HERTING OBERBECK
DATENSCHUTZKANZLEI

Das neue Datenschutzrecht

77 Antworten zur Datenschutz-Grundverordnung

und zum Bundesdatenschutzgesetz

Mai 2019
Version 2.0

Kontakt

DATENSCHUTZKANZLEI
Herting Oberbeck Rechtsanwälte Partnerschaft
Hallerstraße 76, 20146 Hamburg

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

Diese „77 Antworten“ wurden nach bestem Wissen erstellt und geben den Rechtsstand vom Zeitpunkt der Erstellung wieder. Sie dienen einem ersten Überblick und ersetzen freilich nicht die anwaltliche Beratung.

Vorwort

Liebe Leserin, lieber Leser,

seit rund einem Jahr gilt europaweit die Datenschutz-Grundverordnung (DSGVO), welche in Deutschland von einem neuen Bundesdatenschutzgesetz (BDSG) flankiert wird. Bei den meisten Unternehmen brach erst gegen Ende der zweijährigen Umsetzungsfrist eine gewisse Unruhe aus. Auch wenn nicht alles neu war und viele Unternehmen bereits auf etablierte Datenschutzkonzepte zurückgreifen konnten, braucht es oft Zeit, um Prozesse im teilweise undurchsichtigen „Datenschutz-Dschungel“ auf- und umzusetzen.

Mit den vorliegenden 77 Antworten (in der ersten Version waren es noch 55 Antworten und wenn wir ehrlich sind, haben wir hier 81 Antworten für Sie - aber 77 klingt irgendwie besser) möchten wir Ihnen einen 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, Phillip Malinowski, Anna-Lea Burgdorf und Julia Kaiser, die an der Erstellung der „77 Antworten“ mitgewirkt haben.

Dieses Whitepaper wird regelmäßig aktualisiert und sukzessive ausgebaut. Die erste Version haben wir im Oktober 2016 veröffentlicht und seitdem mehrfach überarbeitet. Zum einjährigen Geburtstag der DSGVO haben wir mit der hier vorliegenden Version eine umfassende Überarbeitung vorgenommen, einige Kapitel ergänzt und erneut nützliche weiterführende Informationen der Aufsichtsbehörden, Datenschutzgremien und Fachverbände ergänzt.

Die aktuellste Version finden Sie stets im Internet unter www.datenschutzkanzlei.de. 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 Mai 2019

Ihr Team der Datenschutzkanzlei

Inhaltsverzeichnis

In eigener Sache

Externer Datenschutzbeauftragter

Die Tätigkeit des Datenschutzbeauftragten ist seit 2010 unser Geschäft. Und das verstehen wir genauso gut, wie die Anforderungen von Unternehmen an praxistaugliche Lösungen, verständliche Antworten und eine solide Datenschutz-Compliance. Wir haben Werkzeuge, Taktiken und Vorlagen für ein schnelles Setup der DSGVO-Dokumentationen und der Datenschutz-Management-Prozesse und stellen jedem Kunden einen erfahrenen persönlichen Ansprechpartner zur Seite.

Die Juristinnen und Juristen der Datenschutzkanzlei sind als TÜV-zertifizierte Datenschutzbeauftragte für Unternehmen und Organisationen mit klassischen und neuen Geschäftsmodellen tätig.

www Informationen zu unseren Leistungen und ausgewählte Referenzen finden Sie unter: https://www.datenschutzkanzlei.de/datenschutzbeauftragter

DSGVO-Onlinekurs

Zusammen mit der ZEIT Akademie haben wir einen DSGVO-Onlinekurs entwickelt. In 9 Video-Lektionen zeigen wir, wie die wichtigsten Anforderungen der DSGVO pragmatisch umgesetzt werden können. Wir haben unsere Erfahrungen aus einer Vielzahl erfolgreicher DSGVO-Projekte einfließen lassen. Mit verständlichen Erläuterungen, Praxis-Tipps und passenden Vorlagen unterstützen wir bei der Umsetzung der DSGVO.

Der Onlinekurs richtet sich an Datenschutzbeauftragte, Führungskräfte und sonstige Datenschutzverantwortliche.

www Der Kurs ist abrufbar unter:
https://www.zeitakademie.de/seminare/business/dsgvo

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 seit dem 25. Mai 2018 und löste zu diesem Zeitpunkt die EU-Datenschutzrichtlinie (95/46/EG) ab, auf der das frühere Bundesdatenschutzgesetz (BDSG-alt) beruhte.

Was ist das BDSG?

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

Das BDSG 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 entfaltete zeitgleich mit der DSGVO am 25. Mai 2018 seine Wirkung.

Das BDSG 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 - was gilt seit dem 25. Mai 2018?

Kurz gesagt: beides! Die 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. Darüber hinaus regelt das BDSG 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 unbedingt einfacher. Das BDSG 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 den Handlungsspielraum der Öffnungsklauseln überschritten habe und damit EU-rechtswidrig sei. Für Unternehmen führt das zu erheblicher Rechtsunsicherheit bei der Umsetzung der neuen Bestimmungen.

Zudem gibt es Gremien wie die Datenschutzkonferenz, über die sich die deutschen Aufsichtsbehörden abstimmen und praktische Kurzpapiere und Orientierungshilfen veröffentlichen. Ein ähnliches Gremium auf europäischer Ebene stellt der Europäische Datenschutzausschuss dar (Nachfolger der Artikel-29-Gruppe), 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. Einige Links und Fundstellen finden Sie in diesem Whitepaper.

Für wen gelten die neuen Bestimmungen?

Die DSGVO und das BDSG gelten 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 (Niederlassungsprinzip). In Deutschland ansässige Unternehmen sind daher nahezu vollständig vom Geltungsbereich der DSGVO und des BDSG erfasst.

Darüber hinaus gilt 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).

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 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?

„Personenbezogene 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 endet erst da, wo eine solche Zuordnung auch mit größtmöglichem Aufwand nicht möglich ist.

Praxis-Tipp
Im Datenschutz wird grundsätzlich nicht zwischen geschäftlichen und persönlichen Daten differenziert. Das bedeutet, dass beispielweise auch geschäftliche E-Mail-Adressen, die auf eine Person schließen lassen oder Kontaktdaten des Ansprechpartners eines Unternehmens personenbezogene Daten sind. Auch für diese Daten gelten die gesetzlichen Anforderungen!

Welchen Stellenwert haben die Grundsätze der Datenverarbeitung?

Die DSGVO ist technikneutral und entwicklungsoffen gestaltet. Sie bezieht sich nicht auf einzelne Technologien oder Formen zur Verarbeitung personenbezogener Daten. Die datenschutzrechtlichen Anforderungen an spezifische Datenverarbeitungen müssen daher aus den abstrakt gehaltenen Vorgaben der DSGVO entwickelt werden. Diese ergeben sich im Wesentlichen aus den in Art. 5 Abs. 1 DSGVO benannten Grundsätzen für die Verarbeitung personenbezogener Daten. Diese Grundsätze werden durch weitere Bestimmungen der DSGVO konkretisiert und handhabbar gemacht.

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 „Rechtmäßigkeit der Datenverarbeitung“?

Die Verarbeitung personenbezogener Daten muss gemäß Art. 5 Abs. 1 Buchst. a) DSGVO in rechtmäßiger Weise, also im Rahmen der rechtlichen Vorgaben erfolgen. Anforderungen an die Rechtmäßigkeit ergeben sich insbesondere aus Art. 6 Abs. 1 DSGVO und in Bezug auf besondere Kategorien personenbezogener Daten aus Art. 9 DSGVO. Weitere Erlaubnistatbestände sind in den §§ 22 – 28 BDSG normiert.

Was bedeutet „Verarbeitung nach Treu und Glauben“?

Die Verarbeitung muss gemäß Art. 5 Abs. 1 Buchst. a) DSGVO den Grundsatz von Treu und Glauben beachten. Diese Anforderung ist bisher durch Rechtsprechung und Wissenschaft noch nicht klar ausgearbeitet. Sie kann als Auffangklausel verstanden werden, nach der sich in Einzelfällen eine an sich zulässige Verarbeitung als unfair und damit rechtswidrig erweist.

Dieser Grundsatz verpflichtet den Verantwortlichen jedenfalls dazu, der betroffenen Person die Ausübung der Betroffenenrechte aus Art. 15 bis 22 DSGVO nicht unbillig zu erschweren oder deren Umsetzung zu verweigern. Konkretisiert wird diese Anforderung durch Art. 12 Abs. 2 bis Abs. 6 DSGVO, in denen Vorgaben zu den Modalitäten hinsichtlich der Ausübung der

Betroffenenrechte enthalten sind. Zentral ist Art. 12 Abs. 2 DSGVO, wonach der Verantwortliche der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 22 DSGVO erleichtern muss.

Was bedeutet „Transparenz der Datenverarbeitung“?

Nach dem Grundsatz der Transparenz (ebenfalls Art. 5 Abs. 1 Buchst. a) DSGVO) muss die Verarbeitung personenbezogener Daten für die betroffene Person zu jedem Zeitpunkt nachvollziehbar sein. Eine heimliche Verarbeitung ist damit grundsätzlich untersagt.

Näher ausgestaltet wird der Transparenzgrundsatz durch die Informationspflichten des Verantwortlichen, die in Art. 13 DSGVO und Art. 14 DSGVO geregelt sind. Diese Informationen müssen der betroffenen Person regelmäßig spätestens zum Zeitpunkt der Datenerhebung mitgeteilt werden. Außerdem kommt der betroffenen Person gem. Art. 15 Abs. 1 DSGVO ein Recht auf Auskunft über die konkrete Verarbeitung sie betreffender Daten und ein Recht auf Erhalt einer Kopie dieser Daten zu. Anforderungen an die Modalitäten zu diesen Mitteilungen finden sich in Art. 12 Abs. 1 DSGVO.

Was bedeutet „Zweckbindung“?

Dem Grundsatz der Zweckbindung aus Art. 5 Abs. 1 Buchst. b) DSGVO kommt im Datenschutzrecht zentrale Bedeutung zu. Es setzt sich aus zwei Elementen zusammen: der Zweckfestlegung und der Zweckänderung.

Das Element der Zweckfestlegung meint, dass personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden dürfen. Es muss demnach bereits bei der Datenerhebung festgelegt sein, welche Zwecke mit der weiteren Datenverarbeitung verfolgt werden sollen. Dem festgelegten Zweck der Verarbeitung kommt eine übergreifende Bedeutung innerhalb der Regelungskonzeption der DSGVO zu. So lässt sich die Erforderlichkeit der Datenverarbeitung (siehe dazu „Datenminimierung“) nur anhand der festgelegten Zwecke bestimmen. Auch die Verpflichtung zur Löschung von Daten knüpft im Wesentlichen an die Zweckerreichung und damit den festgelegten Verarbeitungszweck an (siehe dazu „Speicherbegrenzung“). Zusätzlich muss in der Umsetzung des sog. Risikobasierten Ansatzes der DSGVO der festgelegte Zweck der Verarbeitung als Faktor in der Risikoanalyse berücksichtigt werden (siehe dazu „Integrität und Vertraulichkeit“).

Auch das zweite Element, die Zweckänderung, knüpft an den festgelegten Zweck an. Die einmal erhobenen Daten dürfen nämlich nicht in einer mit den festgelegten Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Sofern die Weiterverarbeitung zu einem neuen Sekundärzweck nicht auf einer Einwilligung der betroffenen Person oder einer rechtlichen Grundlage beruht, muss die Zulässigkeit im Rahmen einer Vereinbarkeitsprüfung gem. Art. 6 Abs. 4 DSGVO im Einzelfall festgestellt werden. Die Vereinbarkeit bemisst sich dabei wesentlich an dem Primärzweck. Damit determinieren die bei der Erhebung festgelegten Primärwecke die

Reichweite einer möglichen zukünftigen Weiterverarbeitung der Daten. Aus diesem Grund liegt die sorgfältige Festlegung der Verarbeitungszwecke auch im wesentlichen Interesse des Verantwortlichen.

Was bedeutet „Datenminimierung“?

Nach dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c) DSGVO) muss die Verarbeitung personenbezogener Daten für die Erreichung des festgelegten Zwecks angemessen und erheblich sein. Außerdem muss sie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt und damit zur Zweckerreichung erforderlich sein. Der Grundsatz der Datenminimierung lässt sich also nur relativ in Bezug auf den Verarbeitungszweck konkretisieren. Der Grundsatz der Minimierung richtet sich dabei sowohl auf die Datenbasis als auch die Verarbeitungsprozesse. Es darf nicht so verstanden werden, dass jede Datenverarbeitung zu minimieren wäre. Entscheidender Anknüpfungspunkt der Minimierung ist nämlich der Personenbezug der verarbeiteten Daten.

Was bedeutet „Richtigkeit“?

Nach dem Grundsatz der Richtigkeit (Art. 5 Abs. 1 Buchst. d) DSGVO) sollen verarbeitete personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Der Verantwortliche hat angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden. Relevanz bekommt dieser Grundsatz in Verarbeitungsprozessen, die über einen längeren Zeitraum andauern und sich dabei kontinuierlich auf eine Datenbasis beziehen.

Konkretisiert wird der Grundsatz der Richtigkeit durch das Recht auf Berichtigung gem. Art. 16 DSGVO. Auch das Recht auf Einschränkung der Verarbeitung aus Art. 18 Abs. 1 Buchst. a) DSGVO nimmt Bezug auf die Richtigkeit der Daten.

Was bedeutet „Speicherbegrenzung“?

Der Grundsatz der Speicherbegrenzung gemäß Art. 5 Abs. 1 Buchst. e) DSGVO verlangt, dass personenbezogene Daten in einer Form gespeichert werden, die eine Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Er ist eng mit den Grundsätzen der Zweckbindung in Form der Zweckfestlegung und der Datenminimierung verknüpft und stellt im Wesentlichen die Konsequenz aus dem Zusammenwirken dieser beiden Grundsätze dar. Wenn der festgelegte Verarbeitungszweck erreicht ist, ist die weitere Verarbeitung der Daten bezogen auf diesen Zweck nicht mehr erforderlich.

Eigentlicher Gegenstand der Speicherbegrenzung sind nicht die gespeicherten Daten, sondern die mit ihnen einhergehende Identifizierungsmöglichkeit der betroffenen Person. Löschen im

Sinne der DSGVO bezieht sich daher auch nicht zwingend auf die gespeicherte Datenbasis, sondern den vorhandenen Personenbezug. Daher kann eine Löschung auch im Wege einer Anonymisierung erfolgen, sofern der Verantwortliche diese nicht mehr rückgängig machen kann.

Konkretisiert wird der Grundsatz der Speicherbegrenzung durch das in Art. 17 Abs. 1 DSGVO geregelte Recht auf Löschung und das Recht auf Einschränkung der Verarbeitung aus Art. 18 DSGVO.

Was bedeutet „Integrität und Vertraulichkeit“?

Nach dem Grundsatz der Integrität und Vertraulichkeit aus Art. 5 Abs. 1 Buchst. f) DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Der Verantwortliche hat geeignete technische Maßnahmen zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung der personenbezogenen Daten zu ergreifen.

Konkretisiert wird dieser Grundsatz durch Art. 32 DSGVO, nach dem der Verantwortliche durch geeignete technische und organisatorische Maßnahmen ein dem Risiko der Verarbeitung angemessenen Schutzniveau gewährleisten muss. Die DSGVO schreibt hierbei kein bestimmtes Schutzkonzept vor. Stattdessen muss der Verantwortliche in Umsetzung des sog. risikobasierten Ansatzes für die konkreten Verarbeitungsprozesse bestimmen, welche geeigneten Maßnahmen sich bezogen auf diese jeweils als angemessen darstellen.

In bestimmten Fällen ist es notwendig, diese Risikoanalyse in Form einer Datenschutz-Folgeabschätzung im Sinne der Art. 35 und 36 DSGVO durchzuführen. Auch die in den Art. 33 und Art. 34 DSGVO geregelten Meldepflichten für den Fall einer Verletzung des Schutzes der personenbezogenen Daten sind dem Grundsatz der Datensicherheit zuzuordnen.

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 deren Einhaltung nachweisen können (Rechenschaftspflicht/Accountability).

Es sind daher umfangreiche Dokumentationen erforderlich. Hierzu zählt beispielsweise das Verzeichnis von Verarbeitungstätigkeiten, welches sowohl Verantwortliche als auch Auftragsverarbeiter gem. Art. 30 DSGVO führen müssen. Die Rechenschaftspflicht bedeutet für die Praxis außerdem eine Dokumentation wesentlicher Datenschutz-Prozesse und Entscheidungsgrundlagen als geeigneter Nachweis für die Einhaltung der datenschutzrechtlichen Anforderungen. Unternehmen kommen also nicht daran vorbei, den

Datenschutz aktiv zu managen und wirksame Datenschutzkonzepte/ Datenschutz-Management-Systeme (DSMS) einzuführen.

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

Verarbeitung von personenbezogenen Daten

Art. 6 und 9 DSGVO, §§ 22ff. BDSG

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“. 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.

Weitere Erlaubnistatbestände sind in Art. 9 DSGVO sowie in den §§ 22 – 28 BDSG normiert.

Welche Besonderheiten gelten bei der Einwilligung einer betroffenen Person?

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

Eine Erleichterung für Unternehmen besteht darin, dass sich die DSGVO von der Schriftform verabschiedet. Allerdings liegt die Beweislast für das Vorliegen der Einwilligung weiterhin bei den Unternehmen als Verantwortliche.

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

> **Praxis-Tipp**
> Das „Kopplungsverbot“ erlangt 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 Zweifel an der Wirksamkeit entstehen.

Kurzpapier der Datenschutzkonferenz zur Einwilligung nach der DSGVO:
https://www.tlfdi.de/mam/tlfdi/themen/kurzpapier_20.pdf

Praxishilfe des GDD zur Einwilligung:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_13.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 kann die Einwilligung widerrufen werden?

Die Einwilligung einer betroffenen Person kann gemäß Art. 7 Abs. 3 DSGVO jederzeit widerrufen werden. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit zukünftiger Verarbeitungen aufgehoben. Verarbeitungen, die auf Grundlage der Einwilligung bereits erfolgt sind, bleiben aber rechtmäßig. Formell ist zu beachten, dass der Widerruf so einfach auszuüben sein muss, wie die Erteilung der Einwilligung.

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

Gemäß Art. 6 Abs. 1 Buchst. b) DSGVO sind Verarbeitungen erlaubt, die zur Vertragserfüllung erforderlich sind. Eine Datenverarbeitung ist beispielsweise zur Erfüllung eines Vertrages, 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 zur Durchführung vorvertraglicher Maßnahmen erforderlich sein. 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 hinausgeht, bedarf einer eigenen Rechtfertigung, da sie für den ursprünglichen Zweck nicht erforderlich ist.

Guideline des Europäischen Datenschutzausschusses (EDSA) zur Vertragserfüllung bei Online-Diensten (Englisch):
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf

Wann liegt ein „berechtigtes Interesse“ zur Datenspeicherung vor?

Die Mehrzahl der Datenverarbeitungen von Unternehmen kann wohl über die Klausel des „berechtigten Interesses“ vorgenommen werden. Bei dieser Auffangregelung soll eine Abwägung zwischen legitimen Zwecken des Verantwortlichen einerseits und dem Interesse der betroffenen Person am Erhalt ihrer 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.

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 weiterhin ohne Einwilligung der betroffenen Person erfolgen. Beim E-Mail- und Telefon-Marketing sind jedoch zusätzlich die Anforderungen des § 7 Abs. 2 UWG zu beachten, der in der Regel eine ausdrückliche Einwilligung des Betroffenen verlangt.

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

Was gilt bei 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 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 berechtigt, die für die Gehaltsabrechnung erforderlichen Angaben zu Familienstand, Kinderzahl und Religion sowie krankheitsbedingte Fehlzeiten der Mitarbeiter zu speichern.

Kurzpapier der Datenschutzkonferenz zu besonderen Kategorien personenbezogener Daten: https://www.lda.bayern.de/media/dsk_kpnr_17_besondere_kategorien.pdf

Beschäftigtendatenschutz

§ 26 BDSG

Auch personenbezogene Daten von Beschäftigten fallen in den Anwendungsbereich der DSGVO. Der Begriff des Beschäftigten ist im datenschutzrechtlichen Kontext weit auszulegen. Darunter fallen neben Arbeiternehmerinnen und Arbeitnehmern beispielsweise auch Auszubildende, Leiharbeitnehmerinnen und Leiharbeitnehmer sowie Bewerberinnen und Bewerber.

Risiko Radar

Ein Verstoß gegen die Pflichten des § 26 BDSG ist gemäß Art. 83 Abs. 5 lit. d DSGVO mit einem Bußgeldrahmen von bis zu 20 Millionen Euro (bzw. 4 % des weltweiten Jahresumsatzes) sanktioniert.

Welche Besonderheiten gibt es bei der Datenverarbeitung im Beschäftigungskontext?

Der Beschäftigtendatenschutz unterliegt grundsätzlich den allgemeinen Regelungen der DSGVO. Zusätzlich enthält Art. 88 Abs. 1 DSGVO eine Öffnungsklausel, wodurch die Mitgliedstaaten spezifische Vorschriften für die Datenverarbeitungen im Beschäftigungskontext erlassen können. Von dieser Möglichkeit hat Deutschland mit § 26 BDSG Gebrauch gemacht.

Welche Rechtsgrundlagen gibt es im Beschäftigtendatenschutz?

Eine Verarbeitung ist gemäß § 26 BDSG nur dann erlaubt, wenn diese zur Erfüllung der folgenden Zwecke erforderlich ist:

- Datenverarbeitung zum Zweck des Beschäftigungsverhältnisses
  Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, soweit dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist.

- Kollektiv-/ Betriebsvereinbarungen
  Dazu zählen Tarifverträge sowie Betriebs- und Dienstvereinbarungen. Um dabei sicherzustellen, dass das Schutzniveau der DSGVO nicht unterlaufen wird, sind angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interesse und der Grundrechte der betroffenen Person zu ergreifen.

- Zur Aufdeckung von Straftaten
  Danach dürfen Daten zur Aufdeckung von Straftaten verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte vorliegen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur

Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt. Insbesondere dürfen Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sein.

Welche Besonderheiten gibt es beim Erlaubnistatbestand der Einwilligung?

Grundsätzlich besteht nach § 26 BDSG ebenfalls die Möglichkeit Daten auf Grundlage einer Einwilligung des Beschäftigten zu verarbeiten. Eine Schwierigkeit stellt dabei regelmäßig die Voraussetzung der Freiwilligkeit dar, welche aufgrund des Über-/Unterordnungsverhältnis der beteiligten Parteien in den meisten Fällen nicht vorliegt. Nach § 26 BDSG können Beschäftigte zumindest dann freiwillig in eine Datenverarbeitung einwilligen, wenn für die Beschäftigten ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird. Dasselbe gilt, wenn Arbeitgeber und Beschäftigte gleichgelagerte Interessen verfolgen. Die Einwilligung wird in der Praxis deshalb überwiegend in Konstellationen möglich sein, die nicht das Arbeitsverhältnis als solches, sondern Zusatzleistungen des Arbeitgebers betreffen. Eine weitere Besonderheit stellt die Form der Einwilligung dar. Diese muss im Beschäftigtenkontext in der Regel schriftlich vom Beschäftigten eingeholt werden.

> **Praxis-Tipp**
> In Anbetracht der hohen Anforderungen, die an die Freiwilligkeit einer Einwilligung im Beschäftigungsverhältnis gestellt werden, ist es für Sie als Arbeitgeber empfehlenswert, auf diesen Erlaubnistatbestand nur im Notfall zurückzugreifen.

Kurzpapier der Datenschutzkonferenz zum Beschäftigtendatenschutz:
https://www.lda.bayern.de/media/dsk_kpnr_14_beschaeftigtendatenschutz.pdf

Rechte der betroffenen Personen

Art. 12 – 23 DSGVO

Die DSGVO stärkt in besonderem Maße die Rechte der betroffenen Personen. Damit sind diejenigen Personen gemeint, deren personenbezogene Daten verarbeitet werden. Diese sollen zu jedem Zeitpunkt über die Information verfügen, welche sie betreffenden Daten in welcher Weise und zu welchem Zweck verarbeitet werden. Gleichzeitig soll es ihnen ermöglicht werden, aktiv Einfluss auf diese Datenverarbeitungen zu nehmen. Da die Erfüllung von Informationspflichten und die fristgemäße Beantwortung von Anfragen Betroffener zum Teil einiger Vorbereitungen bedürfen, lohnt sich eine genaue Auseinandersetzung mit diesem Thema. Die wichtigsten Betroffenenrechte werden im Folgenden 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 erfüllt werden?

Einer betroffenen Person muss bei jeder Verarbeitung ihrer Daten eine Reihe von Informationen zur Verfügung gestellt werden. Auf diese Weise soll dem Grundsatz der Transparenz maximale Geltung verschafft werden. Unterschieden wird die Erhebung beim Betroffenen selbst (Art. 13 DSGVO) und die Erhebung bzw. Verarbeitung auf andere Weise (Art. 14 DSGVO).

Praxis-Tipp

Als Verantwortliche sind Sie in der Pflicht, alle Personen, die von einer Datenverarbeitung betroffen sind, zu informieren. Neben Datenschutzerklärungen auf Websites, welche dazu dienen, die Website-Besucher zu informieren, gilt es sämtliche weitere „Touchpoints“ zu identifizieren. So sind beispielsweise auch Beschäftigten, Kunden sowie Lieferanten entsprechende Datenschutzinformationen zur Verfügung zu stellen.

Anleitung zur Gestaltung einer Datenschutzerklärung für Websites:
https://www.datenschutzkanzlei.de/datenschutzerklaerung/

Welche Informationen sind bei Direkterhebung zur Verfügung zu stellen?

Werden die Daten direkt bei der betroffenen Person erhoben, sind der betroffenen Person nach Art. 13 DSGVO folgende Informationen zur Verfügung zu stellen:

- Genaue Kontaktdaten des Verantwortlichen, dessen Vertreter sowie ggf. 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 bei der betroffenen Person erhoben werden?

Nahezu identische Pflichten bestehen, wenn die Daten nicht direkt bei der betroffenen Person erhoben werden (Art. 14 DSGVO). Zusätzlich ist in diesem Fall noch anzugeben, aus welcher Quelle die Daten stammen (Art. 14 Abs. 2 lit. f) DSGVO) und welche Kategorien von personenbezogenen Daten betroffen sind (Art. 14 Abs. 1 lit. d) DSGVO).

Gibt es Ausnahmen von der Informationspflicht?

Die Informationspflichten entfallen, soweit die betroffene Person 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 der betroffenen Personen beinhalten.

Welche Formalien sind zu 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 Informationen müssen der betroffenen Person schriftlich oder in anderer Form, gegebenenfalls auch elektronisch zur Verfügung gestellt werden. 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.
- Die Informationen sind der betroffenen Person zum Zeitpunkt der Erhebung zu Verfügung zu stellen. Im Fall einer anderweitigen Erhebung muss die Informationspflicht innerhalb einer angemessenen Frist (maximal 1 Monat) oder beim erstmaligen in Kontakttreten erfüllt werden.

> **Praxis-Tipp**
> Datenschutzinformationen dienen dazu, Ihre einseitigen Informationspflichten als Verantwortliche zu erfüllen und bedürfen deshalb keiner Gegenzeichnung oder Bestätigung der betroffenen Person.

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

Praxishilfe des GDD zu den Transparenzpflichten:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_7.pdf

Welche Auskunftsrechte haben betroffene Personen nach der DSGVO?

Spiegelbildlich zur Informationspflicht für Verarbeitende haben betroffene Personen gemäß Art. 15 DSGVO das Recht, auf Auskunft über die Datenverarbeitung ihrer personenbezogenen Daten 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 elektronischem 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;
- Die Auskunft über die Verarbeitung von personenbezogenen Daten darf nur gegenüber der tatsächlich betroffenen Person erfolgen. Sofern die betroffene Person 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. Doch beachten Sie, dass jede Verweigerung dokumentiert werden muss. Darüber hinaus muss die Verweigerung mit einer Begründung oder mit Tatsachen gegenüber der betroffenen Person belegt werden.

Praxis-Tipp

Das Auskunftsrecht des Art. 15 DSGVO ist vor allem im Endkundengeschäft eines der wichtigsten Rechte der Betroffenen in der DSGVO. Da Auskunftsanfragen regelmäßig den ersten direkten Kontakt zwischen einer betroffenen Person und dem Verantwortlichen darstellen, sollten Sie die Auskunftsanfragen immer mit besonderer Sorgfalt beantworten. Feste Prozesse und klare Zuständigkeiten vereinfachen die Beantwortung!

Anleitung für eine erfolgreiche Auskunftserteilung:
https://www.datenschutzkanzlei.de/auskunftsrechte/

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

Wann müssen personenbezogene Daten 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 EuGHs bekannte Recht soll betroffenen Personen 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 Verarbeitung war von vornherein unrechtmäßig (keiner der Rechtfertigungsgründe des Art. 6 DSGVO war einschlägig);
- Die betroffene Person hat ihre Einwilligung widerrufen;
- Die Daten von Kindern wurden ohne Einwilligung der Erziehungsberechtigten verarbeitet;
- Die Daten sind für die vorgesehenen Zwecke nicht mehr erforderlich (z.B. bei Ende der Vertragsbeziehung);
- Bei einer Datenverarbeitung auf Grundlage eines „berechtigten Interesses“ hat die betroffene Person Widerspruch eingelegt;
- Die Löschung ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht eines Mitgliedstaates erforderlich.

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.

Neben dem Recht auf Löschung besteht das 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 die betroffene Person die Löschung ihrer 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.

Eine deutsche Besonderheit ist in § 35 Abs. 1 BDSG 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 Löschungsanspruchs ein Einschränkungsanspruch.

Was bedeutet das Recht auf Datenübertragbarkeit?

Eine echte Neuerung der DSGVO ist das „Recht auf Datenübertragbarkeit“. Betroffene Personen haben danach 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 die betroffene Person 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 der betroffenen Person 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 der betroffenen Person sein.

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

Datenschutzbeauftragter

Art. 37 - 39 DSGVO, § 38 BDSG

Der Datenschutzbeauftragte ist erste Anlaufstelle, Berater und Unterstützer für alle Fragen hinsichtlich der Verarbeitung personenbezogener Daten, sowohl innerhalb des Unternehmens als auch für die betroffenen Personen 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.

- 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 Personen, dem Umfang und der Verschiedenartigkeit sowie der geographischen Erstreckung der erhobenen Daten.

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 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. Die bereits erfolgten Benennungen bleiben auch mit Einführung der DSGVO

wirksam – für in Deutschland ansässige Unternehmen ergaben sich diesbezüglich also keine wesentlichen Änderungen.

Zudem bestimmt § 38 Abs. 1 Satz 2 BDSG 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 (Rechenschaftspflicht).

Eine freiwillige Ernennung bleibt weiterhin möglich. Allerdings gilt in diesem Fall gemäß § 38 Abs. 2 BDSG 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 Ihres Unternehmens in eine der Kategorien des Art. 37 Abs. 1 DSGVO oder des § 38 Abs. 1 Satz 2 BDSG fällt, benötigen Sie auch dann einen betrieblichen Datenschutzbeauftragten, wenn Sie unter dem Schwellenwert des BDSG 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 Ihnen 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 **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. Die Wahrnehmung gewisser anderer Aufgaben und Tätigkeiten kann zu einem Interessenkonflikt führen, der die Unabhängigkeit 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. So hat beispielsweise das Bayerische Landesamt für Datenschutzaufsicht die Benennung eines IT-Verantwortlichen zum Datenschutzbeauftragten untersagt und mit einem Bußgeld belegt. Der Fall zeigt, dass die Aufsichtsbehörden die Unabhängigkeit des Datenschutzbeauftragten sehr ernst nehmen.

Interner oder 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 Beratungshaftung auf den externen Datenschutzbeauftragten reduziert das Unternehmensrisiko;
- Das Unternehmen bleibt durch den Abschluss eines Dienstvertrages mit dem externen Datenschutzbeauftragten flexibel. Gemäß § 38 Abs. 2 BDSG i.V.m. § 6 Abs. 4 BDSG genießt der interne Datenschutzbeauftragte nämlich besonderen Kündigungsschutz.

> **Praxis-Tipp**
> Die Juristen der Datenschutzkanzlei sind TÜV-zertifizierte Experten auf dem Gebiet des Datenschutzrechts und sind seit 2010 als externe Datenschutzbeauftragte für Unternehmen tätig.

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.

Wie erfolgt die Meldung des Datenschutzbeauftragten bei der Aufsichtsbehörde?

Verantwortliche und Auftragsverarbeiter müssen die Kontaktdaten ihres Datenschutzbeauftragten der zuständigen Aufsichtsbehörde mitteilen. Diese Pflicht ergibt sich aus Art. 37 Abs. 7 DSGVO. In der DSGVO ist aber nicht festgelegt, auf welchem Weg die Meldung erfolgen muss. Grundsätzlich kann die Meldung daher z.B. per E-Mail, Fax oder Brief erfolgen. Einige Aufsichtsbehörden stellen auf ihren Websites auch elektronische Meldeformulare bereit.

Eine Liste der Aufsichtsbehörden und ein Muster für Meldeformular stellen wir hier bereit: https://www.datenschutzkanzlei.de/meldung-dsb/

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 hat in Deutschland aufgrund der Öffnungsklausel keine praktischen Auswirkungen.

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 wirksam eingerichtet werden können. Hohe Bußgelder können auf diese Weise vermieden werden.

Kurzpapier der Datenschutzkonferenz zum Datenschutzbeauftragten:
https://www.lda.bayern.de/media/dsk_kpnr_12_datenschutzbeauftragter.pdf

Verzeichnis von Verarbeitungstätigkeiten

Art. 30 DSGVO

Zur Erfüllung der Dokumentationspflicht müssen Unternehmen ein „**Verzeichnis von Verarbeitungstätigkeiten**“ führen. In diesem sind gemäß Art. 30 DSGVO für alle Verarbeitungstätigkeiten eine Reihe von Informationen zu dokumentieren. Den Aufsichtsbehörden soll es auf diese Weise erleichtert werden, die Verarbeitungsprozesse eines Unternehmens nachvollziehen und deren Rechtmäßigkeit prüfen zu können. Das Verzeichnis sollte sorgfältig geführt werden, um Vorgänge bei Beschwerden oder Kontrollen der Aufsichtsbehörden 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.

Wer muss ein Verzeichnis von Verarbeitungstätigkeiten führen?

Das Verzeichnis von Verarbeitungstätigkeiten muss sowohl von Verantwortlichen als auch von Auftragsverarbeitern in leicht unterschiedlichem Umfang geführt werden. Dabei obliegt die Pflicht dem Verantwortlichen bzw. dem Auftragsverarbeiter selbst und betrifft somit in erster Linie die Unternehmensleitung. In der Praxis wird diese Aufgabe aber häufig auf den betrieblichen Datenschutzbeauftragten delegiert.

Welche Informationen muss das Verzeichnis eines Verantwortlichen enthalten?

Verantwortliche müssen gemäß Art. 30 Abs. 1 DSGVO ein Verzeichnis von (eigenen) Verarbeitungstätigkeiten führen und darin folgende Informationen dokumentieren:

- 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.

Welche Informationen muss das Verzeichnis eines Auftragsverarbeiters enthalten?

Auftragsverarbeiter müssen zusätzlich gemäß Art. 30 Abs. 2 DSGVO ein Verzeichnis der im Auftrag durchgeführten Verarbeitungstätigkeiten führen und darin folgende Informationen dokumentieren:

- 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 und Abs. 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- Wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO.

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).

Mit unserem Generator „SeeYourData“ erstellen Sie ein erstes Verzeichnis von Verarbeitungstätigkeiten in 5 Minuten:
https://www.datenschutzkanzlei.de/verzeichnis_von_verarbeitungstaetigkeiten/

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 kommt diese Ausnahme aber nur sehr selten vor! 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 erfolgt).

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 nun gefordert, ein Verzeichnis für Verarbeitungstätigkeiten gemäß Art. 30 DSGVO zu führen. Wer dies versäumt, riskiert empfindliche Bußgelder.

> **Praxis-Tipp**
> Um den inhaltlichen Anforderungen des Art. 30 DSGVO gerecht zu werden, ist das Verzeichnis von Verarbeitungstätigkeiten stets aktuell zu halten. Sollten Sie bisher kein Verzeichnis führen, ist es höchste Zeit, damit anzufangen.

Hinweise der Datenschutzkonferenz zum Verzeichnis von Verarbeitungstätigkeiten:
https://datenschutz-hamburg.de/dsgvo-information/verzeichnis-verarbeitungstaetigkeiten/

Handreichungen des BayLDA für kleine Unternehmen und Vereine mit Muster-Verzeichnissen für verschiedene Branchen:
https://www.lda.bayern.de/de/kleine-unternehmen.html

Datenschutz-Management-System

Art. 5 Abs. 2 DSGVO, Art. 24 Abs. 1 DSGVO

Wozu dient ein Datenschutz-Management-System?

Die DSGVO fordert ein aktives Management der Datenschutzprozesse. Gemäß Art. 5 Abs. 2 DSGVO und Art. 24 Abs. 1 DSGVO trifft den Verantwortlichen hinsichtlich der ordnungsgemäßen Verarbeitung personenbezogener Daten eine umfassenden Rechenschafts- und Dokumentationsflicht. Bei einer Prüfung durch die Aufsichtsbehörden müssen die Nachweise über eine ordnungsgemäße Datenverarbeitung durch den Verantwortlichen erbracht werden. Dazu müssen Verantwortliche entsprechende Prozesse schaffen, die die Einhaltung der Datenschutzbestimmungen ermöglichen.

Risiko-Radar

Werden die Grundsätze der DSGVO nicht ordnungsgemäß erfüllt und dokumentiert, so drohen gemäß Art 83 Abs. 5 lit. a) DSGVO Geldbußen von bis zu 20.000.000 EUR oder bis zu 4% des gesamten weltweit erzielten Vorjahresumsatzes des Unternehmens.

In welcher Form kann ein Datenschutz-Management-System geführt werden?

Unter einem Datenschutz-Management-System (DSMS) versteht sich die Sammlung aller Dokumentationen, Richtlinien und Maßnahmen, die dazu dienen, dass die Vorgaben des Datenschutzrechts eingehalten werden können. In welcher Form die Einhaltung der DSGVO nachgewiesen werden muss, wird nicht vorgegeben. Wir empfehlen, das DSMS in einem Datenschutz-Handbuch oder einem Wiki zu beschreiben, um Nachweisbarkeit sowie Überprüfbarkeit gewährleisten zu können. Das Handbuch kann als Nachschlagewerk dienen und ist allen Beschäftigten zur Verfügung zu stellen.

Welche Prozesse sollten ein Datenschutz-Management-System steuern?

In einem Datenschutz-Management-System sollten sämtliche Anforderungen aus der DSGVO für die Unternehmenspraxis geregelt und dokumentiert werden.

Beispielhafte Übersicht der zu dokumentierenden Prozesse im Rahmen eines DSMS:

- Umsetzung der Datenschutz-Grundsätze (Art. 5 Abs. 1 DSGVO)
- Wahrung der Rechte der betroffenen Personen (Art. 12-21 DSGVO)
- Auswahl und Kontrolle von Auftragsverarbeitern (Art. 28 DSGVO)
- Pflege der Datenschutzdokumentation (Art. 30 DSGVO)
- Gewährleistung der Datensicherheit (Art. 32 DGSVO)

- Umgang mit Datenschutzvorfällen (Art. 33, 34 DSGVO)
- Datenschutz-Folgenabschätzung (Art. 35 DSGVO)
- Einbindung des DSB (Art. 38 Abs. 1 DSGVO)
- Schulung und Sensibilisierung der Beschäftigten

Praxis-Tipp

Ein Datenschutz-Management-System hilft Ihnen dabei, datenschutzrechtliche Themen und Prozesse in der täglichen Praxis zu organisieren und Zuständigkeiten zu klären. Auf diese Weise kann die Einhaltung der DSGVO deutlich vereinfacht werden!

Wir haben ein ausgereiftes Framework für ein DSMS, welches sich mit überschaubarem Aufwand auf Ihr Unternehmen anpassen lässt und den Dokumentationsaufwand auf ein Minimum reduziert. Gerne unterstützen wir Sie dabei, die erforderlichen Prozesse mit Ihnen zu entwickeln.

Risikoanalyse und Datenschutz-Folgenabschätzung

Art. 24 Abs. 1 und Art. 35, 36 DSGVO

Was versteht sich unter „risikobasierter Ansatz“?

Die DSGVO folgt einem risikobasierten Ansatz. Maßgebliche Norm ist Art. 24 Abs. 1 DSGVO, wonach der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umsetzen muss. Die Norm ist eng verzahnt mit Art 25 Abs. 1 DSGVO (Datenschutz durch Technikgestaltung) und Art. 32 DSGVO (Sicherheit der Verarbeitung).

Wozu dient eine Risikoanalyse?

Im Rahmen einer Risikoanalyse müssen die Risiken für die Rechte und Freiheiten der betroffenen Personen objektiv bewertet werden. Dabei sind Art, Umfang, Umstände und Zwecke der Verarbeitung als Risikofaktoren zu berücksichtigen. Sie müssen unter Berücksichtigung der Schwere möglicher Schäden für die betroffenen Personen und der jeweiligen Eintrittswahrscheinlichkeit bewertet werden. Als praktische Arbeitshilfe kann Erwägungsgrund 75 der DSGVO konsultiert werden.

Aus der Risikoanalyse lassen sich technische und organisatorische Maßnahmen ableiten, die in einem angemessenen Verhältnis zum Risiko der Verarbeitung stehen müssen. Ziel ist es, durch geeignete Maßnahmen das Risiko kalkulierbar zu machen und soweit einzudämmen, dass bei einer objektiven Bewertung kein hohes Risiko mehr für die Rechte und Freiheiten der betroffenen Personen besteht. So lassen sich die potenziellen Risiken einer Verarbeitung durch Maßnahmen wie z.B. Datenminimierung (Pseudonymisierung, Anonymisierung), Verschlüsselung, Identitäts- und Berechtigungsmanagement sowie Transparenz und Gewährleistung der Rechte der Betroffenen absenken.

> Praxis-Tipp
> Die Risikoanalyse nach Art. 24 Abs. 1 DSGVO ist als Regelfall zu verstehen, während eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO nur in Ausnahmefällen erforderlich ist.

Wann ist eine Datenschutz-Folgenabschätzung vorzunehmen?

Eine Datenschutz-Folgenabschätzung ist gemäß Art. 35 DSGVO vor Einführung der Datenverarbeitung durchzuführen, wenn die Risikobewertung zu dem Ergebnis führt, dass die Verarbeitung (trotz technischer und organisatorischer Maßnahmen) voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat.

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 ausgenommen);
- 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.

Die Aufsichtsbehörden haben gemäß Art. 35 Abs. 4 DSGVO die Möglichkeit, Positiv- sowie Negativlisten zu veröffentlichen mit konkreten Verarbeitungsvorgängen, bei denen ein hohes Risiko anzunehmen ist und daher stets eine Datenschutz-Folgenabschätzung durchzuführen ist. Es ist daher genau zu prüfen, ob die Datenverarbeitungen die Kriterien dieser Listen erfüllen und eine Datenschutz-Folgenabschätzung daher unabhängig vom Ausgang der eigenen Risikoanalyse vorzunehmen ist.

Positiv-Liste der deutschen Aufsichtsbehörden:
https://datenschutz-hamburg.de/dsgvo-information/art-35-mussliste-nicht-oeffentlich

Praxis-Tipp

Es ist nachweisbar sicherzustellen, dass die Vorschriften der DSGVO eingehalten werden und die Verarbeitung in rechtmäßiger Weise erfolgt. Als Verantwortlicher müssen Sie daher einen Prozess etablieren, der bei Einführung einer neuen Datenverarbeitung eine Analyse des Risikos für die Rechte und Freiheiten der betroffenen Person beinhaltet. Anhand dieser Risikoanalyse wird dann entschieden, ob die Verarbeitungstätigkeit die Relevanzschwelle zur Durchführung einer Datenschutz-Folgenabschätzung erreicht. Risikoanalyse und Datenschutz-Folgenabschätzung sind zu dokumentieren.

Wie wird eine Datenschutz-Folgenabschätzung durchgeführt?

Die DSGVO macht keine Vorgaben zur praktischen Durchführung einer Datenschutz-Folgenabschätzung, sondern verhält sich „Methodik-neutral“. Aus Art. 35 Abs. 7 DSGVO sowie Erwägungsgrund 84 lassen sich aber die Mindestinhalte ableiten. Zudem gibt es mittlerweile verschiedene Leitfäden von Branchenverbänden und Aufsichtsbehörden, die Orientierung bieten können. Die französische Aufsichtsbehörde CNIL bietet ein Software-Tool an, welches strukturiert durch den Prozess führt.

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.

Bei der Durchführung der Datenschutz-Folgenabschätzung ist gemäß Art. 35 Abs. 2 DSGVO der Rat des Datenschutzbeauftragten einzuholen, sofern ein solcher benannt wurde.

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.

Software-Tool der französische Aufsichtsbehörde CNIL:
https://www.datenschutz-bayern.de/technik/pia-tool.html.de (DE)
oder https://www.cnil.fr/en/privacy-impact-assessment-pia (EN)

Fallbeispiel einer Datenschutz-Folgenabschätzung der bayerischen Aufsichtsbehörde:
https://www.lda.bayern.de/media/03_dsfa_fallbeispiel_baylda_iso29134.pdf

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

Was ist, wenn die Datenschutz-Folgenabschätzung ein hohes Risiko bestätigt?

Bestätigt sich im Rahmen der Datenschutz-Folgenabschätzung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen, muss noch vor Durchführung des Verarbeitungsvorgangs die zuständige Aufsichtsbehörde konsultiert werden. Diese soll so die Möglichkeit erhalten, auf kritische Verarbeitungen Einfluss zu nehmen und geeignete Maßnahmen vorzuschlagen.

Der Verantwortliche stellt der Aufsichtsbehörde bei einer Konsultation folgende Informationen zur Verfügung (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.

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 dazu aufgefordert, datenschutzfreundliche Techniken einzusetzen („Data Protection by Design“) sowie Produkte oder Dienstleistungen mit datenschutzfreundlichen Voreinstellungen anzubieten („Data Protection 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

Bei Verstößen gegen technische und organisatorische Vorgaben 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, je nachdem was höher ist.

Was bedeutet „Datenschutz durch Technikgestaltung“?

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.

Schon in der Entwicklungsphase und sodann fortlaufend hat der Verantwortliche gemäß Art. 25 Abs. 1 DSGVO geeignete technische und organisatorische Maßnahmen zu treffen, die dafür ausgelegt sind, die in Art. 5 Abs. 1 DSGVO enthaltenen Datenschutzgrundsätze wirksam umzusetzen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Personen zu schützen („Datenschutz durch Technikgestaltung“ bzw. „Data Protection by Design“).

Der Verantwortliche hat bei der Entwicklung von Verarbeitungstechnologien die Grundsätze des Art. 5 Abs. 1 DSGVO zu beachten und nach Möglichkeit in diese einzubetten. Weitere konkrete Vorgaben zur Technikgestaltung wurden durch den Gesetzgeber nicht formuliert. Dem Verantwortlichen obliegt es stattdessen selbst, geeignete präventive Maßnahmen zur Umsetzung der Datenschutzgrundsätze zu treffen. Dabei muss die Gestaltung der Technologie nicht in der bestmöglichsten Weise erfolgen. Dem Verantwortlichen ist vielmehr ein risikobasierter Beurteilungsspielraum hinsichtlich der Auswahl geeigneter Maßnahmen eingeräumt, der sich am Stand der Technik, den Kosten der Implementierung und den Risiken für die Betroffenen orientieren soll. Art. 24 Abs. 1 DSGVO sowie die beispielhafte Aufzählung von Maßnahmen in Art. 32 Abs. 1 DSGVO können dabei als Orientierung dienen.

Was sind „datenschutzfreundliche Voreinstellungen“?

Nach Art. 25 Abs. 2 DSGVO ist der Verantwortliche verpflichtet, durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass durch Voreinstellung nur die personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind („datenschutzfreundliche Voreinstellungen“ bzw. „Data Protection by Default“).

Unter Voreinstellungen wird üblicherweise eine Konfiguration verstanden, die initialisiert ist und die sich ändern lässt. Dazu gehört aber auch, ob eine Verarbeitung, bspw. eine Veröffentlichung von Daten, automatisch erfolgt oder ob vorher eine Interaktion mit den Nutzenden erforderlich ist. Verarbeitungstechnologien sind daher in ihren „Werkeinstellungen“ datenschutzfreundlich auszurichten. Mit Anpassung der Einstellungen oder durch gezielte Freigaben durch den Nutzer ist eine Erweiterung der Datenverarbeitung aber durchaus möglich. Die Idee dahinter ist: Wer seine Voreinstellungen nicht ändert, setzt sich keinem erhöhten Risiko aus.

Die Vorschriften des Art. 25 DSGVO sind für den Verantwortlichen zwingende Verpflichtungen. Ein Verstoß kann durch die Aufsichtsbehörden mit einem Bußgeld geahndet werden. Außerdem könnte die Behörde die Fortsetzung der Verarbeitung verbieten, was einem Verbot der Verarbeitungssoftware gleichkäme.

Risiko-Radar

Die Vorschriften des Art. 25 DSGVO sind für den Verantwortlichen zwingende Verpflichtungen. Ein Verstoß kann durch die Aufsichtsbehörden mit einem Bußgeld geahndet werden. Außerdem könnte die Behörde die Fortsetzung der Verarbeitung verbieten, was einem Verbot der Verarbeitungssoftware gleichkäme.

Welche technischen Maßnahmen müssen getroffen werden?

Welche konkreten Sicherheitsmaßnahmen angewendet werden müssen, hängt vom Umfang der Datenverarbeitung und dem Risiko für die Rechte und Freiheiten der natürlichen 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.

Welche organisatorischen Maßnahmen müssen getroffen werden?

Unter organisatorische Maßnahmen fallen all solche Maßnahmen, die durch Handlungsanweisung, Verfahrens- und Vorgehensweisen umgesetzt werden können. Der Risikofaktor Mensch spielt hierbei eine große Rolle. Durch konkrete Anweisungen und feste Prozesse zum Umgang mit personenbezogenen Daten, Schulungsmaßnahmen sowie geeignete Richtlinien beispielsweise zur IT-Nutzung kann zur Sicherheit der Daten beigetragen werden. In diesem Zusammenhang spielt auch die Verpflichtung auf Vertraulichkeit eine wichtige Rolle. Nach Art. 29 DSGVO dürfen Personen, die mit personenbezogenen Daten in Berührung kommen, diese ausschließlich auf Weisung des Verantwortlichen verarbeiten. Aus Nachweisgründen sind die Beschäftigten darüber zu belehren und auf die Vertraulichkeit von Daten zu verpflichten.

> **Praxis-Tipp**
> Vor allem für Auftragsverarbeiter ist die Etablierung technischer und organisatorischer Maßnahmen von großer Bedeutung. In ihrer Rolle als Verarbeiter im Auftrag liegt der Schutz der Daten des Auftraggebers in ihren Händen. Ein Datensicherheitskonzept kann somit zusätzlich einen Wettbewerbsvorteil darstellen. Eine saubere und sorgfältige Dokumentation der technischen und organisatorischen Maßnahmen der Datensicherheit sind dafür unerlässlich.

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 nun auch Auftragsverarbeiter mit einem Bußgeld belastet werden.

Unternehmen sollten ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung etablieren, sodass dauerhaft ein angemessenes Schutzniveau gewährleistet werden kann. 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 technischen und organisatorischen Maßnahmen dringend zu empfehlen.

Pflichten bei Datenpannen

Art. 33, 34 DSGVO

Besondere Pflichten treffen einen Verantwortlichen, wenn der Schutz personenbezogener Daten verletzt wurde.

Risiko-Radar
Kehren Sie Datenschutzvorfälle nicht unter den Teppich. Bei Verstößen gegen die Melde- oder Benachrichtigungspflicht 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.

Was ist ein Datenschutzvorfall?

Ein Datenschutzvorfall umfasst jedweden (potenziellen) unberechtigten Zugriff auf die bei einem Verantwortlichen oder einem Auftragsverarbeiter gespeicherten Daten. Dabei ist unerheblich, ob dieser Zugriff in böser Absicht erfolgt oder nicht. Beispielhaft für eine Datenpanne ist der Hack eines Unternehmensservers, durch den Kundendaten in das Internet gelangen. Eine Datenpanne kann aber schon vorliegen, wenn eine E-Mail an einen falschen Empfänger gesendet oder ein Diensthandy im Zug vergessen wurde.

Wann liegt ein meldepflichtiger Datenschutzvorfall vor?

Sofern ein Risiko für die Rechte und Freiheiten einer natürlichen Person nicht ausgeschlossen werden kann, muss die Datenpanne an die zuständige Aufsichtsbehörde gemeldet werden. Ob dabei 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). Zum anderen kann ein Risiko aber wieder eingedämmt worden sein, wenn der Verantwortliche rechtzeitig entsprechende Gegenmaßnahmen vorgenommen hat, um das Datenleck zu schließen.

Kurzpapier der Datenschutzkonferenz zum Risiko für die Rechte und Freiheiten natürlicher Personen
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf

Was muss der Aufsichtsbehörde gemeldet werden?

Im Fall einer meldepflichtigen 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).

Einige Aufsichtsbehörden bieten die Möglichkeit, Datenpannen über ein Onlineformular zu melden. Eine Übersicht gibt es hier: https://www.datenschutzkanzlei.de/meldung-datenpanne/

Wann müssen die betroffenen Personen benachrichtigt werden?

Die Benachrichtigung der betroffenen Personen 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 Person haben.

Die Pflicht zur Benachrichtigung betroffener Personen 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, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen 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).

Wie müssen die betroffenen Personen benachrichtigt werden?

Wenn eine Benachrichtigungspflicht besteht, müssen die betroffenen Personen in klarer und einfacher Sprache benachrichtigt werden. Die Benachrichtigung muss folgende Informationen enthalten (Art. 34 Abs. 2, Abs. 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.

Müssen Datenschutzvorfälle dokumentiert werden?

Um der Aufsichtsbehörde die nachträgliche Kontrolle der Einhaltung aller Pflichten zu ermöglichen, sind Datenpanne vom Verantwortlichen zu 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 steuern. 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 und ggf. in Rücksprache mit der Aufsichtsbehörde erfolgen. Die Dokumentation der Vorfälle und Maßnahmen muss auch in Ausnahmesituationen stets erfolgen

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

Gemeinsame Verantwortlichkeit

Art. 26 DSGVO

Das Konstrukt der gemeinsam für die Verarbeitung Verantwortlichen in der DSGVO stellt eine Neuerung dar. Gemäß Art. 26 Abs. 1 DSGVO sind dabei mehrere Stellen gemeinsam für die Verarbeitung Verantwortliche, wenn sie gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen.

Risikoradar

Besteht eine gemeinsame Verantwortlichkeit, ohne dass darüber eine Vereinbarung getroffen wurde, können hierfür gemäß Art. 83 Abs. 4 Buchst. a) DSGVO Geldbußen von bis zu 10.000.000 EUR oder bis zu 2% des gesamten weltweit erzielten Vorjahresumsatzes des Unternehmens verhängt werden.

Wann liegt gemeinsame Verantwortlichkeit vor?

Eine gemeinsame Verantwortlichkeit kommt dann in Betracht, wenn zwei oder mehr Verantwortliche gemeinsame über die Zwecke und Mittel der Verarbeitung bestimmen. Sie setzt voraus, dass jeder der Beteiligten einen bestimmenden tatsächlichen Einfluss auf die Datenverarbeitung nimmt. Die Beteiligung kann hierbei verschiedene Formen annehmen und muss nicht gleichmäßig verteilt sein.

So hat beispielsweise der Europäische Gerichtshof entschieden, dass Facebook als Anbieter der gleichnamigen Plattform und Unternehmen, die auf dieser Plattform eine Fanpage betreiben, gemeinsam Verantwortliche bei der Erhebung personenbezogener Daten der Endnutzer sind. Dies folgt daraus, dass Facebook die Daten (auch) für eigene Zwecke verwendet und der Fanpage-Betreiber die Datenverarbeitung zumindest mittelbar beeinflusst. Weitere Beispiele für gemeinsame Verantwortlichkeit finden sich häufig in Unternehmensgruppen, bei denen einzelne Unternehmen eigenverantwortlich Datenverarbeitungen als „Shared Services“ für die Gruppe übernehmen (z.B, gemeinsame Personalverwaltung oder gemeinsames Data Warehouse).

Welche Pflichten haben gemeinsam Verantwortliche?

Die gemeinsam Verantwortlichen müssen eine Vereinbarung schließen, in welcher sie in transparenter Form festlegen, wer welche DSGVO-Pflichten wahrnimmt. Insbesondere geht es hierbei um den Schutz der Daten durch geeignete technische und organisatorische Maßnahmen sowie um die Informationspflichten und die Gewährleistung der Rechte der betroffenen Personen. Die Vereinbarung muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln.

Die wesentlichen Inhalte der Vereinbarung müssen den betroffenen Personen zur Verfügung gestellt werden. Auf diese Weise soll die Transparenz gefördert und die Rechtsdurchsetzung für die betroffenen Personen vereinfacht werden. Unabhängig von der konkreten Regelung der Vereinbarung kann die betroffene Person ihre Rechte bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

Wer haftet für Schäden bei einer gemeinsamen Verantwortlichkeit?

Jeder der gemeinsam Verantwortliche haftet nach Art. 82 DSGVO im Falle rechtswidriger Verarbeitung für den gesamten Schaden, sofern er nicht sein fehlendes Verschulden nachweisen kann.

Ist Art. 26 DSGVO eine Rechtsgrundlage für die gemeinsame Datenverarbeitung?

Bei einer gemeinsamen Verantwortlichkeit stehen die transparente Aufteilung und Dokumentation der DSGVO-Pflichten im Vordergrund. Die Vereinbarung über die gemeinsame Verantwortlichkeit ist aber kein Ersatz für eine Rechtsgrundlage. Alle beteiligten Verantwortliche benötigen weiterhin eine eigene Rechtsgrundlage zur Verarbeitung der Daten. Auch die Übermittlung von Daten zwischen den Verantwortlichen bedarf einer Rechtsgrundlage und ist ohne eine solche unrechtmäßig.

Kurzpapier der Datenschutzkonferenz zur gemeinsam für die Verarbeitung Verantwortliche:
https://www.lda.bayern.de/media/dsk_kpnr_16_gemeinsam_verantwortliche.pdf

Auftragsverarbeitung

Art. 28 DSGVO

Die Verarbeitung personenbezogener Daten in einem Unternehmen wird oftmals ganz oder zum Teil von externen Dienstleistern, sogenannten Auftragsverarbeitern, übernommen. 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 Lettershop-Leistungen, die Auslagerung der Datenspeicherung (Hosting) und Datenverarbeitung (Software-as-a-Service) in die Cloud oder auch die Aktenvernichtung durch spezialisierte Dienstleister.

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. Auftragsverarbeitern drohen auch Schadenersatzforderungen von betroffenen Personen (Art. 82 Abs. 2 DSGVO) und von Auftraggebern (Art. 28 Abs. 4 DSGVO).

Kurzpapier der Datenschutzkonferenz zur Auftragsverarbeitung:
https://www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf

Unter welchen Voraussetzungen ist Auftragsverarbeitung zulässig?

Anders als bei der gemeinsamen Verantwortlichkeit, liegt die Entscheidung über die Mittel und Zwecke der Datenverarbeitung allein beim Verantwortlichen. Der Datenempfänger darf die Datenverarbeitung daher ausschließlich auf Weisung des Verantwortlichen vornehmen (Art. 28 Abs. 3 Satz 2 lit. a), Art. 29 DSGVO).

Der Verantwortliche ist in der Pflicht, den Auftragsverarbeiter sorgfältig auszuwählen und zu kontrollieren. Im Gegenzug hat 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. PDF) erfolgen kann (Art. 28 Abs. 9 DSGVO).

Vertragsmuster und Praxishinweis des GDD zur Auftragsverarbeitung:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_4.pdf
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_12.pdf

Unser Blogbeitrag zum elektronischen Vertragsschluss des AV-Vertrages:
https://www.datenschutzkanzlei.de/elektronischer-vertragsschluss-der-auftragsverarbeitung-art-28-dsgvo/

Welche Pflichten treffen den Auftraggeber?

Erwägt ein Verantwortlicher, einen Teil der Datenverarbeitung durch externe Dienstleister 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).
- 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 verpflichtet, ein Verzeichnis seiner im Auftrag durchgeführte Verarbeitungen zu führen (Art. 30 Abs. 2 DSGVO). Einzelheiten werden im Kapitel „Dokumentationspflicht“ beschrieben.

> Praxis-Tipp
> Wenn Sie personenbezogene Daten im Auftrag verarbeiten, sollten Sie, sofern noch nicht geschehen, ein Augenmerk auf eine präzise Dokumentation legen. Die DSGVO enthält eine Reihe von Pflichten für Sie bereit!

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 nun auch elektronisch geschlossen werden können.

Datenübermittlung in Drittstaaten

Art. 44 ff. DSGVO

Während bei einer Datenübertragung innerhalb von EU-Mitgliedstaten und des EWR lediglich die allgemeinen Rechtfertigungstatbestände des Art. 6 DSGVO gelten, bestehen im Falle einer Übermittlung in Drittstaaten (Staaten außerhalb der EU und des EWR) zusätzliche Anforderungen.

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.

Was ist bei einer Datenübermittlung in Drittstaaten zu beachten?

Im Falle einer Datenübermittlung in Drittstaaten ist eine zweistufige Prüfung vorzunehmen. Zunächst muss, wie bei Datenübermittlungen im Inland bzw. Übermittlungen in das EU-Ausland, eine Rechtsgrundlage des Art. 6 DSGVO vorliegen. Ist dies der Fall, muss in einem zweiten Schritt festgestellt werden, ob beim Empfänger der Daten ein angemessenes Datenschutzniveau vorliegt.

Für die Feststellung des angemessenen Datenschutzniveaus sieht die DSGVO verschiedene 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). Angemessenheitsbeschlüsse gibt es für: Andorra, Argentinien, Färöer-Inseln, Guernsey, Isle of Man, Israel, Japan, Jersey, Kanada (eingeschränkt), Neuseeland, Schweiz und Uruguay.
    - **Sonderfall USA:** Die Angemessenheitsentscheidung der EU-Kommission sieht außerdem ein angemessenes Datenschutzniveau für Unternehmen mit Sitz in den USA vor, sofern diese sich dem Selbstzertifizierungsmechanismus des **EU-US Privacy Shield** unterzogen haben.

Zertifizierte Unternehmen werden in dieser Liste des U.S. Department of Commerce geführt: https://www.privacyshield.gov/list

- 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-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.
    - **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
> Das EU-US Privacy Shield steht immer wieder in der Kritik, kein angemessenes Schutzniveau zu bieten. Da eine Verwerfung durch den EuGH nicht auszuschließen ist, sollten Sie Datenübermittlungen in die USA nach Möglichkeit nicht ausschließlich auf dieses Abkommen stützen. 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 der betroffenen Person** (Art. 49 Abs. 1 lit. a) DSGVO). Über die allgemeinen Anforderungen an eine Einwilligung hinaus muss die betroffene Person

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 der betroffenen Person (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 Entscheidung des EuGHs, die etwa das Privacy Shield-Abkommen oder die EU-Standarddatenschutzklauseln betreffen könnten. 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

Weiterführende Dokumente und Gesetzestexte (Links)

Eine gelungene Darstellung der einschlägigen Gesetzestexte der DSGVO, der Erwägungsgründen zur DSGVO und des BDSG finden Sie hier:
https://dsgvo-gesetz.de/

Für eine interaktive Darstellung der DSGVO empfehlen wir Ihnen ein Informationsportal der Europäischen Kommission, welches sich an kleine und mittlere Unternehmen richtet (deutsche Version):
https://ec.europa.eu/justice/smedataprotect/index_de.htm

Eine nach Zielgruppen organisierte Informationssammlung mit Kurzpapieren, Stellungnahmen, Leitfäden und Anleitungen bietet die Stiftung Datenschutz:
https://www.stiftungdatenschutz.org/dsgvo-info/

Das BayLDA stellt Handreichungen für kleine Unternehmen und Verein sowie alle Kurzpapiere der Datenschutzkonferenz zum Abruf bereit:
https://www.lda.bayern.de/de/datenschutz_eu.html

Zusammen mit der ZEIT Akademie haben wir ein Videoseminar zur DSGVO herausgebracht. In 9 Lektionen erhalten Sie einen kompakten Überblick über die Anforderungen der DSGVO an Unternehmen mit praktischen Umsetzungstipps:
https://www.zeitakademie.de/seminare/business/dsgvo

Dieses Whitepaper wird regelmäßig aktualisiert. Die aktuelle Version steht stets auf der Website der Datenschutzkanzlei zum kostenfreien Abruf bereit:
https://www.datenschutzkanzlei.de

Ausgewählte Leistungen im Datenschutzrecht

Anwaltliche Beratung

Datenschutz-Management und DSGVO-Beratung

Wir Unterstützung bei der Umsetzung der DSGVO und der Gestaltung passender Datenschutzkonzepte. Beratung in Einzelfragen, projektbegleitend oder als Sparringpartner, z.B. für den Datenschutzbeauftragten oder das Marketing. Rechtliche Absicherung, wenn Daten das Unternehmen und/oder die EU verlassen, z.B. bei Software-as-a-Service, Plattformen und Datentransfer im Konzern. Beratung u.a. bei der Wahrung von Betroffenenrechten, der Durchführung von Datenschutz-Folgenabschätzungen und bei der Meldung von Datenschutzvorfällen.

Online-Marketing und klassische Werbung

Website, Online-Shop, Social Media, Newsletter und Apps – wir prüfen den Internetauftritt und gestalten die passenden Datenschutzerklärungen und sonstigen Pflichtangaben (Impressum). Beratung zu Tracking, Analytics, Adserver und E-Mail-Marketing. Rechtliche Prüfung von Marketingkampagnen und Werbemitteln.

Legal Services

Externer Datenschutzbeauftragter

Die TÜV-zertifizierten Juristen der Herting Oberbeck Datenschutz GmbH können von Unternehmen und Organisationen zum externen Datenschutzbeauftragten benannt werden.

EU-Inlandsvertreter

Die Herting Oberbeck Datenschutz GmbH kann als EU-Inlandsvertreter i.S.d. Art. 27 DSGVO für Unternehmen aus Drittstaaten benannt werden.

Schulungen & Vorträge

Wir bieten Schulungen, Workshops und Vorträge zu verschiedenen Datenschutzthemen an. Außerdem schulen wir Datenschutzbeauftragte, Führungskräfte, Fachabteilungen und ganze Teams. Als individueller Workshop, Inhouse-Schulung oder mit praktischen Online-Kursen. Die Juristen der Datenschutzkanzlei sind erfahrene Referenten und verstehen es, auch komplexe Themen greifbar und verständlich zu vermitteln.

Haben wir Ihr Interesse geweckt?

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 auf Ihre Anfrage!