

Datenschutz für Unternehmen

(fast) 100 Antworten zu den
wichtigsten Anforderungen aus
DSGVO, BDSG und TDDDG





Datenschutz für Unternehmen

**(fast) 100 Antworten zu den
wichtigsten Anforderungen aus
DSGVO, BDSG und TDDDG**

**2024
Version 3.4**

Herausgeber

DATENSCHUTZKANZLEI
Herting Oberbeck Rechtsanwälte Partnerschaft
Hallerstraße 76, 20146 Hamburg

Telefon +49. 40. 226 34 56 0
E-Mail info@datenschutzkanzlei.de
Web datenschutzkanzlei.de

Wir stellen dieses eBook kostenfrei zur Verfügung und es freut uns, wenn wir Sie damit bei der Umsetzung der Datenschutzregelungen unterstützen können. Nutzen Sie es also und leiten Sie es auch gerne an Ihre Arbeitskolleg:innen oder Geschäftspartner:innen weiter. Die Veröffentlichung – auch in Auszügen – oder die Entfernung von Logos, Kontaktdaten oder anderen Hinweisen auf die Urheberschaft ist hingegen nur mit unserer schriftlichen Einwilligung erlaubt.

Das eBook wurde nach bestem Wissen erstellt und gibt den Rechtsstand vom Zeitpunkt der Erstellung wieder. Es dient einem ersten Überblick und ersetzt nicht die anwaltliche Beratung.

Vorwort

Liebe Leserin, lieber Leser,

die Datenschutz-Grundverordnung (DSGVO) gilt nun bereits seit mehreren Jahren. Die 2018 bei den meisten Unternehmen vorherrschende Unruhe ist mittlerweile größtenteils einer gesicherten Routine gewichen. Die Aufsichtsbehörden haben mit Leitlinien und Orientierungshilfen dazu beigetragen, die DSGVO für die Praxis handhabbar zu machen. In gerichtlichen Verfahren wurden die datenschutzrechtlichen Konturen weiter geschärft, aber auch neue Fragen aufgeworfen. Datenschutz wird damit mit jedem Tag zu einer komplexeren Angelegenheit.

Mit den vorliegenden Praxisleitfaden möchten wir Ihnen einen Einstieg und Überblick in die Grundlagen des Datenschutzrechts ermöglichen. Wir haben unsere Erfahrungen aus der anwaltlichen Beratung und aus der Tätigkeit als externe Datenschutzbeauftragte einfließen lassen. Mit Risikoeinschätzungen und wertvollen Praxis-Tipps ordnen wir die Anforderungen für Sie ein.

Ein großer Dank gilt unseren (teilweise ehemaligen) juristischen Mitarbeiter:innen Hanno Dormagen, Phillip Malinowski, Anna-Lea Burgdorf, Melina Voss, Louisa El-Dbeissi und Moritz Marks, die an der Erstellung des eBooks mitgewirkt haben und dieses von Version zu Version besser machen.

Dieses eBook wird regelmäßig aktualisiert und sukzessive ausgebaut. Die erste Version haben wir im Oktober 2016 veröffentlicht und seitdem mehrfach überarbeitet.

Die aktuelle Version des eBooks finden Sie stets auf unserer Website 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 und Onlinerecht entgehen. Wir freuen uns auf Ihren Besuch!

Hamburg im Juni 2024

Ihr Team der Datenschutzkanzlei

Inhaltsverzeichnis

Vorwort	2
Inhaltsverzeichnis	3
Über die Datenschutzkanzlei	6
Rechtliche Beratung für Daten, Technologie und Marketing	6
Externer Datenschutzbeauftragter	6
Beratung interner Datenschutzbeauftragter	6
Grundsatzfragen	7
Was regelt die DSGVO?	7
Was regelt das BDSG?	7
Was regelt das TDDDG?	7
DSGVO, BDSG, TDDDG – was gilt denn jetzt?	8
Herrscht in Europa ein einheitlicher Datenschutz?	9
Für wen gelten die Datenschutzbestimmungen?	10
Wer ist „Verantwortlicher“?	10
Was bedeutet „Verarbeitung“ von Daten?	10
Was sind „personenbezogene Daten“ und „betroffene Personen“?	11
Welchen Stellenwert haben die Grundsätze der Datenverarbeitung?	11
Was bedeutet „Rechtmäßigkeit der Verarbeitung“?	11
Was bedeutet „Verarbeitung nach Treu und Glauben“?	12
Was bedeutet „Transparenz der Datenverarbeitung“?	12
Was bedeutet „Zweckbindung“?	12
Was bedeutet „Datenminimierung“?	13
Was bedeutet „Richtigkeit“?	13
Was bedeutet „Speicherbegrenzung“?	14
Was bedeutet „Integrität und Vertraulichkeit“?	14
Was bedeutet die „Rechenschaftspflicht“ für die Praxis?	15
Verarbeitung von personenbezogenen Daten	16
Welche Anforderungen gelten für eine Einwilligung einer betroffenen Person?	17
Was gilt für die Einwilligung zu Cookies?	17
Wie müssen Cookie-Banner gestaltet sein?	18
Was gilt bei Einwilligungen von Kindern?	18
Wann kann die Einwilligung widerrufen werden?	18
Wann ist eine Datenverarbeitung für die Erfüllung eines Vertrags „erforderlich“?	19
Wann liegt ein „berechtigtes Interesse“ zur Datenspeicherung vor?	19
Was gilt bei sensiblen Daten?	20
Beschäftigtendatenschutz	21
Welche Besonderheiten gibt es bei der Datenverarbeitung im Beschäftigungskontext?	21
Welche Rechtsgrundlagen gibt es im Beschäftigtendatenschutz?	21
Welche Besonderheiten gibt es beim Erlaubnistatbestand der Einwilligung?	22
Rechte der betroffenen Person	23

Welche Informationspflichten müssen erfüllt werden?	23
Welche Informationen sind bei Direkterhebung zur Verfügung zu stellen?	23
Was gilt, wenn Daten nicht direkt bei der betroffenen Person erhoben werden?	24
Gibt es Ausnahmen von der Informationspflicht?	24
Welche Formalien sind zu beachten?	24
Welche Auskunftsrechte haben betroffene Personen nach der DSGVO?	25
Wann müssen personenbezogene Daten dauerhaft gelöscht werden?	26
Was ist mit Daten, die (noch) nicht gelöscht werden können?	27
Was bedeutet das Recht auf Datenübertragbarkeit?	27
Gemeinsame Verantwortlichkeit	28
Wann liegt eine gemeinsame Verantwortlichkeit vor?	28
Welche Pflichten haben gemeinsam Verantwortliche?	28
Wer haftet für Schäden bei einer gemeinsamen Verantwortlichkeit?	29
Ist Art. 26 DSGVO eine Rechtsgrundlage für die gemeinsame Datenverarbeitung?	29
Auftragsverarbeitung	30
Unter welchen Voraussetzungen ist eine Auftragsverarbeitung zulässig?	30
Welche Form muss der Vertrag mit einem Auftragsverarbeiter haben?	30
Welche Pflichten treffen den Auftraggeber?	30
Welche Pflichten treffen den Auftragsverarbeiter?	31
Was bedeuten die Regelungen für die Praxis?	32
Datenschutzbeauftragte:r	33
Wann muss ein:e Datenschutzbeauftragte:r benannt werden?	33
Was gilt für Konzerne und Unternehmensgruppen?	34
Was sind die Aufgaben des oder der Datenschutzbeauftragten?	34
Welche Voraussetzungen müssen Datenschutzbeauftragte erfüllen?	35
Interne oder externe Datenschutzbeauftragte?	36
Wie läuft die Zusammenarbeit mit Datenschutzbeauftragten?	36
Wie erfolgt die Meldung von Datenschutzbeauftragten bei der Aufsichtsbehörde?	37
Was bedeuten die Regelungen für die Praxis?	37
Verzeichnis von Verarbeitungstätigkeiten	38
Wer muss ein Verzeichnis von Verarbeitungstätigkeiten führen?	38
Welche Informationen muss das Verzeichnis eines Verantwortlichen enthalten?	38
Welche Form muss das Verzeichnis haben?	39
Gibt es Ausnahmen für kleine und mittlere Unternehmen?	40
Datenschutz-Management-System	41
Wozu dient ein Datenschutz-Management-System?	41
In welcher Form kann ein Datenschutz-Management-System geführt werden?	41
Welche Prozesse sollten ein Datenschutz-Management-System steuern?	41
Risikoanalyse und Datenschutz-Folgenabschätzung	42
Was versteht sich unter „risikobasierter Ansatz“?	42
Wozu dient eine Risikoanalyse?	42

Wann ist eine Datenschutz-Folgenabschätzung vorzunehmen?	43
Wie wird eine Datenschutz-Folgenabschätzung durchgeführt?	44
Was ist, wenn die Datenschutz-Folgenabschätzung ein hohes Risiko bestätigt?	45
Technischer und organisatorischer Datenschutz	46
Was bedeutet „Datenschutz durch Technikgestaltung“?	46
Was sind „datenschutzfreundliche Voreinstellungen“?	47
Welche technischen Maßnahmen müssen getroffen werden?	47
Welche organisatorischen Maßnahmen müssen getroffen werden?	48
Was bedeuten die Regelungen für die Praxis?	48
Pflichten bei Datenpannen	50
Was ist ein Datenschutzvorfall?	50
Wann liegt ein meldepflichtiger Datenschutzvorfall vor?	50
Was muss der Aufsichtsbehörde gemeldet werden?	50
Wann müssen die betroffenen Personen benachrichtigt werden?	51
Wie müssen die betroffenen Personen benachrichtigt werden?	52
Müssen Datenschutzvorfälle dokumentiert werden?	52
Was bedeuten die Regelungen für die Praxis?	53
Datenübermittlung in Drittstaaten	54
Was ist bei einer Datenübermittlung in Drittstaaten zu beachten?	54
Was versteht man unter einem Angemessenheitsbeschluss?	54
Was gilt, falls kein Angemessenheitsbeschluss vorliegt?	54
Was gilt, wenn auch keine geeigneten Garantien vorliegen?	55
Bußgelder und Sanktionen	56
Wie hoch können Bußgelder ausfallen?	57
Woran bemisst sich die Höhe eines Bußgeldes?	57
Drohen wettbewerbsrechtliche Abmahnungen?	57
Können Schadensersatzansprüche geltend gemacht werden?	58
Gibt es weitere Sanktionen?	58
Weiterführende Dokumente und Gesetzestexte	59
Wie erfahre ich von neuen Versionen dieses eBooks?	59
Wie kann die Datenschutzkanzlei unterstützen?	60
Rechtliche Beratung für Daten, Technologie und Marketing	60
Externer Datenschutzbeauftragter	60
Beratung interner Datenschutzbeauftragter	60

Über die Datenschutzkanzlei

Rechtliche Beratung für Daten, Technologie und Marketing

Viele Geschäftsmodelle, wirksames Marketing und effizienter Vertrieb sind ohne Daten nicht mehr denkbar. Den Möglichkeiten von Digitalisierung und künstlicher Intelligenz stehen dabei neue Risiken und Rechtspflichten gegenüber. Unsere Anwält:innen sind hochspezialisierte Experten für Datenschutz- und Datenwirtschaftsrecht und beraten an dieser Schnittstelle verschiedener Rechtsgebiete. Wir unterstützen Sie bei der Umsetzung Ihrer Ideen und bei der Nutzung personenbezogener Daten innerhalb der rechtlichen Spielräume. Ob bei der Unternehmensgründung, der Entwicklung von Software und Diensten oder der Planung und Umsetzung von Datenprojekten – wir zeigen Ihnen Fallstricke und gesetzeskonforme Lösungsmöglichkeiten auf.

Externer Datenschutzbeauftragter

Bei der Datenschutzkanzlei unterstützen Sie erfahrene und zertifizierte Datenschutz-Jurist:innen in enger Abstimmung mit auf Daten, Tech und Marketing spezialisierten Rechtsanwält:innen. Wir stellen Ihnen feste Ansprechpartner:innen zur Seite, die Sie vertrauensvoll begleiten und mit Ihnen wirtschaftliche und praktikable DSGVO-Maßnahmen umsetzen. Mit unserer smarten **Datenschutz-Management-Cloud DataDesk**¹ haben Sie Ihre DSGVO-Pflichten schnell im Griff und jederzeit nachweisbar. Über die **Lernplattform unserer Academy**² stehen Ihnen unsere eLearnings für die gesetzlich geforderten Schulungen zur Verfügung. Wichtiges Basiswissen wird praxisnah und verständlich vermittelt – mit Teilnahmezertifikat und Reportings für Ihre Nachweispflicht.

Beratung interner Datenschutzbeauftragter

Sie sind als Datenschutzbeauftragte:r oder Datenschutzkordinator:in intern für die Umsetzung der DSGVO zuständig und wünschen Beratung, Anleitung oder einfach einen Sidekick, um Herausforderungen und Lösungsansätze zu besprechen? Gerne unterstützen wir Sie mit unserer Erfahrung aus der Tätigkeit als Datenschutzbeauftragte und Anwälte für Datenschutz.

Sprechen Sie uns an

Telefon +49. 40. 226 34 56 0
E-Mail info@datenschutzkanzlei.de

LINK

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

¹ <https://www.datenschutzkanzlei.de/datadesk/>

² <https://www.datenschutzkanzlei.de/academy/>

Grundsatzfragen

Was regelt 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 regelt 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 (DSAnpUG-EU) vom deutschen Bundestag beschlossen und wurde am 30. Juni 2017 im Bundesgesetzblatt veröffentlicht. Das BDSG entfaltete zeitgleich mit der DSGVO am 25. Mai 2018 seine Wirkung. Im Rahmen einer Aktualisierung des BDSG (durch das 2. DSAnpUG-EU) im Jahre 2019 wurden einige wenige, aber praxisrelevante Normen noch einmal inhaltlich verändert.

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.

Was regelt das TDDDG?

Das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) konkretisiert und ergänzt die Bestimmungen der DSGVO in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation und digitalen Dienste. Es enthält Vorschriften zum Schutz personenbezogener Daten bei der Nutzung von Telekommunikationsdiensten und digitalen Diensten.

Das am 01. Dezember 2021 ursprünglich als TTDSG in Kraft getretene Gesetz wurde am 13. Mai 2024 mit dem Digitalen-Dienste-Gesetz (DDG) in TDDDG umbenannt, um sprachlich den Anforderungen des seit dem 17. Februar 2024 geltenden Digital Services Act (DSA) gerecht zu werden. Der Begriff „Telemedium“ wurde durch die Terminologie „digitaler Dienst“ ersetzt.

Den Anlass für diese Gesetzgebung bildete ursprünglich die notwendige Umsetzung der Richtlinie 2018/1972/EU über den europäischen Kodex für die elektronische Kommunikation. Der Gesetzgeber nutzte dies, um die Datenschutzvorschriften für Telekommunikationsdienste und digitale Dienste im TDDDG zu bündeln und hierbei an die DSGVO und die ePrivacy-Richtlinie anzupassen. Damit wurde auch die Rechtsunsicherheit beseitigt, die durch das vorherige Nebeneinander von DSGVO, TMG und TKG entstand.

Teil 1 des TDDDG legt den Anwendungsbereich, Begriffsbestimmungen und allgemeine Regelungen fest, die den Datenschutz und die Privatsphäre bei der Nutzung von Telekommunikationsdiensten und digitalen Diensten regeln.

In Teil 2 enthält es Bestimmungen zum Datenschutz und Schutz der Privatsphäre in der Telekommunikation. Zentral ist hier das in § 3 TDDDG geregelte Fernmeldegeheimnis. Der Datenschutz für digitale Dienste und der Schutz der Privatsphäre bei Endeinrichtungen ist in Teil 3 des TDDDG geregelt. Hier finden sich besondere Vorschriften zu technischen und organisatorischen Vorkehrungen für digitale Dienste sowie die Anforderungen an die Erteilung von Auskünften über Bestands- und Nutzungsdaten. Daneben ist mit § 25 TDDDG in diesem Teil auch der sehr praxisrelevante Einsatz von Cookies und ähnlichen Technologien geregelt.

DSGVO, BDSG, TDDDG – was gilt denn jetzt?

Kurz gesagt: alle drei! 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.

Das Verhältnis von TDDDG und DSGVO bestimmt sich nach der Kollisionsregel des Art. 95 DSGVO. Danach gelten diejenigen Vorschriften im TDDDG, die wie etwa § 25 TDDDG auf der ePrivacy-Richtlinie beruhen, vorrangig vor den Bestimmungen der DSGVO

Herrscht in Europa ein einheitlicher Datenschutz?

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 und zum Profiling. Zudem wurden die Vorgaben für den betrieblichen Datenschutzbeauftragten aus dem BDSG-alt zunächst übernommen, sodass Unternehmen in Deutschland ab zehn Beschäftigten einen Datenschutzbeauftragten benennen mussten. Im Zuge des zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2.DSAnpUG) wurde diese Grenze auf 20 Beschäftigte erhöht.

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 teils zu erheblicher Rechtsunsicherheit bei der Umsetzung der Bestimmungen aus dem BDSG.

Das jeweilige nationale Umsetzungsniveau unterscheidet sich auch zwischen den EU-Mitgliedsstaaten. Zwar werden durch den Europäischen Datenschutzausschuss (EDSA) als Zusammenschluss aller europäischen Datenschutz-Aufsichtsbehörden bereits viele grundlegenden Datenschutzaspekte im Rahmen von Leitlinien, Empfehlungen oder Stellungnahmen beschrieben. Trotzdem gibt es weiterhin einige nationale Sonderregelungen sowie unterschiedliche Auslegungen zu datenschutzrechtlichen Themen, die insbesondere für international tätige Unternehmen zu Rechtsunsicherheit führen können.

Auch innerhalb Deutschlands gibt es durch das föderale System und die einzelnen Landes-Aufsichtsbehörde teils unterschiedliche Rechtsansichten. Auch die verschiedenen Landesbeauftragten veröffentlichen (in unterschiedlicher Frequenz) hilfreiche Materialien. Auf nationaler Ebene gibt es zudem, analog zu dem Europäischen Datenschutzausschuss, die Datenschutzkonferenz (DSK), in der sich alle Datenschutz-Aufsichtsbehörden aus den verschiedenen Bundesländern zusammenfinden.

Letztlich prägen natürlich auch die Gerichte die Umsetzungsregeln der DSGVO. Insbesondere durch Entscheidungen des Europäischen Gerichtshofs (EuGH) werden die Regeln der DSGVO konkretisiert und abschließend mit Wirkung für alle festgelegt. Seit der Geltung der DSGVO im

PRAXIS-TIPP

Nutzen Sie die Leitlinien, Praxishilfen, Kurzpapiere und Vorlagen der Datenschutzbehörden, Datenschutzgremien und Fachverbände. Einige Links und Fundstellen finden Sie in diesem eBook.

LINKS

Auf der Website des EDSA finden Sie viele hilfreiche Leitlinien und Empfehlungen zu unterschiedlichen praxisrelevanten Themen:

https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de

Eine Übersicht der deutschen Datenschutzaufsichtsbehörden finden Sie hier:

https://www.bfdi.bund.de/DE/Service/Anschriften/anschriften_table.html

Informationen und Materialien der DSK sind hier abrufbar:

<https://www.datenschutzkonferenz-online.de/>

Mai 2018 wurden bereits einige wichtige

Für wen gelten die Datenschutzbestimmungen?

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 „Markortprinzip“: 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 Buchst. a) DSGVO / § 1 Abs. 4 Nr. 3 BDSG).

LINK

Kurzpapier der
Datenschutzkonferenz zum
Markortprinzip:
<https://cutt.ly/markort>

Wer ist „Verantwortlicher“?

Adressat: in 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 personenbezogenen 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“ und „betroffene Personen“?

„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 erheblichem Aufwand nicht möglich ist.

Sobald eine Person mittels personenbezogener Daten identifiziert werden kann, spricht man von ihr als „betroffene Person“. Betroffene sind also alle Personen, dessen personenbezogene Daten verarbeitet werden.

Welchen Stellenwert haben die Grundsätze der Datenverarbeitung?

Die DSGVO ist technikneutral und entwicklungs offen 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 genannten Grundsätzen für die Verarbeitung personenbezogener Daten. Diese Grundsätze werden durch weitere Bestimmungen der DSGVO konkretisiert und handhabbar gemacht.

Was bedeutet „Rechtmäßigkeit der Verarbeitung“?

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.

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 (z.B. personalisierte E-Mail-Adressen) personenbezogene Daten sind. Auch für diese Daten gelten die gesetzlichen Anforderungen!

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 „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 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. Er 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 Primärzwecke 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 („so viel wie nötig, so wenig wie möglich“). Der Grundsatz der Datenminimierung lässt sich also nur relativ in Bezug auf den Verarbeitungszweck konkretisieren.

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 angemessene 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 oder nur mit unverhältnismäßigem Aufwand 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 angemessenes 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.

LINK

Praxishilfe des GDD zur
Accountability:
<https://cutt.ly/cHP4NDj>

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 zunächst 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 (für die Verarbeitung besonderer Kategorien personenbezogener Daten) sowie in den §§ 22 – 28 BDSG normiert.

Welche Anforderungen gelten für eine Einwilligung einer betroffenen Person?

Für die Wirksamkeit der 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. Grundsätzlich muss eine Einwilligung immer freiwillig, für den bestimmten Fall, in informierter Weise sowie in Form einer unmissverständlich abgegebenen Handlung abgegeben werden. Nur dann ist eine abgegebene Einwilligung auch tatsächlich wirksam. Insbesondere im Online-Kontext ist zudem deshalb zu achten, dass eine Einwilligung stets eine aktive bestätigende Handlung darstellen muss (z.B. über Checkboxes).

Einwilligungen bedürften grundsätzlich keiner Schriftform, können also insbesondere auch elektronisch eingeholt werden. Zu beachten ist allerdings die Nachweispflicht des Verantwortlichen. Einwilligungen sollten daher immer sorgfältig dokumentiert werden.

Besonders zu beachten ist das ausdrücklich erwähnte Kopplungsverbot in Art. 7 Abs. 4 DSGVO: 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. Hier ist aber weiterhin umstritten, was als „nicht erforderlich“ anzusehen ist, sodass für Unternehmen gewisse Handlungsspielräume bestehen.

Was gilt für die Einwilligung zu Cookies?

Seit dem 01. Dezember 2021 regelt § 25 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG) den Einsatz von Cookies und ähnlichen Technologien, mittels derer Informationen auf Endeinrichtungen gespeichert oder aus diesen ausgelesen werden. Während die DSGVO dem Schutz personenbezogener Daten dient, gilt § 25 TDDDG unabhängig davon, ob die Daten personenbezogen sind oder nicht. TDDDG und DSGVO gelten nebeneinander.

§ 25 TDDDG bezieht sich auf „die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder den Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind“. Hiermit sind insbesondere Cookies gemeint. Die Regelung erfasst daneben aber auch andere Technologien wie LocalStorage, Web-Storage oder das Auslesen von Werbe- und Geräte-IDs. Die Verwendung von Cookies und vergleichbaren Technologien ist grundsätzlich einwilligungsbedürftig. Diese Einwilligungspflicht besteht aber

PRAXIS-TIPP

Das „Kopplungsverbot“ in Art. 7 Abs. 4 DSGVO kann in manchen Fällen zur Unwirksamkeit von Einwilligungen führen. 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, ist die Wirksamkeit genauer zu prüfen.

LINK

Kurzpapier der Datenschutzkonferenz zur Einwilligung nach der DSGVO: <https://cutt.ly/dskdsgvo>
Auch der EDSA hat sich bereits detailliert mit der Einwilligung auseinandergesetzt:
https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_de

LINK

Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021: https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf

LINK

FAQ zu Cookies und Tracking der Aufsichtsbehörde Baden-Württemberg: <https://cutt.ly/FSg6jwH>

nicht, wenn die Verwendung von Cookies oder vergleichbaren Technologien (technisch) unbedingt erforderlich ist, um einen von Nutzer:innen nachgefragten Dienst zu erbringen. Die Ausnahme ist eng zu verstehen und umfasst etwa Warenkorb-Cookies, Log-In-Cookies oder auch das Vermerken des Einwilligungstatus.

Wie müssen Cookie-Banner gestaltet sein?

Die Einwilligung der Nutzer:innen muss den Anforderungen der DSGVO genügen. Zur Umsetzung dieser Anforderungen wird regelmäßig ein Consent-Management-Tool und ein Consent-Banner auf der Website verwendet. Die Gestaltung des Consent-Banners muss dabei den Vorgaben des Art. 7 DSGVO gerecht werden. Durch den EuGH wurde hierzu festgestellt, dass eine vorangekreuzte Checkbox den Anforderungen einer wirksamen Einwilligung nicht genügt. Auch dürfen Nutzer:innen nicht durch eine manipulative Gestaltung des Banners, etwa durch die farbliche Hervorhebung oder besondere Positionierung eines Buttons unterschwellig zur Abgabe einer Einwilligung beeinflusst werden. Die Ablehnung muss für die Nutzer:innen genauso einfach sein wie die Erklärung der Einwilligung, was über gleichwertig gestaltete Buttons auf der gleichen Ebene des Banners erreicht werden kann.

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 die Trägerin oder 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 oder die Trägerin der elterlichen Verantwortung für das Kind oder mit dessen bzw. deren 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.

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.

LINK

Informationen zu den Anforderungen der deutschen Aufsichtsbehörden im Hinblick auf die Gestaltung von Consent-Bannern finden Sie ebenfalls in der Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien: https://www.datenschutzkonferenzen-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf

LINK

Kurzpapier des BayLDA zur Einwilligung eines Kindes: <https://cutt.ly/uHP06py>

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 erforderlich, wenn die Speicherung und Verarbeitung von Kundendaten zur Durchführung einer Warenbestellung benötigt wird. Denn ohne diese Form der Verarbeitung kann die Ware weder verschickt, noch können mögliche Nachfragen der Kund:innen beantwortet werden. Selbst wenn eine Kundin oder ein Kunde nur Informationen zu der Ware anfordert, ohne aber eine Bestellung aufzugeben, kann eine Speicherung ihrer oder 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 zu Kund:innen hinausgeht, bedarf einer eigenen Rechtfertigung, da sie für den ursprünglichen Zweck nicht erforderlich ist.

LINK

Leitlinien des Europäischen Datenschutzausschusses (edpb) zur Vertragserfüllung bei Online-Diensten: <https://cutt.ly/oHP2Dry>

Zu beachten ist, dass Art. 6 Abs. 1 Buchst. b) DSGVO nur dann zur Anwendung kommen kann, wenn es sich bei dem Vertragspartner des Verantwortlichen oder Auftragsverarbeiters um die betroffene Person selbst handelt („dessen Vertragspartei die betroffene Person ist“). Zur Erfüllung von Verträgen zwischen Unternehmen kann die Rechtsgrundlage daher in aller Regel nicht herangezogen werden. Aus diesem Grund spielt Art. 6 Abs. 1 Buchst. b) DSGVO im B2B-Bereich nur eine stark untergeordnete Rolle.

Wann liegt ein „berechtigtes Interesse“ zur Datenspeicherung vor?

Eine Vielzahl der Datenverarbeitungen von Unternehmen kann zudem über die Klausel des „berechtigten Interesses“ vorgenommen werden. Bei dieser Auffangregelung soll eine Abwägung zwischen legitimen Interessen 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 oder eine Kundin 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 von 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). Darüber hinaus liegt ein berechtigtes Interesse in der Regel auch dann vor, wenn Pflichten aus einem Vertrag zwischen Unternehmen erfüllt werden müssen und dazu die Verarbeitung personenbezogener Daten, beispielsweise von Ansprechpartner:innen der Vertragspartner, erforderlich ist.

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 in Art. 9 Abs. 1 DSGVO 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 von Betroffenen vor allem Einrichtungen im Gesundheits- und Sozialbereich und Fälle, in denen ein Verantwortlicher zur Erfüllung rechtlicher Pflichten auf diese Daten angewiesen ist. So sind beispielsweise nach Art. 9 Abs. 2 Buchst. b) DSGVO Arbeitgeber:innen berechtigt, die für die Gehaltsabrechnung erforderlichen Angaben zu Familienstand, Kinderzahl und Religion sowie krankheitsbedingte Fehlzeiten der Mitarbeiter:innen zu speichern.

LINK

Kurzpapier der Datenschutzkonferenz zur Verarbeitung personenbezogener Daten für Werbung: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_3.pdf

LINK

Kurzpapier der Datenschutzkonferenz zu besonderen Kategorien personenbezogener Daten: <https://cutt.ly/dskkategorien>

Beschäftigtendatenschutz

§ 26 BDSG

Auch personenbezogene Daten von Beschäftigten fallen in den Anwendungsbereich der DSGVO. Der Begriff der Beschäftigten ist im datenschutzrechtlichen Kontext weit auszulegen. Darunter fallen gem. § 26 Abs. 8 DSG neben Arbeitnehmer:innen beispielsweise auch Auszubildende, Leiharbeiter:innen sowie Bewerber:innen.

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 (§ 26 Abs. 1 S. 1 BDSG).

- **Kollektiv-/ Betriebsvereinbarungen**

Datenverarbeitungen können auch auf Grundlage von Kollektivvereinbarungen legitimiert werden (§ 26 Abs. 4 BDSG). 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 Interessen und der Grundrechte der betroffenen Person zu ergreifen.

- **Zur Aufdeckung von Straftaten**

Personenbezogene Daten von Beschäftigten dürfen dann 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

RISIKO-RADAR

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

LINK

Kurzpapier der Datenschutzkonferenz zum Beschäftigtendatenschutz: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_14.pdf

LINK

Die Aufsichtsbehörde in Baden-Württemberg hat viele praxisrelevante Aspekte des Beschäftigtendatenschutzes im „Ratgeber Datenschutz“ zusammengefasst: <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/04/Ratgeber-Besch%C3%A4ftigtendatenschutz.pdf>

das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt (§ 26 Abs. 1 S. 2 BDSG). Insbesondere dürfen Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sein.

— **Verarbeitung besonderer Kategorien personenbezogener Daten**

Auch für die Verarbeitung von besonders sensiblen Daten gem. Art. 9 Abs. 1 DSGVO hält der § 26 Abs. 3 BDSG eine Regelung bereit. Darin wird klargestellt, dass sensible personenbezogene Daten von Beschäftigten auch dann verarbeitet werden dürfen, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich sind und die schutzwürdigen Interessen der Betroffenen nicht überwiegen.

Welche Besonderheiten gibt es beim Erlaubnistatbestand der Einwilligung?

Grundsätzlich besteht nach § 26 Abs. 2 BDSG ebenfalls die Möglichkeit, Daten auf Grundlage einer Einwilligung von Beschäftigten zu verarbeiten. Eine Schwierigkeit stellt dabei regelmäßig die Voraussetzung der Freiwilligkeit dar, welche aufgrund des Über-/Unterordnungsverhältnisses der beteiligten Parteien in den meisten Fällen nicht vorliegt. Nach § 26 Abs. 2 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:innen 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 der Arbeitgeber:innen betreffen.

Rechte der betroffenen Person

Art. 12 – 23 DSGVO

Die DSGVO stärkt in besonderem Maße die Rechte der betroffenen Personen. 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.

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 bei Betroffenen selbst (Art. 13 DSGVO) und die Erhebung bei Dritten (Art. 14 DSGVO).

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:

- Kontaktdaten des Verantwortlichen, dessen Vertretung sowie ggf. des Datenschutzbeauftragten;
- Die Zwecke und die Rechtsgrundlage der Verarbeitung, bei einer Verarbeitung auf Grundlage eines „berechtigten Interesses“ zudem eine genaue Darlegung derer;
- Im Falle einer Einwilligung den Hinweis auf das Recht, diese jederzeit zu widerrufen;
- Neben der Offenlegung von Empfängergruppen insbesondere eine mögliche Weiterleitung der Daten in Drittländer (z.B. USA) sowie die Rechtsgrundlage für diese Übermittlung (z.B. Standardvertragsklauseln);
- 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) sowie das Beschwerderecht bei einer Aufsichtsbehörde;

RISIKO-RADAR

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

PRAXIS-TIPP

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

LINK

Anleitung zur Gestaltung von Datenschutzinformationen für Websites:
<https://cutt.ly/derklaerung>

- 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 Buchst. f) DSGVO) und welche Kategorien von personenbezogenen Daten betroffen sind (Art. 14 Abs. 1 Buchst. 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 Buchst. 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.

PRAXIS-TIPP

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

LINK

Kurzpapier der Datenschutzkonferenz zu Informationspflichten:
<https://cutt.ly/dskinfo>

- Ergänzend können 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 in einer von anderen Informationen getrennten Form erfolgen, Art. 21 Abs. 4 DSGVO. Ob dieser Hinweis dazu beispielsweise zwingend besonders hervorgehoben werden muss, ist umstritten.
- 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.

Welche Auskunftsrechte haben betroffene Personen nach der DSGVO?

Spiegelbildlich zur Informationspflicht für Verarbeitende haben betroffene Personen gemäß Art. 15 DSGVO das Recht, proaktiv Auskunft über die Verarbeitung 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. per 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.

LINK

Praxishilfe des GDD zu den Transparenzpflichten:
<https://cutt.ly/gddtransparenz>

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!

LINKS

Anleitung für eine erfolgreiche Auskunftserteilung:
<https://cutt.ly/dkauskunft>

Kurzpapier der Datenschutzkonferenz zu Auskunftsrechten:
<https://cutt.ly/uHP25b6>

Guideline des Europäischen Datenschutz-Ausschusses zum Auskunftsrecht:
https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_de

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.

Wann müssen personenbezogene Daten dauerhaft gelöscht werden?

Betroffene Personen haben das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten gelöscht werden (Art. 17 Abs. 1 DSGVO). Eine Löschung können Betroffene 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);
- Die betroffene Person hat Widerspruch gem. Art. 21 DSGVO eingelegt;
- Die Löschung ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht eines Mitgliedstaates erforderlich.

Durch die DSVO wurde neben dem eigentlichen Recht auf Löschung, das vorher schon in ähnlicher Form innerhalb des Bundesdatenschutzgesetzes galt, das neuartige „Recht auf Vergessenwerden“ kodifiziert. Dieses aus der „Google-Rechtsprechung“ des EuGHs bekannte Recht soll betroffenen Personen ermöglichen, (z.B. falsche oder ehrwürdige) Informationen zuverlässig und umfassend (auch aus dem Netz) entfernen zu lassen.

Das „Recht auf Vergessenwerden“ findet sich in Art. 17 Abs. 2 DSGVO. Sofern der Verantwortliche die Daten öffentlich zugänglich gemacht hat (z.B. auf einer Website), 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).

LINK

Kurzpapier der
Datenschutzkonferenz zum Recht
auf Löschung:
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_11.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 der oder 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 Lösungsanspruchs ein Einschränkungsanspruch.

Was bedeutet das Recht auf Datenübertragbarkeit?

Die DSGVO normiert zudem ein „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 Kund:innen 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.

WEBSITE

Leitlinie der Artikel 29-Datenschutzgruppe zum Recht auf Datenübertragbarkeit:
<https://cutt.ly/art29>

Gemeinsame Verantwortlichkeit

Art. 26 DSGVO

Eine Auslagerung von Datenverarbeitung findet nicht mehr nur im Auftragsverarbeitungsverhältnis statt, sondern kann auch anderen Regelungen unterliegen. Das Konstrukt der gemeinsam für die Verarbeitung Verantwortlichen gewinnt dabei in der Praxis immer mehr an Bedeutung.

Wann liegt eine gemeinsame Verantwortlichkeit vor?

Eine gemeinsame Verantwortlichkeit kommt dann in Betracht, wenn zwei oder mehr Verantwortliche gemeinsam 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 der damalige Anbieter Facebook Inc. (mittlerweile in Meta Inc. umbenannt) der gleichnamigen Plattform und Unternehmen, die auf dieser Plattform eine Fanpage betreiben, gemeinsam Verantwortliche bei der Erhebung personenbezogener Daten der Endnutzenden 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.

RISIKO-RADAR

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.

LINK

Leitlinien des Europäischen Datenschutzausschusses zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ vom 07.07.21:
https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_de.pdf

LINK

Vertragsmuster zur gemeinsamen Verantwortlichkeit der LfDI BW:
<https://t1p.de/sai9>

Wer haftet für Schäden bei einer gemeinsamen Verantwortlichkeit?

Jeder der gemeinsam Verantwortlichen 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.

LINK

Kurzpapier der
Datenschutzkonferenz zur
gemeinsam für die Verarbeitung
Verantwortliche:
<https://cutt.ly/dsk-verantwortliche>

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.

Unter welchen Voraussetzungen ist eine 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 Buchst. 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 auch in einem elektronischen Format (z.B. PDF) erfolgen kann (Art. 28 Abs. 9 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

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).

LINK

Kurzpapier der Datenschutzkonferenz zur Auftragsverarbeitung: <https://cutt.ly/dsk-av>

LINK

Praxishilfe des GDD zur Auftragsverarbeitung: <https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/GDDPraxishilfeDSGVOPraxishilfepdf.pdf>

LINK

Unser Blogbeitrag zum elektronischen Vertragsschluss des AV-Vertrages: <https://cutt.ly/dk-blog-av>

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 Buchst. 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 über entsprechende Vorgänge informiert und ihm ein Einspruchsrecht eingeräumt werden (Art. 28 Abs. 2 DSGVO). Für den Vertrag mit einem Unterauftragnehmer sieht Art. 28 Abs. 4 DSGVO zudem weitere Voraussetzungen vor, die die Einhaltung der notwendigen Datensicherheit auch in diesem Verhältnis garantieren sollen. Der Auftragsverarbeiter ist dabei auch selbst für die 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 (Art. 28 Abs. 3 Satz 2 Buchst. b) DSGVO).
- Alle personenbezogenen Daten müssen nach Wahl des Verantwortlichen nach Auftragsende zurückgegeben oder gelöscht

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!

werden, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (Art. 28 Abs. 3 Satz 2 Buchst. g) DSGVO).

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

Was bedeuten die Regelungen für die Praxis?

Jeder Verantwortliche sollte sicherstellen, dass alle Auftragsverarbeitungsverhältnisse auch durch entsprechende Verträge gem. Art. 28 Abs. 3 DSGVO legitimiert worden sind. Dazu ist die Erstellung einer Übersicht über alle eingesetzten Dienstleister und Datenempfänger hilfreich. Der Verantwortliche muss insgesamt dafür Sorge tragen, nur geeignete Dienstleister zu beauftragen, und ist gefordert, deren Sicherheitsvorkehrungen vorab und daraufhin regelmäßig zu prüfen.

Datenschutzbeauftragte:r

Art. 37 – 39 DSGVO, § 38 BDSG

Der oder die 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.

Wann muss ein:e Datenschutzbeauftragte:r benannt werden?

Eine generelle Pflicht zur Benennung eines bzw. einer 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 der deutsche Gesetzgeber im Rahmen der Öffnungsklausel des Art. 37 Abs. 4 Satz 2 DSGVO mit § 38 Abs. 1 BDSG eine erweiterte Benennungspflicht umgesetzt hat. Danach muss ein:e Datenschutzbeauftragte:r benannt werden, wenn in der Regel mindestens zwanzig Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt waren..

RISIKO-RADAR

Unterlässt der Verantwortliche oder der Auftragsverarbeiter die Bestellung eines bzw. einer Datenschutzbeauftragten, so drohen 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.

PRAXIS-TIPP

Für Start-ups und kleine Unternehmen mit weniger als 20 Beschäftigten gilt also: Wenn die Tätigkeit Ihres Unternehmens in eine der Kategorien des § 38 Abs. 1 Satz 2 BDSG oder des Art. 37 Abs. 1 DSGVO fällt, benötigen Sie auch dann eine:n Datenschutzbeauftragte:n, wenn Sie unter dem Schwellenwert des § 38 Abs. 1 Satz 1 BDSG liegen.

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).

Unabhängig von der gesetzlichen Pflicht können Unternehmen allerdings auch freiwillig eine:n Datenschutzbeauftragte:n benennen. Allerdings gilt in diesem Fall gemäß § 38 Abs. 2 BDSG nicht der erweiterte Kündigungsschutz.

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 oder der Datenschutzbeauftragten?

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

Art. 39 Abs. 1 DSGVO zählt folgende Aufgaben von 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;

RISIKO-RADAR

Die Pflicht zur Umsetzung der Anforderungen aus der DSGVO und dem BDSG besteht für alle Unternehmen, Handwerksbetriebe und Vereine unabhängig von der Größe oder Beschäftigtenanzahl oder der Pflicht zur Benennung eines oder einer Datenschutzbeauftragten.

LINK

Praxishilfe des GDD zu Datenschutzbeauftragten: <https://cutt.ly/gdd-dsb>

PRAXIS-TIPP

Der oder die 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.

- 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:innen 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.

LINK

Praxishilfe des GDD zu den Aufgaben von Datenschutzbeauftragten:
<https://cutt.ly/PHP9jQj>

Welche Voraussetzungen müssen Datenschutzbeauftragte erfüllen?

Zu Datenschutzbeauftragten können nur solche Personen bestellt werden, die die erforderliche Fachkunde und Zuverlässigkeit besitzen.

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..

Interne oder externe Datenschutzbeauftragte?

Als Datenschutzbeauftragte können gemäß Art. 37 Abs. 6 DSGVO sowohl Mitarbeiter:innen des Unternehmens (interne:r Datenschutzbeauftragte:r) als auch Dritte auf Grundlage eines Dienstleistungsvertrags (externe:r Datenschutzbeauftragte:r) benannt werden.

Die Beauftragung von externen Datenschutzbeauftragten bietet dabei einige Vorteile:

- Durch die Auswahl eines geeigneten Dienstleisters sind Fachkunde und Zuverlässigkeit gesichert;
- Unternehmen profitieren von der Erfahrung des/der Datenschutzbeauftragten aus einer Vielzahl von Mandaten mit häufig ähnlichen Herausforderungen und Fragestellungen;
- Es entfallen die Kosten und Ausfallzeiten für die Aus- und Weiterbildung eines bzw. einer internen Datenschutzbeauftragten. Zudem kann der oder die Datenschutzbeauftragte anhand des tatsächlich anfallenden Aufwands vergütet werden, was hohe Fixkosten und Bindung von Arbeitszeit vermeidet;
- Die Verlagerung der Beratungshaftung auf eine:n externe:n Datenschutzbeauftragte:n reduziert das Unternehmensrisiko;
- Das Unternehmen bleibt durch den Abschluss eines Dienstvertrages mit dem oder der externen Datenschutzbeauftragten flexibel. Gemäß § 38 Abs. 2 BDSG i.V.m. § 6 Abs. 4 BDSG genießt der oder die interne Datenschutzbeauftragte nämlich besonderen Kündigungsschutz.

Wie läuft die Zusammenarbeit mit Datenschutzbeauftragten?

Der oder die 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 oder die 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.

Wichtig für die Praxis ist jedoch: Der oder die Datenschutzbeauftragte ist nicht dafür zuständig, Entscheidungen zur Datenverarbeitung zu treffen oder alle Anforderungen der DSGVO im Unternehmen umzusetzen. Vielmehr nimmt der/die Datenschutzbeauftragte allein eine beratende, unterstützende Funktion ein.

PRAXIS-TIPP

Die Jurist:innen der Datenschutzkanzlei sind TÜV-zertifizierte Experten auf dem Gebiet des Datenschutzrechts und sind seit 2010 als externe Datenschutzbeauftragte für Unternehmen tätig.

LINK

Informationen zu unseren Leistungen und ausgewählte Referenzen finden Sie unter: <https://cutt.ly/dk-dsb>

Der Verantwortliche bzw. Auftragsverarbeiter hat den oder die Datenschutzbeauftragte:n gemäß Art. 38 Abs. 2 DSGVO bei seinen bzw. ihren Aufgaben durch die Bereitstellung des Zugangs zu den personenbezogenen Daten und Verarbeitungsvorgängen zu unterstützen. Die ebenfalls notwendige Bereitstellung der erforderlichen Ressourcen sowie die zur Erhaltung des Fachwissens erforderliche Schulungszeit betreffen hingegen primär interne Datenschutzbeauftragte. Datenschutzbeauftragte sind ihrerseits verpflichtet, unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters über ihre Arbeit Rechenschaft zu leisten (Art. 38 Abs. 3 DSGVO). Datenschutzbeauftragte bleiben hinsichtlich ihrer Aufgaben allerdings unabhängig und sind nicht an Weisungen der Auftraggeber gebunden.

LINK

Kurzpapier der Datenschutzkonferenz zum Datenschutzbeauftragten: <https://cutt.ly/dsk-dsb>

Wie erfolgt die Meldung von Datenschutzbeauftragten bei der Aufsichtsbehörde?

Verantwortliche und Auftragsverarbeiter müssen die Kontaktdaten der bzw. der 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. Die meisten Aufsichtsbehörden stellen auf ihren Websites auch elektronische Meldeformulare bereit.

LINK

Eine Liste der Aufsichtsbehörden und Links zur Online-Meldung stellen wir hier bereit: <https://cutt.ly/dk-dsb-meldung>

Was bedeuten die Regelungen für die Praxis?

Dem oder der Datenschutzbeauftragten kommt im Unternehmen eine entscheidende Bedeutung bei der Vorbereitung und Unterstützung zur Umsetzung der Vorgaben aus der DSGVO zu. Die vermeintliche Beschränkung bei der Benennungspflicht hat in Deutschland aufgrund der Öffnungsklausel keine praktischen Auswirkungen, sodass der Großteil der Unternehmen verpflichtet ist, eine:n Datenschutzbeauftragte:n zu benennen.

Auch in den Fällen, in denen keine Pflicht zur Benennung besteht, ist eine Einbindung eines oder einer externen Datenschutzbeauftragten in Erwägung zu ziehen: Die umfangreichen Pflichten bei der Verarbeitung personenbezogener Daten bedürfen oftmals entsprechender betrieblicher Prozesse, die mit Hilfe des bzw. der Datenschutzbeauftragten wirksam eingerichtet werden können. Hohe Bußgelder können auf diese Weise vermieden werden.

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. Ein gut geführtes Verzeichnis hilft allerdings nicht nur im Umgang mit Aufsichtsbehörden, sondern auch bei dem Aufbau einer internen Grund-Compliance sowie insbesondere bei der Beantwortung von Betroffenenanfragen.

Wer muss ein Verzeichnis von Verarbeitungstätigkeiten führen?

Das Verzeichnis von Verarbeitungstätigkeiten muss sowohl von Verantwortlichen als auch von Auftragsverarbeitern geführt werden. Auftragsverarbeiter müssen ein weiteres Verzeichnis für die im Auftrag erbrachten Verarbeitungstätigkeiten führen. Diese Pflicht sowie die Inhalte des Verzeichnisses ergeben sich aus Art. 30 Abs. 1, 2 DSGVO. Dabei obliegt die Pflicht dem Verantwortlichen bzw. dem Auftragsverarbeiter selbst und betrifft somit in erster Linie die Unternehmensleitung bzw. die jeweiligen Fachabteilungen. Der oder die Datenschutzbeauftragte kann bei der Erstellung und Pflege eines Verzeichnisses lediglich unterstützend tätig werden.

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, der Vertretung 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

RISIKO-RADAR

Nachlässigkeit kann sich rächen. Bei Verstößen gegen die Dokumentationspflicht drohen 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.

LINK

Hinweise der Datenschutzkonferenz zum Verzeichnis von Verarbeitungstätigkeiten: <https://cutt.ly/dsk-verzeichnis>

LINK

Handreichungen des BayLDA für kleine Unternehmen und Vereine mit Muster-Verzeichnissen für verschiedene Branchen: <https://cutt.ly/lda-handreichung>

LINK

Mit unserer Software DataDesk können Sie das Verzeichnis von Verarbeitungstätigkeiten mit Hilfe bestehender Vorlagen einfach erstellen. Weitere Infos zu DataDesk unter: datenschutzkanzlei.de/datadesk/

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 von Verarbeitungstätigkeiten im Auftrag enthalten?

Auftragsverarbeiter müssen gemäß Art. 30 Abs. 2 DSGVO ein weiteres Verzeichnis der im Auftrag erbrachten 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, der Vertretung 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 in gewissen Fällen (Art. 49 DSGVO) die Dokumentation geeigneter Garantien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 32 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).

Heißt also, dass das Verzeichnis sowohl in Excel oder Word aber auch in einer Software gepflegt und verwaltet werden kann. Während eine Dokumentation anhand der gängigen Office-Programme mit zunehmender Anzahl an Verarbeitungstätigkeiten und ständiger Veränderung der unternehmensinternen Prozesse unübersichtlich und schwerfällig werden kann, bietet die Nutzung einer Software einige Vorteile:

- Benutzerfreundliche Workflows und die Bereitstellung von Vorlagen vereinfachen die Erstellung der Verzeichnisse.

PRAXIS-TIPP

Um den inhaltlichen Anforderungen des Art. 30 DSGVO gerecht zu werden, sind die Verzeichnisse von Verarbeitungstätigkeiten stets aktuell zu halten. Sollten Sie bisher kein Verzeichnis führen, ist es höchste Zeit, damit anzufangen.

SOFTWARE-TIPP

DataDesk, die Datenschutz Management Cloud der Datenschutzkanzlei finden Sie hier:

datenschutzkanzlei.de/datadesk/

- Ergänzungen und Änderungen können strukturiert und zeitsparend eingepflegt werden.
- Für Unternehmensgruppen bedeutet die Multimandantenfähigkeit eine wahre Erleichterung.
- Die Problematik unterschiedlicher und veralteter Versionen ist passé. Die zentrale Ablage ermöglicht allen User:innen stets den Blick auf den aktuellen Stand und vereinfacht die Abstimmung mit Ihrem (externen) Datenschutzbeauftragten.
- Durch die Reporting-Funktionen lässt sich das gesamte Verzeichnis oder nur einzelne Verarbeitungstätigkeiten jederzeit in ein übersichtliches PDF oder ein strukturiertes Excel-Dokument extrahieren.

Im Ergebnis kann die Nutzung einer Software enorme Effekte auf Ihre Datenschutz-Compliance haben und das Datenschutzniveau in Ihrem Unternehmen nachhaltig verbessern. Neben den Verzeichnissen von Verarbeitungstätigkeiten lassen sich mit Hilfe einer Software weitere Pflichtdokumentationen und Prozesse pflegen und verwalten.

Gibt es Ausnahmen für kleine und mittlere Unternehmen?

Es gibt eine Ausnahme für kleine und mittlere Unternehmen und Einrichtungen mit weniger als 250 Beschäftigten. 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 oder
- 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 Beschäftigtendaten dazu führt, dass nicht mehr „nur gelegentlich“ Daten verarbeitet werden, dürfte diese Ausnahme für die meisten Unternehmen bedeutungslos bleiben.

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 umfassende Rechenschafts- und Dokumentationspflicht. Bei einer Prüfung durch die Aufsichtsbehörde müssen die Nachweise über eine ordnungsgemäße Datenverarbeitung durch den Verantwortlichen erbracht werden. Dazu müssen Verantwortliche entsprechende Prozesse schaffen, die die Einhaltung der Datenschutzbestimmungen ermöglichen.

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 internen 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 DSGVO)
- 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

RISIKO-RADAR

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

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 DSGVO, 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 so weit 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.

LINK

Beschreibung der Risikostufen der bayerischen Aufsichtsbehörde:
<https://t1p.de/rqn2>

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

In allen weiteren Fällen sind Art, Umfang, Umstände und 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 mit konkreten Verarbeitungsvorgängen zu veröffentlichen, bei denen ein hohes Risiko anzunehmen 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 demzufolge unabhängig vom Ausgang der eigenen Risikoanalyse vorzunehmen ist.

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.

LINK

Positiv-Liste der deutschen Aufsichtsbehörden:
<https://cutt.ly/abpositiv>

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 einer Datenschutz-Folgenabschätzung 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 Buchst. 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.

LINKS

Software-Tool der französischen Aufsichtsbehörde CNIL:
<https://cutt.ly/PIA-CNIL> (DE)
oder
<https://cutt.ly/PIA-CNIL-en> (EN)

Fallbeispiel einer Datenschutz-Folgenabschätzung der bayerischen Aufsichtsbehörde:
<https://cutt.ly/lda-bsp>

Kurzpapier der Datenschutzkonferenz zur Datenschutz-Folgenabschätzung:
<https://t1p.de/d0y2>

Orientierungshilfe der bayrischen Aufsichtsbehörde zur Datenschutz-Folgenabschätzung:
<https://t1p.de/x2cl>

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 und organisatorischer 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.

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“).

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 bestmöglichen 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.

RISIKO-RADAR

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

LINK

Guideline des Europäischen Datenschutzausschusses (edpb) zu „Privacy by Design“ und „Privacy by Default“:
<https://t1p.de/ozgw1>

Was sind „datenschutzfreundliche Voreinstellungen“?

Nach Art. 25 Abs. 2 DSGVO ist der Verantwortliche verpflichtet, durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass durch Voreinstellungen 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 „Werkseinstellungen“ datenschutzfreundlich auszurichten. Mit Anpassung der Einstellungen oder durch gezielte Freigaben durch die Nutzenden 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.

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 in den Vorwegen eine Risikobewertung ihrer Datenverarbeitung vornehmen. Unter anderem müssen folgende Maßnahmen durch den Verantwortlichen berücksichtigt und bestenfalls in einem Sicherheitskonzept festgelegt werden:

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.

PRAXIS-TIPP

Vor allem für Auftragsverarbeiter ist die Etablierung und Dokumentation technischer und organisatorischer Maßnahmen von großer Bedeutung. In ihrer Rolle als Auftragsverarbeiter 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.

- 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. Zu den empfehlenswerten Maßnahmen zählen insbesondere:

- konkrete Anweisungen und feste Prozesse zum Umgang mit personenbezogenen Daten, die den Beschäftigten zugänglich gemacht werden;
- regelmäßige Schulungs- und Sensibilisierungsmaßnahmen;
- Verabschiedung von geeigneten Richtlinien beispielsweise zur IT-Nutzung und zum richtigen Verhalten im Home-Office.

PRAXIS-TIPP

Über unsere Academy bieten wir mehrere eLearnings an. Weitere Infos zum Inhalt und zur Buchung unter:
<https://www.datenschutzkanzlei.de/academy/>

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.

Was bedeuten die 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 also 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.

Was ist ein Datenschutzvorfall?

Ein Datenschutzvorfall umfasst jedwede Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu bei einem Verantwortlichen oder einem Auftragsverarbeiter gespeicherten personenbezogenen Daten führt. Dabei ist unerheblich, ob dieses Ereignis in böser Absicht erfolgt oder nicht. Beispielhaft für eine Datenpanne ist der Hack eines Unternehmensservers, durch den Kund:innendaten in das Internet gelangen. Eine Datenpanne kann aber schon vorliegen, wenn eine E-Mail an falsche Empfänger:innen 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 die Panne zu beheben.

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;

RISIKO-RADAR

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

LINKS

Kurzpapier der Datenschutzkonferenz zum Risiko für die Rechte und Freiheiten natürlicher Personen
<https://cutt.ly/dsk-risiko>

Guideline des Europäischen Datenschutzausschusses zur Meldung von Datenschutzvorfällen,
https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targedupdate_en.pdf

- 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).

LINK

Einige Aufsichtsbehörden bieten die Möglichkeit, Datenpannen über ein Onlineformular zu melden. Eine Übersicht gibt es hier: <https://cutt.ly/dk-datenpanne>

Wann müssen die betroffenen Personen benachrichtigt werden?

Die Benachrichtigung der betroffenen Personen muss erfolgen, wenn voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen in Folge der Datenpanne besteht. Dies ist etwa dann der Fall, wenn sensible 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 der Betroffenen gegenüber dem 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, Art. 33 Abs. 3 Buchst. b, c, d 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 Datenpannen 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 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. Um diese kurzen Fristen in der Praxis zu wahren, sollten klare und leicht verständliche interne Prozesse sowie eindeutige Zuständigkeiten geschaffen werden. Nur so kann sichergestellt werden, dass etwaige Pannen früh identifiziert und bewerte werden können.

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.

LINK

Kurzpapier des BayLDA zum Umgang mit Datenpannen
<https://cutt.ly/lda-dp>

Datenübermittlung in Drittstaaten

Art. 44 ff. DSGVO

Während bei einer Datenübertragung innerhalb von EU-Mitgliedstaaten 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.

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 in den Art. 45 ff. DSGVO erläutert werden.

Was versteht man unter einem Angemessenheitsbeschluss?

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). Liegt ein wirksamer Angemessenheitsbeschluss der EU-Kommission vor, so werden Datentransfers in diesen Drittstaat letztlich so behandelt, als würde der Drittstaat zum EU-Raum gehören. Für die Legitimation der Datenübermittlung stellen sich daher nur die Grundsatzfragen rund um die Auftragsverarbeitung & Co.

Was gilt, falls kein Angemessenheitsbeschluss vorliegt?

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 Buchst. c), Buchst. d) DSGVO). Eine Verwendung der Standarddatenschutzklauseln ist ohne eigenständige Genehmigung möglich. Solche Standarddatenschutzklauseln liegen in Form der Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer vor, die von der Europäischen Kommission erlassen wurden. Wichtig ist das passende Modul für die jeweilige Datenübermittlung. Sofern die Klauseln unverändert übernommen

RISIKO-RADAR

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

LINK

Eine aktuelle Liste aller Angemessenheitsbeschlüsse der EU-Kommission finden Sie hier: <https://datenschutz.hessen.de/datenschutz/internationaler-datentransfer/angemessenheitsbeschluesse-der-europaeischen-kommission>

PRAXIS-TIPP

Prüfen Sie, ob in den AGB und sonstigen Verträgen die Standardvertragsklauseln enthalten sind.

werden, ist außerdem im Rahmen eines sog. Transfer Impact Assessment (TIA) festzustellen, ob der Einhaltung der Standardvertragsklauseln im Drittland keine nationalen Gesetze oder Gepflogenheiten entgegenstehen. Gibt es nationale Gesetze oder Gepflogenheiten, die die Einhaltung der Standardvertragsklauseln gefährden, müssen zusätzliche Maßnahmen implementiert sein, die ein angemessenes Schutzniveau herstellen. Gelingt dies nicht, sind die Standarddatenschutzklauseln unwirksam und der Datentransfer muss auf einen anderen Transfer-Mechanismus gestützt werden.

- **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. Auch bei der Verwendung von verbindlichen internen Datenschutzvorschriften ist zusätzlich ein Transfer Impact Assessment durchzuführen.
- Durch die Aufsichtsbehörde **genehmigte Vertragsklauseln** (Art. 46 Abs. 3 Buchst. 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), sofern durch ein Transfer Impact Assessment gewährleistet wird, dass nationale Gesetze und Gepflogenheiten der Wirksamkeit der Vertragsklauseln nicht entgegenstehen.
- Seit Einführung der DSGVO gibt es zudem die Möglichkeit, Datentransfers über ie genehmigte **Verhaltensgarantien** (Art. 40 DSGVO) oder genehmigte **Zertifizierungsverfahren** (Art. 42 DSGVO) zu legitimieren. Aufgrund der umfassenden und langwierigen Zulassungs- und Akkreditierungsverfahren für solche Garantien und Zertifizierungen gibt es aktuell allerdings in der Praxis noch keine Instrumente, auf die sich eine Legitimation beziehen könnten.

Was gilt, wenn auch keine geeigneten Garantien vorliegen?

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

LINK

Link zum Abruf der aktuellen Standardvertragsklauseln für den internationalen Datentransfer: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_de

LINK

Empfehlungen des Europäischen Datenschutzausschusses für zusätzliche Maßnahmen zur Herstellung eines angemessenen Schutzniveaus im Drittland: <https://cutt.ly/nHmFn1f>

Bußgelder und Sanktionen

Art. 82, 83, 84 DSGVO §§ 41 - 43 BDSG

- Die **Einwilligung der betroffenen Person** (Art. 49 Abs. 1 Buchst. 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 zu Grunde liegende Datenverarbeitung sollte, zumindest nach Ansicht der Behörden, zudem nicht systematischer Natur sein, sondern nur gelegentlich erfolgen.
- Eine Datenübermittlung **zur Erfüllung eines Vertrages** oder zur **Durchführung von vorvertraglichen Maßnahmen** auf Antrag der betroffenen Person (Art. 49 Abs. 1 Buchst. b) DSGVO). Dies kann etwa erforderlich sein bei grenzüberschreitenden Bestellungen über ein deutsches Portal oder im Fall einer Kreditkartennutzung im Ausland.

LINK

Bußgeldkonzept des Europäischen Datenschutzausschusses:
<https://t1p.de/bdjzu>

Was ist ein Transfer Impact Assessment?

Ein sogenanntes Transfer Impact Assessment (TIA) ist durch den Verantwortlichen oder Auftragsverarbeiter durchzuführen, wenn die Datenübermittlung in ein Drittland auf der Grundlage der Standardvertragsklauseln oder anderer geeigneter Garantien aus Art. 46 DSGVO erfolgt. Denn der EuGH hat in dem Urteil Schrems II entschieden, dass die Datenübermittlung in ein Drittland auf der Grundlage der geeigneten Garantien nur erfolgen darf, wenn durch das geltende Recht oder die Gepflogenheiten des Drittlands die Wirksamkeit der in Art. 46 DSGVO genannten Übermittlungsinstrumente nicht beeinträchtigt wird.

PRAXIS-TIPP

Unser Bußgeldrechner zeigt Ihnen wie hoch ein Bußgeld im konkreten Fall ausfallen könnte:
<https://dsgvo-bussgeld-rechner.de/#rechner>

Im Rahmen des TIA muss der Datenexporteur daher für die konkrete Datenübermittlung dokumentiert feststellen, ob es durch die im Drittland geltende Rechtslage oder Gepflogenheiten zu einer Beeinträchtigung der Wirksamkeit des verwendeten Übermittlungsinstruments kommt. Sollte dies der Fall sein, ist im Anschluss zu ermitteln, ob zusätzliche Maßnahmen ergriffen werden können, um die Einhaltung des unionsrechtlichen Schutzniveaus zu gewährleisten. Eine solche zusätzliche Maßnahme kann etwa die Verschlüsselung der übermittelten Daten darstellen. Sofern ein hinreichendes Schutzniveau nicht durch zusätzliche Maßnahmen hergestellt werden kann, darf die Datenübermittlung in das betreffende Drittland nicht erfolgen.

Verstößt ein Unternehmen gegen die Pflichten und Vorgaben der DSGVO, kann das weitreichende Konsequenzen haben. Neben Bußgeldern und Sanktionen, die sich direkt aus der DSGVO ergeben, enthält Art. 84 DSGVO eine Öffnungsklausel für weitere nationale Regelungen. Davon hat der deutsche Gesetzgeber in §§ 43, 44 BDSG Gebrauch gemacht.

Wie hoch können Bußgelder ausfallen?

Bei Verstößen gegen die DSGVO kann die zuständige Aufsichtsbehörde Bußgelder in Höhe von maximal 20 Millionen Euro oder 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängen (Art. 83 Abs. 5 DSGVO). Bußgelder fallen vor allem dann besonders hoch aus, wenn Verstöße gegen die Grundsätze der Datenverarbeitung in Art. 5 DSGVO festgestellt oder personenbezogene Daten ohne Rechtsgrundlage nach Art. 6 und Art. 9 DSGVO verarbeitet wurden.

Woran bemisst sich die Höhe eines Bußgeldes?

Bußgelder sollen wirksam, verhältnismäßig und abschreckend sein. Bei der Höhe der Sanktionen muss die zuständige Aufsichtsbehörde eine Reihe von Faktoren berücksichtigen. Darunter fallen insbesondere:

- Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
- jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
- Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;
- etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
- Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelpfen und seine möglichen nachteiligen Auswirkungen zu mindern;
- Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind.

Drohen wettbewerbsrechtliche Abmahnungen?

Ob Verstöße gegen die DSGVO wettbewerbsrechtlich abmahnfähig sind und Mitbewerber:innen einen Unterlassungsanspruch geltend machen können, ist derzeit noch umstritten. Dabei steht die Frage im Raum, ob ein Datenschutzverstoß überhaupt Gegenstand eines wettbewerbsrechtlichen Anspruchs auf Unterlassen sein kann. Abschließend ist dieser Streit in der Rechtsprechung noch nicht geklärt, ein entsprechendes

LINK

Um über wichtige Neuigkeiten im Datenschutz informiert zu werden, lohnt sich die Anmeldung zu unserem Newsletter:
<https://www.datenschutzkanzlei.de/newsletter/>

Vorabentscheidungsverfahren beim EuGH ist noch anhängig (Rs. C-752/22).

Können Schadensersatzansprüche geltend gemacht werden?

Bei Verstößen gegen die DSGVO können Betroffene nach Art. 82 DSGVO Schadensersatz für materiellen und immateriellen Schaden verlangen. Ein materieller Schaden meint jede Wertminderung des tatsächlichen Vermögens, die in Geld bemessen werden kann. Durch den Ersatz soll diese Minderung ausgeglichen werden. Ein immaterieller Schaden ist dagegen gegeben, wenn die Beeinträchtigung nicht konkret in Geld bemessen werden kann, wie es etwa bei der Gesundheit oder dem Persönlichkeitsrecht der Fall ist. Beispiele für immaterielle Schäden sind Diskriminierung, Rufschädigung, Verlust der Vertraulichkeit und Kontrollverlust über die eigenen Daten. Die Bemessung der konkreten Schadenshöhe obliegt dem entscheidenden Gericht, das hierzu eine Abwägung vornimmt. Der Anspruch auf Schadensersatz bildet neben dem Beschwerderecht aus Art. 77 DSGVO einen weiteren Mechanismus für individuellen Rechtsschutz im Datenschutzrecht.

Gibt es weitere Sanktionen?

Die zuständige Behörde kann neben der Verhängung von Bußgeldern Anordnungen zur Beendigung des Verstoßes aussprechen und den Verantwortlichen anweisen, die Datenverarbeitung den gesetzlichen Vorgaben anzupassen.

§ 42 BDSG legt zudem strafrechtliche Sanktionen für bestimmte Verhaltensweisen fest. So kann bei gewerbsmäßigem Vorgehen oder Bereicherungsabsicht eine Freiheitsstrafe bis zu 3 Jahren drohen.

Weiterführende Dokumente und Gesetzestexte

Wo gibt es weiterführende Informationen zum Datenschutz?

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://stiftungdatenschutz.org/ehrenamt/praxisratgeber>

Das BayLDA stellt Handreichungen für kleine Unternehmen und Vereine sowie alle Kurzpapiere der Datenschutzkonferenz zum Abruf bereit:

https://www.lida.bayern.de/de/datenschutz_eu.html

Wie erfahre ich von neuen Versionen dieses eBooks?

Dieses eBook wird regelmäßig aktualisiert. Die aktuelle Version erhalten Sie als Abonnent unseres Newsletters. Sollten Sie noch nicht angemeldet sein, können Sie dies hier nachholen:

<https://www.datenschutzkanzlei.de/newsletter/>

Wie kann die Datenschutzkanzlei unterstützen?

Rechtliche Beratung für Daten, Technologie und Marketing

Viele Geschäftsmodelle, wirksames Marketing und effizienter Vertrieb sind ohne Daten nicht mehr denkbar. Den Möglichkeiten von Digitalisierung und künstlicher Intelligenz stehen dabei neue Risiken und Rechtspflichten gegenüber. Unsere Anwält:innen sind hochspezialisierte Experten für Datenschutz- und Datenwirtschaftsrecht und beraten an dieser Schnittstelle verschiedener Rechtsgebiete. Wir unterstützen Sie bei der Umsetzung Ihrer Ideen und bei der Nutzung personenbezogener Daten innerhalb der rechtlichen Spielräume. Ob bei der Unternehmensgründung, der Entwicklung von Software und Diensten oder der Planung und Umsetzung von Datenprojekten – wir zeigen Ihnen Fallstricke und gesetzeskonforme Lösungsmöglichkeiten auf.

Externer Datenschutzbeauftragter

Bei der Datenschutzkanzlei unterstützen Sie erfahrene und zertifizierte Datenschutz-Jurist:innen in enger Abstimmung mit auf Daten, Tech und Marketing spezialisierten Rechtsanwält:innen. Wir stellen Ihnen feste Ansprechpartner:innen zur Seite, die Sie vertrauensvoll begleiten und mit Ihnen wirtschaftliche und praktikable DSGVO-Maßnahmen umsetzen. Mit unserer smarten **Datenschutz-Management-Cloud DataDesk**³ haben Sie Ihre DSGVO-Pflichten schnell im Griff und jederzeit nachweisbar. Über die **Lernplattform unserer Academy**⁴ stehen Ihnen unsere eLearnings für die gesetzlich geforderten Schulungen zur Verfügung. Wichtiges Basiswissen wird praxisnah und verständlich vermittelt – mit Teilnahmezertifikat und Reportings für Ihre Nachweispflicht.

Beratung interner Datenschutzbeauftragter

Sie sind als Datenschutzbeauftragte:r oder Datenschutzkordinator:in intern für die Umsetzung der DSGVO zuständig und wünschen Beratung, Anleitung oder einfach einen Sidekick, um Herausforderungen und Lösungsansätze zu besprechen? Gerne unterstützen wir Sie mit unserer Erfahrung aus der Tätigkeit als Datenschutzbeauftragte und Anwälte für Datenschutz.

Sprechen Sie uns an

Telefon +49. 40. 226 34 56 0
E-Mail info@datenschutzkanzlei.de

WEBSITE

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

³ <https://www.datenschutzkanzlei.de/datadesk/>

⁴ <https://www.datenschutzkanzlei.de/academy/>