVO auch die Verarbeitung zum Zwecke der Direktwerbung als berechtigtes Interesse erwähnt. Die postalische Werbung kann demnach wohl weiterhin ohne Einwilligung des Betroffenen erfolgen. Beim E-Mail- und Telefon-Marketing sind jedoch zusätzlich die Anforderungen des UWG zu beachten, welche eine ausdrückliche Einwilligung des Betroffenen einfordern.

Ein berechtigtes Interesse können auch Verantwortliche haben, die Teil einer Unternehmensgruppe sind und personenbezogene Daten innerhalb dieser Unternehmensgruppe für interne Verwaltungszwecke gegenseitig übermitteln **(„kleines Konzernprivileg“** aus DSGVO-Erwägungsgrund 48). Davon unberührt bleibt allerdings der Datentransfer an Unternehmensteile in Drittländern (etwa die USA).

Kurzpapier der Datenschutzkonferenz zur Verarbeitung personenbezogener Daten für Werbung: https://www.lda.bayern.de/media/dsk_kpnr_3_werbung.pdf

Kurzpapier des BayLDA zur Verarbeitung personenbezogener Daten für Werbung: https://www.lda.bayern.de/media/baylda_ds-gvo_12_advertising.pdf

Was gilt bei besonders sensiblen Daten?

Eine strengere Regelung sieht die DSGVO hinsichtlich „besonderer Kategorien“ personenbezogener Daten vor. Hierbei handelt es sich um Informationen, die sich auf besonders grundrechtssensible Bereiche beziehen. Die abschließende Aufzählung umfasst Daten, 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.

Für die Verarbeitung dieser Daten gilt ebenfalls das „Verbot mit Erlaubnisvorbehalt“, wobei Art. 9 Abs. 2 DSGVO und § 22 Abs. 1 BDSG-neu eigenständige, enger gefasste Rechtfertigungsgründe enthalten. Diese betreffen neben der auch hier möglichen Einwilligung des Betroffenen vor allem Einrichtungen im Gesundheits- und Sozialbereich und Fälle, in denen ein Verantwortlicher zur Erfüllung rechtlicher Pflichten auf diese Daten angewiesen ist. So ist beispielsweise nach Art. 9 Abs. 2 lit. b) DSGVO ein Arbeitgeber weiter berechtigt, die unter anderem für die Gehaltsabrechnung erforderlichen Angaben zu Familienstand, Kinderzahl und Religion sowie krankheitsbedingte Fehlzeiten der Mitarbeiter zu speichern.

Die Mitgliedsstaaten haben vor allem hinsichtlich der Rechtmäßigkeit der Verarbeitung von Mitarbeiterdaten weiterhin einen eigenen Gestaltungsspielraum. Die bereits aus § 32 BDSG bekannten Grundsätze bei der Verarbeitung sensibler Daten im Arbeitsverhältnis wurden in § 26 BDSG-neu übergenommen.

Kurzpapier des BayLDA zu besonderen Kategorien personenbezogener Daten: https://www.lda.bayern.de/media/baylda_ds-gvo_6_special_categories.pdf

Praxis-Tipp
Bei der Verarbeitung sensibler Daten sollte mit besonderer Vorsicht vorgegangen und geprüft werden, ob diese zu den „besonderen Kategorien“ personenbezogener Daten gehören. Neu ist z.B. die Aufnahme biometrischer Informationen, welche bis dato nicht als sensible Daten vom BDSG erfasst waren.

Wann haben Betroffene ein Widerrufsrecht?

Eine Einwilligung eines Betroffenen kann gemäß Art. 7 Abs. 3 DSGVO jederzeit widerrufen werden. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit zukünftiger, nicht aber bereits erfolgter Verarbeitungen aufgehoben. Formell ist zu beachten, dass es möglich sein muss, den Widerruf so einfach wie die Erteilung der Einwilligung auszuüben.

Wann haben Betroffene ein Widerspruchsrecht?

Nach Art. 21 Abs. 1 DSGVO besteht ein Widerspruchsrecht insbesondere bei einer Datenverarbeitung, die sich auf berechtigte Interessen (Art. 6 Abs. 1 lit. f) DSGVO) beruft. Der Datenverarbeiter darf dann nur weiterverarbeiten, wenn er „zwingende Gründe“ für die Verarbeitung nachweisen kann (selten!). Dafür trägt er zudem die Darlegungs- und Beweislast. Ohne jede Begründung können Betroffene gemäß Art. 21 Abs. 2 DSGVO widersprechen, wenn die Datenverarbeitung zum Zwecke des Direktmarketings erfolgt.

Auf das Widerspruchsrecht ist der Betroffene spätestens mit der ersten Kommunikation hinzuweisen (Art. 21 Abs. 4 DSGVO).

Was ändert sich bei der Datenverarbeitung im Gegensatz zur alten Rechtslage?

Bei der Rechtmäßigkeit der Verarbeitung personenbezogener Daten weicht die DSGVO nicht groß vom bisher geltenden deutschen Datenschutzrecht ab. Die weite Formulierung der „berechtigten Interessen“ scheint eine Erleichterung für Unternehmen zu sein, schafft aber zunächst Rechtsunsicherheit. Hier ist auf eine zügige Klarstellung durch den EuGH zu hoffen.

Eine Neuerung stellt zum einen das umfangreiche Widerrufsrecht und zum anderen die ausdrückliche Regelung eines „Kopplungsverbots“ bei Einwilligungen dar. Bei einer Verbindung einer Einwilligung mit einem Vertragsangebot ist in Zukunft neben einem Augenmerk auf Transparenz und Verständlichkeit besonders darauf zu achten, dass kein unzulässiger Druck auf den Vertragspartner ausgeübt wird.

Auftragsverarbeitung

Art 28 DSGVO

Die Verarbeitung personenbezogener Daten in einem Unternehmen wird oftmals ganz oder zum Teil von Dritten, sogenannten Auftragsverarbeitern, übernommen. Die Voraussetzungen für diese Zusammenarbeit werden sich nach der DSGVO in einigen Punkten ändern. Wurde der Auftragsverarbeiter bisher als der Organisation des Verantwortlichen zugehörig behandelt, ist dies nun umstritten. So wird die Meinung vertreten, dass auch bei der Auftragsverarbeitung jede Weitergabe von Daten einer eigenständigen Rechtfertigung bedürfe. Diese Meinung scheint aber nicht praxisgerecht, da in diesem Fall beispielsweise Gesundheitsdaten kaum im Wege der Auftragsverarbeitung durch Dienstleister verarbeitet werden könnten. Im Ergebnis bleibt es somit bei der Privilegierung der Auftragsverarbeitung gegenüber den herkömmlichen Voraussetzungen der Datenübermittlung.

Risiko-Radar

Auftragsverarbeitern drohen gemäß Art 83 Abs. 4 lit a) DSGVO Geldbußen von bis zu 10.000.000 EUR oder bis zu 2% des gesamten weltweit erzielten Vorjahresumsatzes des Unternehmens, wenn sie ihren Pflichten als Auftragsverarbeiter nicht nachkommen. Auftragsverarbeiter drohen zukünftig auch Schadenersatzforderungen von Betroffenen (Art. 82 Abs. 2 DSGVO) und von Auftraggebern (Art. 28 Abs. 4 DSGVO).

Wann liegt eine Auftragsverarbeitung vor?

Auftragsverarbeiter ist gemäß Art. 4 Nr. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Typische Fälle der Auftragsverarbeitung sind etwa die Auslagerung von Daten in die Cloud oder auch die Aktenvernichtung durch spezialisierte Dienstleister.

Unter welchen Voraussetzungen ist Auftragsverarbeitung zulässig?

Zunächst darf der Datenempfänger nicht selbst über Zweck und Mittel der Datenverarbeitung entscheiden. Die Datenverarbeitung muss daher weiterhin „weisungsgebunden“ erfolgen (Art. 28 Abs. 3 Satz 2 lit. a), Art. 29 DSGVO). Der Verantwortliche muss den Auftragsverarbeiter sorgfältig auswählen und kontrollieren. Im Gegenzug muss der Auftragsverarbeiter dem Verantwortlichen alle nötigen Informationen zum Nachweis seiner Pflichten aus Art. 28 Abs. 1 DSGVO zur Verfügung stellen. Vor Beginn der Datenverarbeitung müssen alle Rechte und Pflichten in einem Vertrag vereinbart werden. Erst im Anschluss darf die Auftragsverarbeitung beginnen.

Welche Form muss der Vertrag mit einem Auftragsverarbeiter haben?

Eine Auftragsverarbeitung bedarf eines Vertrags zwischen Auftraggeber und Auftragsverarbeiter (Art. 28 Abs. 3 DSGVO). Dieser muss schriftlich abgefasst werden, was neuerdings auch in einem elektronischen Format (z.B. korrespondierende E-Mails) erfolgen kann (Art. 28 Abs. 9 DSGVO).

Vertragsmuster des GDD zur Auftragsverarbeitung:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_4.pdf

Welche Pflichten treffen den Auftraggeber?

Erwägt ein Verantwortlicher, einen Teil der Datenverarbeitung durch Dritte vornehmen zu lassen, muss er bereits bei der Auswahl des Auftragsverarbeiters besondere Vorsicht walten lassen. Gemäß Art. 28 Abs. 1 DSGVO darf ein Verantwortlicher nur dann einen Auftragsverarbeiter verpflichten, wenn dieser hinreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet ist. Die DSGVO sieht zu diesem Zweck eine mögliche Vereinbarung von Verhaltensregeln etwa durch Verbände und andere Vereinigungen vor, deren Einhaltung Auftragsverarbeiter als geeignete Garantie vertraglich zusichern könnten. Zudem können entsprechende Zertifizierungen eine hinreichende Gewähr bieten (Art. 42 DSGVO).

Der Verantwortliche muss zudem gemeinsam mit dem Auftragsverarbeiter darauf hinwirken, dass durch geeignete technische und organisatorische Maßnahmen ein angemessenes Schutzniveau für die betroffenen Personen gewährleistet ist (Art. 32 DSGVO).

Welche Pflichten treffen den Auftragsverarbeiter?

Die Artikel 28 – 34 DSGVO enthalten eine Vielzahl von Pflichten für den Auftragsverarbeiter. Die wichtigsten werden im Folgenden dargestellt:

- Der Auftragsverarbeiter darf nur aufgrund dokumentierter Weisungen des Auftraggebers personenbezogene Daten verarbeiten (Art. 28 Abs. 3 Satz 2 lit. a) DSGVO).

- Auftraggeber und Auftragsverarbeiter müssen geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko für die Rechte und Freiheiten Betroffener angemessenes Schutzniveau zu gewährleisten (Art. 32 DSGVO). Dazu zählt:

    - Die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

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

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

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

- Die Bestellung eines Unterauftragsverarbeiters bedarf einer schriftlichen Genehmigung des Verantwortlichen. Im Fall einer allgemeinen schriftlichen Genehmigung muss der Verantwortliche darüber hinaus über entsprechende Vorgänge informiert werden (Art. 28 Abs. 2 DSGVO). Für den Vertrag mit einem Unterauftragnehmer sieht Art. 28 Abs. 4 DSGVO zudem weitere Voraussetzungen vor, die eine Datensicherheit auch in diesem Verhältnis garantieren sollen. Der Auftragsverarbeiter ist dabei auch selbst für eine Einhaltung dieser Vorgaben verantwortlich.

- Der Auftragsverarbeiter muss gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

- Alle personenbezogenen Daten müssen nach Wahl des Verantwortlichen nach Auftragsende zurückgegeben oder gelöscht werden, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

- Der Auftragsverarbeiter ist zukünftig verpflichtet, ein Verzeichnis seiner Auftraggeber zu führen (Art. 30 Abs. 2 DSGVO). Einzelheiten werden im Kapitel „Dokumentationspflicht“ beschrieben.

> **Praxis-Tipp**
> Wenn Sie personenbezogene Daten im Auftrag verarbeiten, sollten Sie die Zeit bis Mai 2018 nutzen, um Ihre Dokumentation auf Vordermann zu bringen. Die DSGVO enthält eine Reihe neuer Pflichten für Sie!

Kurzpapier des BayLDA zur Auftragsverarbeitung:
https://www.lda.bayern.de/media/baylda_ds-gvo_10_processor.pdf

Was bedeuten die neuen Regelungen für die Praxis?

Die Änderungen der Regelungen zur Auftragsverarbeitung bringen vor allem einen Mehraufwand auf Seiten des Auftragsverarbeiters mit sich. Hierzu zählt insbesondere das Führen eines

eigenen Verzeichnisses für Verarbeitungstätigkeiten. Der Verantwortliche muss weiterhin dafür Sorge tragen, nur geeignete Dienstleister zu beauftragen, und ist gefordert, deren Sicherheitsvorkehrungen vorab zu prüfen. Positiv ist, dass Verträge zukünftig elektronisch geschlossen werden können.

Umfangreicher Praxisleitfaden der IHK Nürnberg zur Auftragsverarbeitung:
https://www.ihk-nuernberg.de/de/media/PDF/Innovation-Umwelt/Datenschutz-in-der-betrieblichen-Praxis/praxisleitfaden-zur-ds-gvo.pdf

Betroffenenrechte

Art. 12 – 23 DSGVO

Die DSGVO stärkt in besonderem Maße die Rechte Betroffener einer Datenverarbeitung. Diese sollen zu jedem Zeitpunkt genauen Einblick erhalten, welche sie betreffenden Daten in welcher Weise und zu welchem Zweck verwendet werden. Gleichzeitig soll es ihnen ermöglicht werden, aktiv Einfluss auf diese Daten zu nehmen. Da die Erfüllung von Informationspflichten und die fristgemäße Beantwortung von Anfragen Betroffener zum Teil einiger Vorbereitungen bedürfen, lohnt sich eine frühzeitige Auseinandersetzung mit diesem Thema. Die wichtigsten Betroffenenrechte werden im Folgenden überblicksmäßig dargestellt.

Risiko-Radar

Werden die Betroffenenrechte nicht ordnungsgemäß gewährt, so drohen gemäß Art 83 Abs. 5 lit. b) DSGVO Geldbußen von bis zu 20.000.000 EUR oder bis zu 4% des gesamten weltweit erzielten Vorjahresumsatzes des Unternehmens.

Welche Informationspflichten müssen beachtet werden?

Eine betroffene Person muss bei jeder Verarbeitung ihrer Daten gemäß Art. 13, 14 DSGVO über eine Reihe von Informationen aufgeklärt werden. Auf diese Weise soll dem Grundsatz der Transparenz maximale Geltung verschafft werden. Die DSGVO geht an dieser Stelle zum Teil deutlich über bisherige Regelungen des BDSG und des TMG hinaus. Unterschieden wird die Erhebung beim Betroffenen selbst und die Erhebung bzw. Verarbeitung auf andere Weise.

Praxis-Tipp

Die Datenschutzerklärungen auf Webseiten müssen bis zum Stichtag entsprechend angepasst werden. Art. 13 und 14 DSGVO ersetzen dabei auch die Informationspflichten des § 13 Abs. 1 TMG.

Unsere Anleitung zur Erstellung der neuen Datenschutzerklärung:
https://www.datenschutzkanzlei.de/machen-sie-ihre-datenschutzerklaerung-fit-fuer-die-dsgvo/

Bei einer Erhebung von Daten beim Betroffenen selbst (Art. 13 DSGVO) müssen nun u.a. folgende Informationen angegeben werden:

- Genaue Kontaktdaten des Verantwortlichen, dessen Vertreter sowie des Datenschutzbeauftragten;

- Die Zwecke und die Rechtsgrundlage der Verarbeitung, bei einer Verarbeitung auf Grund eines „berechtigten Interesse“ zudem eine genaue Darlegung dessen;
- Neben der Offenlegung weiterer Empfänger der Daten insbesondere eine mögliche Weiterleitung der Daten in Drittländer (z.B. USA) sowie die Rechtsgrundlage für diese Übermittlung (z.B. bei Übermittlung an weitere Unternehmen im Konzernverbund oder an einen Cloud-Anbieter);
- Die Dauer der Speicherung der personenbezogenen Daten (z.B. 3 Jahre) oder die Kriterien der Festlegung (z.B. während der Dauer der Vertragsbeziehung);
- Eine Belehrung über sämtliche bestehende Betroffenenrechte (Auskunft, Berichtigung, Löschung, u.U. Widerspruch sowie Datenübertragbarkeit);
- Das Bestehen einer automatisierten Entscheidungsfindung (z.B. SCHUFA-Prüfung vor einer Kreditvergabe) sowie dessen Logik;
- Hinweis, ob die Bereitstellung der Daten gesetzlich oder vertraglich erforderlich ist und die Folgen der Nichtbereitstellung.

Was gilt, wenn Daten nicht direkt erhoben werden?

Nahezu identische Pflichten bestehen, wenn die Daten nicht direkt beim Betroffenen erhoben werden (Art. 14 DSGVO). Zusätzlich ist in diesem Fall noch anzugeben, aus welcher Quelle die Daten kommen (Art. 14 Abs. 2 lit. f) DSGVO) und welche Kategorien von personenbezogenen Daten betroffen sind (Art. 14 Abs. 1 lit. d) DSGVO). Der Hinweis, ob die Bereitstellung gesetzlich oder vertraglich erforderlich ist, entfällt hingegen.

Gibt es Ausnahmen von der Informationspflicht?

Die Informationspflichten bestehen nur, wenn der Betroffene nicht bereits über diese Informationen verfügt (Art. 13 Abs. 4, Art. 14 Abs. 5 lit. a) DSGVO).
Werden die Daten nicht direkt erhoben, entfällt sie auch, wenn sich die Erteilung der Information als unmöglich erweist oder unverhältnismäßigen Aufwand erfordert (z.B. Archive, Forschungszwecke), die Daten vertraulich behandelt werden müssen (z.B. zur Wahrung eines Berufsgeheimnisses) oder wenn besondere Regelungen der EU oder der Mitgliedstaaten die Erlangung oder Offenlegung ausführlich regeln und geeignete Maßnahmen zum Schutz Betroffener beinhalten.

Was müssen Unternehmen formell beachten?

Hinsichtlich der Form der Informationspflichten ist (in beiden Fällen) insbesondere Folgendes zu beachten:

- Informationen müssen präzise, leicht zugänglich sowie in klarer und einfacher Sprache abgefasst werden (z.B. in einer Erklärung auf einer Website), Art. 12 Abs. 1 DSGVO.
- Wenn sich die Verarbeitung an Kinder richtet, sollten Informationen in kindgerechter Sprache erfolgen.
- Die Übermittlung der Informationen muss schriftlich oder in anderer Form, gegebenenfalls auch elektronisch erfolgen. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.
- Ergänzend können bzw. sollten Bildsymbole verwendet werden. Diese müssen „maschinenlesbar“ sein, wenn sie in elektronischer Form dargestellt werden, Art. 12 Abs. 7 DSGVO.
- Der Hinweis auf einen möglichen Widerspruch muss getrennt dargestellt werden, Art. 21 Abs. 4 DSGVO.
- Bei einer Erhebung der Daten direkt beim Betroffenen hat die Belehrung sofort zu erfolgen, im Fall einer anderweitigen Erhebung bzw. Verarbeitung muss die Informationspflicht innerhalb einer angemessenen Frist (maximal 1 Monat) erfolgen.

Kurzpapier der Datenschutzkonferenz zu Informationspflichten:
https://www.lda.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf

Welche Auskunftsrechte haben Betroffene nach DSGVO?

Spiegelbildlich zur Informationspflicht für Verarbeitende haben Betroffene zusätzlich gemäß Art. 15 DSGVO das Recht, auf Anfrage umfangreiche Informationen über die Datenverarbeitung zu erhalten. Der Katalog dieser Informationen entspricht dabei im Wesentlichen dem der Informationspflichten aus Art. 13, 14 DSGVO. Bei der Erfüllung einer Anfrage ist folgendes zu beachten:

- Die Auskunft muss grundsätzlich unentgeltlich erfolgen; ein angemessenes Entgelt kann nur bei einer häufigen Wiederholung der Anfrage erhoben werden (Art. 12 Abs. 5 DSGVO);
- Die Informationen sind auf gängigem elektronischen Weg verfügbar zu machen, wenn die Anfrage elektronisch (z.B. E-Mail) erfolgt;
- Die Pflicht gilt nur insoweit, als keine Rechte und Freiheiten Dritter beeinträchtigt werden (etwa bei einer Offenlegung von Geschäftsgeheimnissen oder bei einer Verletzung von

Urheberrechten). In Konfliktfällen sollte zunächst der Datenschutzbeauftragte bzw. die Aufsichtsbehörde konsultiert werden;

- Sofern der Betroffene nicht identifiziert werden kann, darf die Auskunft nach glaubhafter Darlegung verweigert werden. Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, so können zusätzliche Informationen angefordert werden;

- Informationen müssen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung gestellt werden. Bei Komplexität und hoher Anzahl kann die Frist um weitere zwei Monate verlängert werden.

Weitere Beschränkungen der Auskunftspflicht bestehen nach §§ 27 – 29, 34 BDSG-neu. Doch beachten Sie, dass jede Verweigerung dokumentiert werden muss. Darüber hinaus muss die Verweigerung mit einer Begründung oder mit Tatsachen gegenüber dem Betroffenen belegt werden.

Kurzpapier der Datenschutzkonferenz zu Auskunftsrechten:
https://www.lda.bayern.de/media/dsk_kpnr_6_auskunftsrecht.pdf

Kurzpapier des BayLDA zum Auskunftsrecht der betroffenen Person:
https://www.lda.bayern.de/media/baylda_ds-gvo_16_right_of_access.pdf

Wann müssen Informationen dauerhaft gelöscht werden?

Einen neuen Namen sowie eine umfassendere Regelung hat das Recht auf Löschung personenbezogener Daten in der DSGVO erfahren („Recht auf Vergessenwerden“). Dieses aus der „Google-Rechtsprechung“ des EuGH bekannte Recht soll Betroffenen ermöglichen, (z.B. falsche oder ehrrührige) Informationen zuverlässig und umfassend (auch aus dem Netz) entfernen zu lassen.

Eine Löschung kann ein Betroffener insbesondere bei Vorliegen einer der folgenden Voraussetzungen verlangen:

- Die Daten sind für die vorgesehenen Zwecke nicht mehr erforderlich (z.B. bei Ende der Vertragsbeziehung);

- Der Betroffene hat seine Einwilligung widerrufen;

- Bei einer Datenverarbeitung auf Grundlage eines „berechtigten Interesses“ hat der Betroffene Widerspruch eingelegt;

- Die Verarbeitung war von vornherein unrechtmäßig (keiner der Rechtfertigungsgründe des Art. 6 DSGVO war einschlägig);

- Die Löschung ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht eines Mitgliedstaates erforderlich;

- Die Daten von Kindern wurden ohne Einwilligung der Erziehungsberechtigten verarbeitet.

Das eigentliche „Recht auf Vergessenwerden“ findet sich in Art. 17 Abs. 2 DSGVO. Sofern der Verantwortliche die Daten öffentlich zugänglich gemacht hat, ist er im Rahmen seiner Möglichkeiten auch dazu verpflichtet, andere Verantwortliche auf den Löschantrag hinzuweisen. Welche Maßnahmen für den Verantwortlichen noch angemessen sind, ist bis dato noch unklar. Insbesondere die Verbreitung von Links könnte in der Praxis zu erheblichen Schwierigkeiten führen.

Dem Löschanspruch können im Einzelfall andere Rechte entgegenstehen (etwa die Meinungsfreiheit, rechtliche Ansprüche oder Verpflichtungen des Verantwortlichen oder Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit).
Neben dem Recht auf Löschung besteht auch weiterhin das aus § 35 Abs. 1 BDSG-alt bekannte Recht auf Berichtigung unzutreffender personenbezogener Daten (Art. 16 DSGVO).

Kurzpapier der Datenschutzkonferenz zum Recht auf Löschung:
https://www.lda.bayern.de/media/dsk_kpnr_11_vergessenwerden.pdf

Was ist mit Daten, die (noch) nicht gelöscht werden können?

Es kann Situationen geben, in denen der Betroffene die Löschung seiner Daten verlangt, der Verantwortliche diesem Begehren aber nicht nachkommen kann, beispielsweise weil die Daten des Betroffenen noch buchhalterischen Aufbewahrungspflichten unterliegen oder zur Durchsetzung von Rechtsansprüchen erforderlich sind. Unter bestimmten Voraussetzungen tritt dann an die Stelle der Löschung das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO). Gleiches gilt in Zweifelsfällen während der Prüfung einer Löschung. Das Recht auf Einschränkung tritt an die Stelle des bisher aus §§ 35 Abs. 3, 4 BDSG-alt bekannten Rechts auf Sperrung.

Eine deutsche Besonderheit ist in § 35 Abs. 1 BDSG-neu normiert. Demnach tritt in den Fällen einer nicht automatisierten Datenverarbeitung, bei welcher eine besondere Art der Speicherung der Daten vorliegt, das Interesse des Betroffenen als gering einzuschätzen ist und eine

Löschung nur mit einem erheblichen Aufwand möglich ist, an die Stelle des Löschungs- ein Einschränkungsanspruch.

Was bedeutet das Recht auf Datenübertragbarkeit?

Eine echte Neuerung der DSGVO ist das „Recht auf Datenübertragbarkeit“. Betroffene haben danach in Zukunft das Recht, die sie betreffenden personenbezogenen Daten, die sie einem für die Verarbeitung Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Zudem haben sie das Recht, diese Daten auf einfachem Weg zu neuen Anbietern übermitteln zu lassen. Auf diese Weise soll ein reibungsloser Anbieterwechsel für Kunden erleichtert werden.

Umfasst sind zunächst diejenigen persönlichen Daten, die der Betroffene selbst unmittelbar an den Verantwortlichen übermittelt hat (etwa durch Ausfüllen eines Webformulars). Darüber hinaus gilt das Recht aber auch für solche Daten, die als direkte Folge der Aktivitäten des Betroffenen bei dem Verantwortlichen gespeichert werden (z.B. Suchaufträge und Standort-Daten). Ausgenommen sind hingegen Datensätze, die erst auf Grundlage einer weiteren Berechnung oder Bewertung der Rohdaten entstanden sind. Dies können etwa die Ergebnisse einer Einschätzung der Kreditwürdigkeit oder des allgemeinen Gesundheitszustands des Betroffenen sein.

Soweit personenbezogene Daten Dritter in direktem Zusammenhang mit den Nutzerdaten gespeichert wurden (etwa die E-Mail-Adressen der Kontakte bei einem Webmail-Provider oder die Kontodaten von bisherigen Geschäftspartnern bei einer Bank), müssen auch diese auf Anfrage vollständig übermittelt werden. Soweit eine Übertragung auf einen anderen Anbieter vorgesehen ist, muss dieser jedoch dafür Sorge tragen, dass der Betroffene die ausschließliche Kontrolle über die Daten behält. Eine eigene Verwendung der personenbezogenen Daten Dritter durch den neuen Anbieter ist unzulässig.

Ein „strukturiertes, gängiges und maschinenlesbares“ Format setzt in der Regel voraus, dass nicht bloß der gesamte interne Datensatz zu dem Betroffenen übermittelt wird, sondern die relevanten Informationen herausgefiltert und in übersichtlicher und leicht verständlicher Weise dargestellt werden. Um größtmögliche Kompatibilität zu gewährleisten, sollen vor allem Branchenverbände auf einheitliche Formate hinwirken.

Praxis-Tipp

Rechtzeitig vor Einführung der DSGVO sollten vor allem Cloud-Anbieter, die für Ihre Kunden Software as a Service-Dienstleistungen anbieten, die technischen Voraussetzungen schaffen, um entsprechende Anfragen automatisiert beantworten zu können. Die Frist für die Beantwortung beträgt lediglich einen Monat; nur in begründeten Ausnahmefällen können es bis zu drei Monate sein!

Leitlinie der Artikel 29-Datenschutzgruppe zum Recht auf Datenübertragbarkeit:
https://www.datenschutzkanzlei.de/download/2110/

Was bedeuten die Neuerungen für die Praxis?

Vor allem die erweiterten Informationspflichten führen zu einem erheblichen Mehraufwand für Unternehmen. Ein besonderes Augenmerk sollte auf die entsprechenden Frist- und Formvorschriften gelegt werden, um sich nicht Abmahnungen und Bußgeldern ausgesetzt zu sehen. Bei den klassischen Betroffenenrechten bleibt hingegen vieles wie gehabt. Schwierigkeiten bereiten erneut unklare und schwammige Formulierungen der DSGVO. Dies gilt etwa für die Pflicht, bei dem „Recht auf Vergessenwerden“, Einfluss auf andere Verantwortliche zu nehmen, sowie insgesamt für das neue „Recht auf Datenübertragbarkeit“. Hier kann nur geraten werden, die weitere Entwicklung aufmerksam zu verfolgen.

Dieser Ratgeber wird laufend aktualisiert. Die aktuelle Fassung finden Sie unter:
https://www.datenschutzkanzlei.de/dsgvo

Dokumentationspflicht

Art. 30 DSGVO

Neben der Information der Betroffenen müssen Unternehmen bei Datenverarbeitungen auf Grundlage der DSGVO zusätzlich in einem „**Verzeichnis von Verarbeitungstätigkeiten**“ eine Reihe von Informationen dokumentieren (Art. 30 DSGVO). Aufsichtsbehörden soll es auf diese Weise erleichtert werden, die Erfüllung sämtlicher Pflichten der DSGVO rückblickend zu kontrollieren. Das Verzeichnis sollte sorgfältig geführt werden, um Vorgänge bei Beschwerden lückenlos darlegen zu können.

Risiko-Radar
Nachlässigkeit kann sich rächen. Bei Verstößen gegen die Dokumentationspflicht drohen gemäß Art 83 Abs. 4 lit. a) DSGVO Geldbußen von bis zu 10.000.000 EUR oder bis zu 2% des gesamten weltweit erzielten Vorjahresumsatzes des Unternehmens.

Welche Informationen muss das Verzeichnis enthalten?

Das Verzeichnis von Verarbeitungstätigkeiten muss sowohl von Verantwortlichen als auch von Auftragsverarbeitern in leicht unterschiedlichem Umfang geführt werden.

Verantwortliche müssen folgende Informationen dokumentieren (Art. 30 Abs. 1 DSGVO):

- 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;
- 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 in gewissen Fällen (Art. 49

DSGVO) die Dokumentation 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.

Auftragsverarbeiter müssen folgende Informationen dokumentieren (Art. 30 Abs. 2 DSGVO):

- 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 UAbs. 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

- Wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO.

Unterschied zum BDSG-alt

Die Dokumentationspflicht ist bereits aus § 4g Abs. 2 BDSG-alt bekannt. Im Gegensatz zur bisherigen Regelung muss allerdings nur ein einheitliches Verzeichnis geführt werden, das zudem nur den Aufsichtsbehörden auf Anfrage offengelegt werden muss. Die Unterscheidung zwischen „internem“ und „externem“ Verfahrensverzeichnis entfällt daher. Neu ist hingegen das Verzeichnis der Auftragsverarbeitungen!

Welche Form muss das Verzeichnis haben?

Das Verzeichnis ist schriftlich zu führen, was aber auch in einem elektronischen Format erfolgen kann (Art. 30 Abs. 3 DSGVO).

Wer ist für die Führung des Verzeichnisses verantwortlich?

Das Verzeichnis ist durch den Verantwortlichen bzw. durch den Auftragsverarbeiter selbst (also die Unternehmensleitung) zu führen. In der Praxis wird diese Aufgabe aber häufig auf den betrieblichen Datenschutzbeauftragten delegiert werden.

Gibt es Ausnahmen für kleine und mittlere Unternehmen?

Es gibt eine Ausnahme für kleine und mittlere Unternehmen und Einrichtungen mit weniger als 250 Beschäftigen. Diese sind gemäß Art. 30 Abs. 5 DSGVO von der Aufzeichnungspflicht befreit.

In der Praxis wird diese Ausnahme aber nur sehr selten greifen. Die Ausnahme greift nämlich nur, wenn diese Unternehmen

- nur gelegentlich Daten verarbeiten und
- die vorgenommene Verarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt (also z.B. keine Verarbeitung besonderer Datenkategorien nach Art. 9 Abs. 1 DSGVO).

Da bereits die Existenz einer Kundendatenbank oder die Verwaltung von Mitarbeiterdaten dazu führt, dass nicht mehr „nur gelegentlich“ Daten verarbeitet werden, dürfte diese Ausnahme für die meisten Unternehmen bedeutungslos bleiben.

Gerade für kleine Unternehmen, Handwerksbetriebe, Arztpraxen etc., die häufig unter die Befreiung von der Meldepflicht gemäß § 4d Abs. 3 BDSG-alt gefallen sind und meist auch keinen Datenschutzbeauftragten bestellen mussten, ist dies eine gewaltige Änderung. Sie sind zukünftig gefordert, ein Verzeichnis für Verarbeitungstätigkeiten gemäß Art. 30 DSGVO zu führen. Wer dies versäumt, riskiert empfindliche Bußgelder.

> **Praxis-Tipp**
> Nutzen Sie die Zeit bis zum 25. Mai 2018 für ein Update Ihres bisherigen Verfahrensverzeichnisses, damit es den inhaltlichen Anforderungen des Art. 30 DSGVO gerecht wird. Sollten Sie bisher kein Verfahrensverzeichnis geführt haben, ist es höchste Zeit, damit anzufangen.

Was bedeuten die neuen Regelungen für die Praxis?

Bei den Dokumentationspflichten ergeben sich für die meisten Unternehmen keine entscheidenden Veränderungen. Erweiterte Pflichten bestehen für Auftragsverarbeiter und bei der Übermittlung von Daten in Drittländer (etwa die USA). Zukünftig müssen auch kleinere

Anbieter, die bis dato von der Pflicht zum Führen eines Verfahrensverzeichnisses befreit waren, eine Dokumentation nachweisen. Im Hinblick auf die verschärften Maßregeln bei Datenschutzverstößen empfiehlt es sich, bestehende Dokumentationssysteme auf ihre Zuverlässigkeit und Vollständigkeit zu überprüfen und gegebenenfalls rechtzeitig vor Einführung der DSGVO entsprechende Vorkehrungen zu treffen.

Kurzpapier der BayLDA zum Verzeichnis von Verarbeitungstätigkeiten:
https://www.lda.bayern.de/media/baylda_ds-gvo_5_processing_activities.pdf

Praxishilfe des GDD zum Verzeichnis von Verarbeitungstätigkeiten:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf

Leitfaden der Bitkom zum Verzeichnis von Verarbeitungstätigkeiten:
https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Verarbeitungsverzeichnis-online.pdf

Datenschutz-Folgenabschätzung

Art. 35 DSGVO

Eine Neuerung der DSGVO ist die sogenannte „Datenschutz-Folgenabschätzung“, bei der Unternehmen verpflichtet werden, unter bestimmten Voraussetzungen vor Einführung der Datenverarbeitung eine Risikoeinschätzung vorzunehmen. Die Datenschutz-Folgenabschätzung ist immer dann erforderlich, wenn ein hohes Risiko für die Rechte und Freiheiten der Betroffenen vorliegen kann. Bei der Durchführung der Datenschutz-Folgenabschätzung ist der Rat des Datenschutzbeauftragten einzuholen, sofern ein solcher benannt wurde. Bestätigt sich im Rahmen der Datenschutz-Folgenabschätzung ein solches Risiko, muss das Verfahren bei der zuständigen Aufsichtsbehörde gemeldet werden. Diese soll so die Möglichkeit erhalten, auf kritische Verarbeitungen Einfluss zu nehmen und geeignete Maßnahmen vorzuschlagen.

Risiko-Radar

Die Datenschutz-Folgenabschätzung ist ernst zu nehmen, da gemäß Art 83 Abs. 4 lit. a) DSGVO bei Verstößen gegen Art. 35 DSGVO Geldbußen von bis zu 10.000.000 EUR oder bis zu 2% des gesamten weltweit erzielten Vorjahresumsatzes des Unternehmens drohen.

Wann ist eine Datenschutz-Folgenabschätzung vorzunehmen?

Die DSGVO nennt in Art. 35 Abs. 3 einige Fälle, in denen eine Datenschutz-Folgenabschätzung zwingend vorzunehmen ist. Dazu zählen:

- die systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

- die umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (Ärzte und Anwälte sind von dieser Pflicht ausgeschlossen);

- die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (z.B. mittels Videoüberwachung).

In allen weiteren Fällen sind die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung entscheidend, wobei insbesondere die Verwendung neuer Technologien zu berücksichtigen ist.

Praxis-Tipp
Die Aufsichtsbehörden haben angekündigt, eine Liste mit Verarbeitungsvorgängen zu veröffentlichen, die stets eine Datenschutz-Folgenabschätzung erfordern. Informieren Sie sich über neue Entwicklungen im Datenschutz, z.B. durch Anmeldung zu unseren Newsletter: https://www.datenschutzkanzlei.de/newsletter.

Wie ist die Datenschutz-Folgenabschätzung konkret umzusetzen?

Die DSGVO gibt in Art. 35 Abs. 7 vor, wie eine solche Datenschutz-Folgenabschätzung in der Praxis umzusetzen ist. Folgende Aspekte müssen eingehalten und geprüft werden:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und

- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die DSGVO eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Praxis-Tipp
Als Verantwortlicher sollten Sie einen Prozess etablieren, der bei Einführung einer neuen Datenverarbeitung eine Prüfung der Datenschutzfolgen zum Inhalt hat. In dieser Prüfung wird dann entschieden (z.B. durch den Datenschutzbeauftragten), ob ein erhöhtes Risiko der Betroffenen besteht und daraus folgend eine Meldepflicht gegenüber der Aufsichtsbehörde. Auch unterlassene Datenschutz-Folgenabschätzungen sollten zu Nachweiszwecken dokumentiert werden.

Was ist zu tun, wenn ein erhöhtes Risiko festgestellt wird?

Wenn sich bei der Datenschutz-Folgenabschätzung ein hohes Risiko ergibt, muss noch vor Durchführung des Verarbeitungsvorgangs das Verfahren der Aufsichtsbehörde gemeldet werden.

Die Meldung muss folgende Informationen enthalten (vgl. Art. 36 Abs. 3 DSGVO):

- gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen;
- die Zwecke und die Mittel der beabsichtigten Verarbeitung;
- die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß der DSGVO vorgesehenen Maßnahmen und Garantien;
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
- die Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und
- alle sonstigen von der Aufsichtsbehörde angeforderten Informationen.

Unterschied zum BDSG-alt

Im deutschen Datenschutzrecht gibt es bereits eine „Vorabkontrolle“, die in bestimmten Fällen eine interne Prüfung der Datenverarbeitung durch den Datenschutzbeauftragten erforderlich macht. Neu ist bei der Datenschutz-Folgenabschätzung, dass sensible Datenverarbeitungen zusätzlich eine Meldepflicht bei der zuständigen Aufsichtsbehörde auslösen.

Was bedeuten die neuen Regelungen für die Praxis?

Durch die Datenschutz-Folgenabschätzung müssen Verantwortliche neue Meldepflichten gegenüber den Aufsichtsbehörden beachten, welche es bisher in Deutschland nicht gegeben hat. Es bleibt abzuwarten, wie die personell schwach aufgestellten Aufsichtsbehörden diesen zusätzlichen Prüfungs- und Dokumentationsaufwand stemmen wollen. Insbesondere die schnelllebige Digitalbranche muss sich überlegen, wie sie diesen Bewertungsprozess bei der Einführung neuer Programme und Apps mit einbezieht.

Praxishilfe des GDD zur den Voraussetzungen der Datenschutz-Folgenabschätzung:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_10.pdf

Leitlinie der Artikel 29-Datenschutzgruppe der Datenschutz-Folgenabschätzung (EN):
http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

Kurzpapier des BayLDA zur Datenschutz-Folgenabschätzung:
https://www.lda.bayern.de/media/baylda_ds-gvo_18_privacy_impact_assessment.pdf

Kurzpapier der Datenschutzkonferenz zur Datenschutz-Folgenabschätzung:
https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf

Leitfaden der Bitkom zu Risk Assessment und Datenschutz-Folgenabschätzung
https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf

White Paper des Forum Privatheit zur Datenschutz-Folgenabschätzung:
https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf

Technischer Datenschutz

Art. 25 und Art. 32 DSGVO

In der DSGVO finden sich zwei wesentliche Normen zum technischen Datenschutz. Zum einen sind Verantwortliche gemäß Art. 25 DSGVO zukünftig gefordert, datenschutzfreundliche Techniken einzusetzen („Privacy by Design“) sowie Produkte oder Dienstleistungen mit datenschutzfreundlichen Voreinstellungen anzubieten („Privacy by Default“). Zum anderen macht Art. 32 DSGVO konkrete Vorgaben, welche technischen und organisatorischen Maßnahmen bei der Speicherung und Verarbeitung von personenbezogenen Daten gewährleistet werden müssen.

Risiko-Radar

Im Gegensatz zu den bestehenden Vorgaben des BDSG-alt können Verstöße gegen technische und organisatorische Vorgaben zukünftig teuer werden. Gemäß Art. 83 Abs. 4 lit. a) DSGVO drohen bei Verstößen Geldbußen von bis zu 10.000.000 EUR oder bis zu 2% des gesamten weltweit erzielten Vorjahresumsatzes des Unternehmens.

Was müssen Unternehmen bei „Privacy by Design/Default“ beachten?

Verantwortliche sind gefordert, ihre Datenerhebung und -verarbeitung so zu gestalten, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Dabei macht das Gesetz keine konkreten Vorgaben, sondern lässt den Verantwortlichen einen Abwägungsspielraum, der sich am Stand der Technik, den Kosten der Implementierung und den Risiken für die Betroffenen orientieren soll. Als Beispiel erwähnt Art. 25 Abs. 1 DSGVO lediglich die Pseudonymisierung als Maßnahme zur Datenminimierung. Auch die generelle Pflicht zu einer transparenten Datenverarbeitung wird in Erwägungsgrund 78 DSGVO als mögliche Maßnahme erwähnt. Darüber hinaus sind Verantwortliche gefordert, anhand technischer Voreinstellungen grundsätzlich nur diejenigen personenbezogenen Daten zu erheben, die tatsächlich erforderlich sind. Dies erstreckt sich auf die Menge der erhobenen Daten, den Umfang der Verarbeitung, die Speicherfrist und die Zugänglichkeit (durch Dritte). Insbesondere Soziale Netzwerke sind daher zukünftig gefordert, im Rahmen ihrer Voreinstellungen den kleinstmöglichen Empfängerkreis zu wählen.

Welche technischen Sicherheitsvorkehrungen müssen beachtet werden?

Die Schutzrichtung des Art. 32 DSGVO orientiert sich stark an den bereits beschriebenen Anforderungen zum „Privacy by Design/Default“. Welche konkreten Sicherheitsmaßnahmen angewendet werden müssen, hängt vom Umfang der Datenverarbeitung und dem Risiko für die Rechte und Freiheiten der betroffenen Personen ab. Verantwortliche müssen also im Vorwege eine Risikobewertung ihrer Datenverarbeitung vornehmen. Unter anderem müssen folgende

Maßnahmen durch den Verantwortlichen berücksichtigt und bestenfalls in einem Sicherheitskonzept festgelegt werden:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Im Gegensatz zu § 9 BDSG-alt werden in der DSGVO nun die klassischen Begrifflichkeiten der IT-Sicherheit wie Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit verwendet. Es lässt sich somit feststellen, dass der Gesetzgeber mit Art. 32 DSGVO die existierenden Standards im Datenschutzmanagement (z.B. IT-Grundschutz, ISO 27001 etc.) aufgreift.

Praxis-Tipp

Vor allem Start-ups und kleineren Unternehmen fällt es häufig schwer, geeignete Sicherheitsvorkehrungen zu treffen und schriftlich festzuhalten. Eine mögliche Vorlage bieten die VDS Richtlinien für Informationssicherheit in der Version 3473 (einfach mal bei Google eingeben). Die Vorlage bietet eine recht überschaubare Übersicht, was Unternehmen bei der Einführung eines Datenschutzmanagements beachten müssen. Zur Orientierung dient auch weiterhin der Anforderungskatalog an technische und organisatorische Maßnahmen aus der Anlage zu § 9 BDSG-alt. Darüber hinaus können Zertifizierungsverfahren und genehmigte Verhaltensregeln als Maßstab für geeignete Sicherheitsvorkehrungen herangezogen werden, wie Art. 32 Abs. 3 DSGVO ausdrücklich klarstellt.

Kurzpapier des BayLDA zur Sicherheit der Verarbeitung:
https://www.lda.bayern.de/media/baylda_ds-gvo_1_security.pdf

Was bedeuten die neuen Regelungen für die Praxis?

Neben den Verantwortlichen sind auch die Auftragsverarbeiter für die Einhaltung des technischen und organisatorischen Datenschutzes verantwortlich. Bei fehlenden oder unzureichenden Maßnahmen können erstmals auch Auftragsverarbeiter mit einem Bußgeld

belastet werden. Generell sollten sich Unternehmen mit der Einrichtung eines Datenschutzmanagements auseinandersetzen. Bestehende Konzepte zur IT-Sicherheit sind zu prüfen und ggf. um eine Risikoanalyse zu erweitern. Zum Nachweis geeigneter Maßnahmen ist die schriftliche Dokumentation der durchgeführten Maßnahmen dringend zu empfehlen.

Pflichten bei Datenpannen

Art. 33, 34 DSGVO

Besondere Pflichten treffen einen Verantwortlichen dann, wenn bereits eine Verletzung des Schutzes personenbezogener Daten erfolgt ist und diese zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Bei Datenpannen müssen zukünftig zum einen immer die Aufsichtsbehörde (Art. 33 DSGVO), zum anderen in bestimmten Fällen auch die Betroffenen selbst (Art. 34 DSGVO) kontaktiert werden. Der Verantwortliche soll auf diese Weise bei einer schnellen Bewältigung des Vorfalls unterstützt und die Betroffenen vor weiteren Schäden bewahrt werden. Das Vorgehen bei einer Datenpanne muss zudem für nachträgliche Kontrollen der Aufsichtsbehörde umfassend dokumentiert werden.

Risiko-Radar

Nachlässigkeit kann sich rächen. Bei Verstößen gegen die Dokumentationspflicht drohen gemäß Art. 83 Abs. 4 lit. a) DSGVO Geldbußen von bis zu 10.000.000 EUR oder bis zu 2% des gesamten weltweit erzielten Vorjahresumsatzes des Unternehmens.

Wann liegt eine Datenpanne vor?

Eine Verletzung des Schutzes personenbezogener Daten liegt immer dann vor, wenn von dem Verantwortlichen erlangte personenbezogene Daten Betroffener nicht mehr ordnungsgemäß gesichert sind und so in die Hände Dritter gefallen sind oder zu fallen drohen. Der klassische Fall einer Datenpanne ist der Hack eines Unternehmensservers, durch den Kundendaten in das Internet gelangen. Ob darüber hinaus ein Risiko für die Rechte und Freiheiten natürlicher Personen vorliegt, ist im Rahmen einer Abwägung festzustellen. Hierbei ist zum einen zu berücksichtigen, um was für eine Art von Daten es sich handelt (je intensiver etwa die Privatsphäre der Betroffenen oder Dritter berührt ist, desto eher liegt ein Risiko vor). Weiterhin kann ein Risiko dadurch eingedämmt worden sein, wenn der Verantwortliche rechtzeitig entsprechende Gegenmaßnahmen vorgenommen hat, um das Datenleck zu schließen.

Welche Informationen sind der Aufsichtsbehörde zu übermitteln?

Im Fall einer Datenpanne muss Folgendes an die Aufsichtsbehörde gemeldet werden (Art. 33 DSGVO):

- 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.

Diese Meldung muss unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Datenpanne vorgenommen werden. Bei späteren Meldungen muss die Verzögerung begründet werden. Kann der Verantwortliche nicht sofort alle notwendigen Informationen bereitstellen, muss er diese ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen (Art. 33 Abs. 4 DSGVO).

Unterschied zum BDSG-alt
Eine Informationspflicht bei Datenpannen ist aus § 42a BDSG-alt bekannt, es ändern sich aber Form und Inhalt der Pflichten. Zudem gibt es neue Meldefristen.

In welchen Fällen müssen auch die Betroffenen benachrichtigt werden?

Die Benachrichtigung der Betroffenen muss erfolgen, wenn ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen in Folge der Datenpanne besteht. Dies ist etwa dann der Fall, wenn die personenbezogenen Daten bereits von unbefugten Dritten abgerufen wurden oder dies unmittelbar bevorsteht. Zudem müssen die Daten einen nicht unerheblichen Bezug zur Privatsphäre der Betroffenen haben.

Die Pflicht zur Benachrichtigung Betroffener entfällt allerdings in den folgenden Fällen (Art. 34 Abs. 3 DSGVO:

- Der Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen wurden auf die von der Verletzung betroffenen personenbezogenen Daten angewandt (z.B. mittels Verschlüsselung).

- Der Verantwortliche hat durch nachträglich getroffene Maßnahmen sichergestellt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller

Wahrscheinlichkeit nach nicht mehr besteht.

- Die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

Die Benachrichtigungspflicht entfällt ferner gemäß § 29 Abs. 1 BDSG-neu, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interesse eines Dritten, geheim gehalten werden müssen. Diese Ausnahme entfällt wiederum, wenn die Interessen des Betroffenen das Geheimhaltungsinteresse überwiegen.

Die Aufsichtsbehörde kann im Einzelfall aber auch per Beschluss einen Verantwortlichen auffordern, eine Benachrichtigung vorzunehmen (Art. 34 Abs. 4 DSGVO).

Welche Informationen müssen in diesen Fällen an Betroffene übermittelt werden?

Betroffene müssen in den genannten Fällen in klarer und einfacher Sprache über folgendes informiert werden (Art. 34 Abs. 2, 3 DSGVO):

- Die Art der Verletzung des Schutzes personenbezogener Daten;

- Den Namen 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.

Inwieweit müssen Datenpannen dokumentiert werden?

Um der Aufsichtsbehörde die nachträgliche Kontrolle der Einhaltung aller Pflichten zu ermöglichen, muss ein Verantwortlicher im Falle einer Datenpanne zusätzlich eine Reihe von Informationen dokumentieren (Art. 33 Abs. 5 DSGVO). Der Verantwortliche muss Datenschutzverletzungen einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen dokumentieren.

Aufgezeichnet werden müssen dabei alle Verletzungen des Schutzes personenbezogener Daten, also **auch solche, die nicht meldepflichtig sind!** Gerade in diesen Fällen hat die Aufsichtsbehörde ein Interesse daran, nachvollziehen zu können, ob die Meldung berechtigterweise unterblieben ist.

> **Praxis-Tipp**
> Kontaktieren Sie bei Datenpannen oder dem Verdacht auf eine Datenpanne frühzeitig Ihren Datenschutzbeauftragten. Er unterstützt Sie bei der Beurteilung, ob und welche Handlungspflichten bestehen und kann die Kommunikation mit Aufsichtsbehörden und Betroffenen übernehmen. Zudem kann der Datenschutzbeauftragte sicherstellen, dass auch „unerhebliche" Datenschutzvorfälle korrekt dokumentiert werden.

Was bedeuten die neuen Regelungen für die Praxis?

Bei Vorliegen einer Datenpanne ist schnelles Handeln gefragt: Neben einer zügigen Behebung der Schwachstelle ist eine schnelle Kontaktaufnahme mit der Aufsichtsbehörde unerlässlich – in der Regel binnen 72 Stunden. Bei der Frage, ob auch Betroffene benachrichtigt werden müssen, sollte die notwendige Abwägung zusammen mit dem Datenschutzbeauftragten oder nach Rücksprache mit der Aufsichtsbehörde erfolgen. Die Dokumentation der Vorfälle und Maßnahmen darf auch in Ausnahmesituationen nicht außer Betracht bleiben.

Kurzpapier des BayLDA zum Umgang mit Datenpannen
https://www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf

Datenschutzbeauftragter

Art. 37 - 39 DSGVO
§ 38 BDSG-neu

Die hervorgehobene Stellung des Datenschutzbeauftragten war bisher eine deutsche Besonderheit. Mit der DSGVO setzt sich europaweit die Pflicht zur Bestellung eines Datenschutzbeauftragten in bestimmten Fällen durch. Die Regelungen zu Stellung und Aufgaben des Datenschutzbeauftragten entsprechen weitgehend derjenigen des BDSG-alt. Der Datenschutzbeauftragte ist danach erste Anlaufstelle, Berater und Unterstützer für alle Fragen hinsichtlich der Verarbeitung personenbezogener Daten, sowohl innerhalb des Unternehmens als auch für die Betroffenen und für die Aufsichtsbehörde. Gleichzeitig wirkt er auf die Einhaltung der Datenschutzvorschriften hin und ist eng in die Verarbeitungsprozesse im Unternehmen einzubinden.

Risiko-Radar
Unterlässt der Verantwortliche oder der Auftragsverarbeiter die Bestellung eines Datenschutzbeauftragten, so drohen gemäß Art. 83 Abs. 4 lit. a) DSGVO Geldbußen von bis zu 10.000.000 EUR oder bis zu 2% des gesamten weltweit erzielten Vorjahresumsatzes des Unternehmens.

Wann muss ein Datenschutzbeauftragter benannt werden?

Eine generelle Pflicht zur Benennung eines Datenschutzbeauftragten besteht gemäß Art. 37 Abs. 1 DSGVO für Verantwortliche und Auftragsverarbeiter nur, wenn:

- ihre Kerntätigkeit 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. Die Datenverarbeitung stellt in diesen Fällen also nicht nur eine unterstützende Randfunktion dar (wie etwa bei der Gehaltsabrechnung), sondern ist wesentliche Voraussetzung für die Haupttätigkeit. Dies trifft etwa auf Anbieter für personalisierte Werbung zu, die für die Erstellung maßgeschneiderter Anzeigen zwingend auf systematische Auswertung personenbezogener Daten angewiesen sind;

- ihre Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO besteht. Inwieweit eine „umfangreiche Verarbeitung“ vorliegt, richtet sich vor allem nach der Anzahl der Betroffenen, dem Umfang und der Verschiedenartigkeit sowie der geographischen Erstreckung der erhobenen Daten. Umfasst sind beispielsweise Krankenhäuser, die für

eine effektive Behandlung regelmäßig im großen Umfang Gesundheitsdaten der Patienten verarbeiten müssen.

Diese Einschränkung der Benennungspflicht wird allerdings für deutsche Unternehmen keine praktische Relevanz erlangen, da Art. 37 Abs. 4 Satz 2 DSGVO eine Öffnungsklausel für die Mitgliedstaaten enthält. Gemäß § 38 Abs. 1 BDSG-neu wird die erweiterte Benennungspflicht beibehalten. Danach muss ein Datenschutzbeauftragter benannt werden, wenn in der Regel **mindestens zehn Personen** ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind. In Deutschland ansässige Unternehmen haben demnach in der Regel keine wesentlichen Änderungen zu erwarten. Die bereits erfolgten Benennungen bleiben auch mit Einführung der DSGVO wirksam.

Zudem bestimmt § 38 Abs. 1 Satz 2 BDSG-neu eine Benennungspflicht, und zwar unabhängig von der Anzahl der Beschäftigten, wenn der Verantwortliche oder der Auftragsverarbeiter:

- Verarbeitungen vornehmen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO unterliegen, oder

- personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeiten.

Sofern ein Unternehmen nach eingehender Prüfung zu der Einschätzung gelangt, keine Pflicht zur Ernennung eines Datenschutzbeauftragten zu haben, sollten die Grundlagen dieser Entscheidung genau dokumentiert werden.

Eine freiwillige Ernennung bleibt weiterhin möglich. Allerdings gilt in diesem Fall gemäß § 38 Abs. 2 BDSG-neu nicht der erweiterte Kündigungsschutz.

Praxis-Tipp
Für Start-ups und kleine Unternehmen mit weniger als 10 Beschäftigten kann die Neuregelung zu einer Verschärfung führen. Wenn die Tätigkeit des Unternehmens in eine der Kategorien des Art. 37 Abs. 1 DSGVO oder des § 38 Abs. 1 Satz 2 BDSG-neu fällt, benötigen Sie auch dann einen betrieblichen Datenschutzbeauftragten, wenn Sie unter dem Schwellenwert des BDSG-neu liegen.

Praxishilfe des GDD zum Datenschutzbeauftragten:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_1.pdf

Was gilt für Konzerne und Unternehmensgruppen?

Die Bestellung eines Konzerndatenschutzbeauftragten ist gemäß Art. 37 Abs. 2 DSGVO ausdrücklich möglich. Voraussetzung ist lediglich, dass der Datenschutzbeauftragte von jeder Niederlassung erreicht werden kann. Auch bei international tätigen Konzernen sollte der Datenschutzbeauftragte deshalb seinen Sitz in einer Niederlassung innerhalb der EU haben.

Was sind die Aufgaben des Datenschutzbeauftragten?

Der Datenschutzbeauftragte wirkt auf die Einhaltung der Datenschutzgesetze hin und ist der erste Ansprechpartner im Unternehmen, wenn es um Fragen zur Verarbeitung personenbezogener Daten geht.

Art. 37 Abs. 1 DSGVO zählt folgende Aufgaben des Datenschutzbeauftragten auf:

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DSGVO sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;

- Überwachung der Einhaltung der DSGVO, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

- Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung;

- Zusammenarbeit mit der Aufsichtsbehörde;

- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Art. 36 DSGVO, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Praxis-Tipp

Der Datenschutzbeauftragte kann bei der Prüfung und vertraglichen Absicherung einer Auftragsverarbeitung, bei der Prüfung der technischen und organisatorischen Maßnahmen zur Datensicherheit und bei der Erfüllung der Dokumentationspflichten entscheidende Unterstützung leisten.

Praxishilfe des GDD zu den Aufgaben des Datenschutzbeauftragten:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_2.pdf

Welche Voraussetzungen muss der Datenschutzbeauftragte erfüllen?

Zum Datenschutzbeauftragten kann nur bestellt werden, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Die Anforderungen sind daher die gleichen wie im BDSG-alt.

Die **Fachkunde** fußt auf der beruflichen Qualifikation, dem Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis sowie auf der Eignung zur Erfüllung der oben genannten Aufgaben (Art. 37 Abs. 5 DSGVO). Dabei können bei komplexen Datenverarbeitungssystemen oder bei einer umfangreichen Verarbeitung sensibler Daten besondere Kenntnisse und Fähigkeiten erforderlich sein. Die Auswahl ist daher sorgfältig anhand der speziellen Gegebenheiten im Unternehmen zu treffen.

Mit **Zuverlässigkeit** ist die persönliche Integrität gemeint. Wer bereits als unzuverlässig aufgefallen ist, scheidet daher als Datenschutzbeauftragter aus. Daneben kann die Wahrnehmung gewisser anderer Aufgaben und Tätigkeiten zu einem Interessenkonflikt führen, der ebenfalls die Zuverlässigkeit entfallen lässt (vgl. Art. 38 Abs. 6 Satz 2 DSGVO). Das kann z.B. bei einer gleichzeitigen Tätigkeit im Betriebsrat, Aufsichtsrat, in der Geschäftsführung oder auch bei Leitungsaufgaben in IT, Vertrieb, Marketing, Personal etc. der Fall sein. Dies rührt daher, dass bei Positionen mit einer gewissen Entscheidungsmacht über den Umgang mit personenbezogenen Daten eine erhöhte Gefahr besteht, „den Bock zum Gärtner zu machen“. Das Bayerische Landesamt für Datenschutzaufsicht hat kürzlich die Bestellung eines IT-Beauftragten zum Datenschutzbeauftragten untersagt und mit einem Bußgeld belegt. Der Fall zeigt, dass die Aufsichtsbehörden die Unabhängigkeit des Datenschutzbeauftragten sehr ernst nehmen.

Interner und externer Datenschutzbeauftragter?

Als Datenschutzbeauftragter kann gemäß Art. 37 Abs. 6 DSGVO sowohl ein Mitarbeiter des Unternehmens (interner Datenschutzbeauftragter) als auch ein Dritter auf Grundlage eines Dienstleistungsvertrags (externer Datenschutzbeauftragter) benannt werden.

Die Beauftragung eines externen Datenschutzbeauftragten bietet dabei einige Vorteile:

- Durch die Auswahl eines geeigneten Dienstleisters sind Fachkunde und Zuverlässigkeit gesichert;

- Unternehmen profitieren von der Erfahrung des Datenschutzbeauftragten aus einer Vielzahl von Mandaten mit häufig ähnlichen Herausforderungen und Fragestellungen;

- Es entfallen die Kosten und Ausfallzeiten für die Aus- und Weiterbildung eines internen Datenschutzbeauftragten. Zudem kann der Datenschutzbeauftragte anhand des tatsächlich anfallenden Aufwands vergütet werden, was hohe Fixkosten und Bindung von Arbeitszeit vermeidet.

- Die Verlagerung der Haftung auf den externen Datenschutzbeauftragten reduziert das Unternehmensrisiko.

- Das Unternehmen bleibt durch den Abschluss eines Dienstvertrages flexibel. Der besondere Kündigungsschutz des internen Datenschutzbeauftragten bleibt durch § 38 Abs. 2 i.V.m. § 6 Abs. 4 BDSG-neu auch mit Einführung der DSGVO erhalten.

Praxis-Tipp
Die Juristen der Datenschutzkanzlei sind ausgewiesene Experten auf dem Gebiet des Datenschutzrechts und stellen seit 2010 externe Datenschutzbeauftragte für Unternehmen. Informationen zu unseren Leistungen und ausgewählte Referenzen finden Sie unter https://www.datenschutzkanzlei.de/datenschutzbeauftragter.

Wie läuft die Zusammenarbeit mit dem Datenschutzbeauftragten?

Der Datenschutzbeauftragte muss ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden werden (Art. 38 Abs. 1 DSGVO). Dies bedeutet, dass der Datenschutzbeauftragte alle für die Einhaltung der Datenschutzvorschriften relevanten Informationen zu einem Zeitpunkt erhalten muss, der eine angemessene Bearbeitungszeit ermöglicht. Eine Einbindung bereits in der Planungsphase anstehender Datenschutzmaßnahmen kann insofern notwendig sein.

Der Verantwortliche bzw. Auftragsverarbeiter unterstützt den Datenschutzbeauftragten gemäß Art. 38 Abs. 2 DSGVO bei seinen Aufgaben durch die Bereitstellung des Zugangs zu den personenbezogenen Daten und Verarbeitungsvorgängen. Die ebenfalls erforderliche Bereitstellung der erforderlichen Ressourcen sowie die zur Erhaltung des Fachwissens erforderliche Schulungszeit betreffen hingegen primär interne Datenschutzbeauftragte. Der Datenschutzbeauftragte ist seinerseits verpflichtet, unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters über seine Arbeit Rechenschaft zu leisten (Art. 38 Abs. 3 DSGVO). Er bleibt hinsichtlich seiner Aufgaben allerdings unabhängig und ist nicht an Weisungen des Auftraggebers gebunden.

Was bedeuten die neuen Regelungen für die Praxis?

Dem Datenschutzbeauftragten kommt im Unternehmen eine entscheidende Bedeutung bei der Vorbereitung und Umsetzung der Vorgaben aus der DSGVO zu. Die vermeintliche Beschränkung bei der Benennungspflicht wird in Deutschland aufgrund der Öffnungsklausel keine praktischen Auswirkungen haben. Auch in den Fällen, in denen keine Pflicht zur Benennung besteht, ist eine Einbindung eines externen Datenschutzbeauftragten in Erwägung zu ziehen: Die umfangreichen neuen Pflichten bei der Verarbeitung personenbezogener Daten bedürfen oftmals entsprechender betrieblicher Prozesse, die mit Hilfe des Datenschutzbeauftragten rechtzeitig eingerichtet werden können. Hohe Bußgelder bei Einführung der DSGVO können auf diese Weise vermieden werden.

Kurzpapier des BayLDA zum Datenschutzbeauftragten:
https://www.lda.bayern.de/media/baylda_ds-gvo_19_data_protection_officer.pdf

Leitlinie der Artikel 29-Datenschutzgruppe zum Datenschutzbeauftragten:
https://www.datenschutzkanzlei.de/download/2108/

Datenübermittlung in Drittstaaten

Art. 44 ff. DSGVO

Beabsichtigt ein Unternehmen, personenbezogene Daten an Empfänger im Ausland zu übermitteln, ist zu unterscheiden: Während bei einer Datenübertragung innerhalb von EU-Mitgliedstaten lediglich die allgemeinen Rechtfertigungstatbestände des Art. 6 DSGVO gelten, bestehen im Falle einer Übermittlung in Drittstaaten (Staaten außerhalb der EU) zusätzliche Anforderungen. Hier unterscheiden sich die Regelungen der DSGVO allerdings nicht erheblich von der bisherigen Rechtslage.

Risiko-Radar
Unberechtigte Übermittlungen personenbezogener Daten an Empfänger in Drittstaaten können existenzbedrohend sein. Gemäß Art. 83 Abs. 5 lit. c) DSGVO drohen Geldbußen von bis zu 20.000.000 EUR oder bis zu 4% des gesamten weltweit erzielten Vorjahresumsatzes des Unternehmens.

Wann ist eine Datenübermittlung in Drittstaaten gerechtfertigt?

Im Falle einer Datenübermittlung in Drittstaaten ist eine zweistufige Prüfung vorzunehmen. Zunächst muss, wie bei Datenübermittlungen im Inland bzw. Übermittlungen in das EU-Ausland, ein Rechtfertigungsgrund des Art. 6 DSGVO greifen (etwa ein überwiegendes berechtigtes Interesse des Verantwortlichen). Ist dies der Fall, muss in einem zweiten Schritt festgestellt werden, ob bei dem Drittstaat oder zumindest bei dem konkreten Empfänger ein angemessenes Datenschutzniveau vorliegt. Hierbei ist allerdings in der Regel keine eigene Abwägung des Verantwortlichen gefragt.

Für die Feststellung sieht die DSGVO vielmehr eine Reihe verschiedener Instrumente vor:

- Die EU-Kommission kann per **Angemessenheitsbeschluss** feststellen, ob ein bestimmter Drittstaat, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder eine internationale Organisation ein angemessenes Datenschutzniveau im Sinne der Verordnung aufweist (Art. 45 DSGVO). Die bisherigen Beschlüsse nach alter Rechtslage, die ein entsprechendes Datenschutzniveau für Kanada, Australien, Schweiz, Israel, Neuseeland, Andorra, Argentinien, Färöer, Guernsey, Isle of Man, Jersey und Uruguay festgestellt haben, bleiben vorerst wirksam.

- Falls kein Angemessenheitsbeschluss vorliegt, dürfen personenbezogene Daten nur dann in einen Drittstaat übermittelt werden, sofern der Verantwortliche oder der Auftragsverarbeiter **geeignete Garantien** vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen (Art. 46 Abs. 1 DSGVO). Dazu kommen vor allem in Betracht:

- **EU-US Privacy Shield**. Ein angemessenes Datenschutzniveau liegt bei US-amerikanischen Unternehmen und Institutionen vor, die das Zertifizierungsverfahren des „EU-US Privacy Shield"-Abkommens durchlaufen haben.

- **EU-Standarddatenschutzklauseln** (Art. 46 Abs. 2 lit. c), lit. d) DSGVO). Eine Verwendung der Standarddatenschutzklauseln ist ohne eigenständige Genehmigung möglich. Dabei können bis zum Erlass neuer Klauseln durch die EU-Kommission weiterhin die bisherigen Sets genutzt werden. Sofern die Klauseln unverändert übernommen werden, ist eine weitere Prüfung durch die Aufsichtsbehörde nicht notwendig. Allerdings ist hier die weitere Entwicklung zu beobachten, da auch die Standarddatenschutzklauseln in Folge des „Safe Harbor"-Urteils angreifbar sind.

- **Verbindliche interne Datenschutzvorschriften** („Binding Corporate Rules"). Diese müssen in einem aufwändigen Genehmigungsverfahren unter Beteiligung der EU-Kommission und der Aufsichtsbehörde zertifiziert werden (Art. 46 Abs. 2, Art. 47 DSGVO). Wirksamkeit erlangen die Vorschriften zudem nur im eigenen Unternehmensverbund, nicht gegenüber Drittunternehmen.

- Durch die Aufsichtsbehörde **genehmigte Vertragsklauseln** (Art. 46 Abs. 3 lit. a) DSGVO). Auch nach alter Rechtslage erfolgte Genehmigungen bleiben wirksam, bis sie von der Aufsichtsbehörde geändert, ersetzt oder aufgehoben werden (Art. 46 Abs. 5 DSGVO).

- Eine Neuerung stellen die genehmigten **Verhaltensgarantien** (Art. 40 DSGVO) und die genehmigten **Zertifizierungsverfahren** (Art. 42 DSGVO) dar. Wie diese konkret aussehen werden und ob sie einen praktischen Mehrwert gegenüber den Alternativen bieten, bleibt zu diesem Zeitpunkt allerdings noch undeutlich.

Praxis-Tipp

Besondere Bedeutung für Datentransfers in die USA hat das „Safe-Harbor"-Urteil des EuGH aus dem Jahr 2015, in dem das Datenschutz-Abkommen zwischen der EU und den USA für unwirksam erklärt wurde. Zwischenzeitlich ist ein neues Abkommen namens „Privacy Shield" getroffen worden. Allerdings steht das Privacy Shield in der Kritik, nicht sämtliche Vorgaben des „Safe Harbor"-Urteils zu berücksichtigen. Da eine erneute Verwerfung durch den EuGH nicht auszuschließen ist, sollte ein Datentransfer nach Möglichkeit nicht ausschließlich auf dieses Abkommen gestützt werden. Gleiches gilt für EU-Standarddatenschutzklauseln. Wir empfehlen daher, möglichst „mehrgleisig" zu fahren und sich darauf einzustellen, die Datenübermittlung in die USA von Zeit zu Zeit neu rechtfertigen zu müssen.

Sofern ein angemessenes Datenschutzniveau nach diesen Vorschriften nicht vorliegt, kann dennoch eine Ausnahme des Art. 49 DSGVO greifen. Praxisrelevant für Unternehmen sind insbesondere folgende Ausnahmetatbestände:

- Die **Einwilligung des Betroffenen** (Art. 49 Abs. 1 lit. a) DSGVO). Über die allgemeinen Anforderungen an eine Einwilligung hinaus muss der Betroffene jedoch über die bestehenden möglichen Risiken bei Datenübermittlungen in einen Drittstaat ohne angemessenes Datenschutzniveau informiert werden. Die Einwilligung muss zudem für den konkreten Einzelfall vorliegen; eine pauschale Einwilligung ist nicht möglich.

- Eine Datenübermittlung zur **Erfüllung eines Vertrages** oder zur **Durchführung von vorvertraglichen Maßnahmen** auf Antrag des Betroffenen (Art. 49 Abs. 1 lit. b) DSGVO). Dies kann etwa erforderlich sein bei grenzüberschreitenden Bestellungen über ein deutsches Portal oder im Fall einer Kreditkartennutzung im Ausland.

Was bedeuten die neuen Regelungen für die Praxis?

Bei der Datenübertragung in Drittstaaten kann in den meisten Fällen auf die bisherigen Modelle zurückgegriffen werden. Eine Unsicherheit besteht allerdings im Zusammenhang mit der „Safe Harbor“-Rechtsprechung. Weitere Folgeurteile des EuGHs, die etwa das Privacy Shield-Abkommen oder die EU-Standarddatenschutzklauseln betreffen können, erscheinen nicht ausgeschlossen. Da zudem die Angemessenheitsbeschlüsse der EU-Kommission regelmäßig überprüft und gegebenenfalls wieder aufgehoben werden können, ist eine aufmerksame Beobachtung der Rechtslage unerlässlich.

Kurzpapier der Datenschutzkonferenz zur Datenübermittlung in Drittländer:
https://www.lda.bayern.de/media/dsk_kpnr_4_drittlaender.pdf

Gesetzestexte (Links)

DSGVO inklusive Erwägungsgründen: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

BDSG-neu:
https://www.datenschutzkanzlei.de/download/2678/

DSGVO mit Zuordnung BDSG-neu (GDD-Version):
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_6.pdf

Unsere Leistungen im Datenschutzrecht

Datenschutz-Grundverordnung
Optimale Vorbereitung: Wir begleiten Sie bei der Umsetzung der DSGVO und des BDSG-neu und machen Sie fit für das neue Datenschutzrecht.

Projektberatung
Wir unterstützen Sie bei der Umsetzung Ihrer Geschäftsideen und bei der Nutzung personenbezogener Daten innerhalb der rechtlichen Spielräume.

Externer Datenschutzbeauftragter
Unsere Juristen können von Unternehmen, Behörden und Organisationen zum externen Datenschutzbeauftragten benannt werden.

Cloud-Dienste
Wir unterstützen Sie bei der rechtlichen Absicherung von Software-as-a-Service, Cloud-IT, Auftragsverarbeitung und internationalem Datentransfer.

Krisenmanagement
Wir übernehmen das Kommando bei Datenpannen und sorgen für eine reibungslose Kommunikation mit Behörden und Betroffenen.

Datenschutzerklärung
Wirksamer Abmahnschutz: Wir sorgen bei Ihrem Internetauftritt für ein korrektes Impressum und die passende Datenschutzerklärung.

Schulungen
Wir schulen Führungskräfte, Fachabteilungen und ganze Teams. Als individueller Workshop, Inhouse-Schulung oder mit praktischen Online-Kursen.

Vorträge
Die Anwälte der Datenschutzkanzlei sind erfahrene Referenten und verstehen es, auch komplexe Themen greifbar und verständlich zu vermitteln. Wir haben Spaß an Vorträgen, Podiumsdiskussionen, Webinaren, Interviews etc.

Zudem beraten wir Sie bei Rechtsfragen rund um IT, Online, Mobile und Social Media.

Wünschen Sie rechtliche Beratung oder möchten Sie uns zu Ihrem Datenschutzbeauftragten bestellen? Rufen Sie uns an unter +49 (0)40 228 691 140 oder schreiben Sie uns eine E-Mail an info@datenschutzkanzlei.de. Wir freuen uns, von Ihnen zu hören!