# Grundsätze des Datenschutzrechts

**Einigen grundlegenden Prinzipien zum Umgang mit personenbezogenen Daten begegnet man im Datenschutzrecht immer wieder. Auf ihnen bauen alle gesetzlichen Regelungen auf.**

Von Nick Akinci

Um die DSGVO und die darin enthaltenen Anforderungen an den Datenschutz (besser) zu verstehen, ist es hilfreich, zunächst die grundlegenden Prinzipien des Datenschutzrechts kennenzulernen. Diese sind zentral in Artikel 5 der DSGVO geregelt. In diesem Artikel finden sich Grundsätze wie das Verbot mit Erlaubnisvorbehalt, der Zweckbindungsgrundsatz, der Grundsatz der Datenminimierung sowie die beiden eng miteinander verknüpften Prinzipien *Privacy by Design* und *Privacy by Default*. Darüber hinaus ist es auch wichtig zu unterscheiden, welche Arten von personenbezogenen Daten es gibt.

## Verbot mit Erlaubnisvorbehalt

Der Grundsatz des Verbots mit Erlaubnisvorbehalt ist der zentrale Grundsatz des Datenschutzrechts. Er galt bereits vor Inkrafttreten der DSGVO und besagt: Jegliche Verarbeitung von personenbezogenen Daten ist grundsätzlich erst einmal verboten, es sei denn, das Gesetz erlaubt dies ausdrücklich.

Dies mag vielleicht zunächst überraschen, ist jedoch sinnvoll angesichts des Ziels des Datenschutzes, die Persönlichkeitsrechte des Einzelnen zu schützen. Jede Datenverarbeitung muss daher auf eine Rechtsgrundlage gestützt werden, also eine gesetzliche Regelung, die es unter gewissen Voraussetzungen explizit erlaubt, dass personenbezogene Daten verarbeitet werden dürfen. In der DSGVO findet sich eine Liste dieser Rechtsgrundlagen in Artikel 6.

## Rechtsgrundlagen für die Erlaubnis

Insbesondere rund um den 25. Mai 2018 las man vielfach davon, dass unter der DSGVO fortan immer eine Einwilligung für beabsichtigte Datenverarbeitungen einzuholen sei. Dies ist schlicht falsch. Zwar bildet die Einwilligung eine der drei wichtigsten Rechtsgrundlagen der DSGVO. Daneben lassen sich Verarbeitungen aber insbesondere auf die Erfüllung eines mit dem Betroffenen geschlossenen Vertrags und auf die berechtigten Interessen der datenverarbeitenden Stelle stützen.

Zunächst darf der Verantwortliche im Rahmen von Vertragsverhältnissen, die zur Durchführung dieser Verträge erforderlichen Datenverarbeitungen vornehmen. Datenschutzrechtlich unproblematisch ist daher insbesondere die Speicherung des Namens und der Anschrift eines Vertragspartners. Beim Betrieb eines Online-Shops darf man deshalb die E-Mail-Adresse und die Zahlungsdaten des Kunden auf dieser Rechtsgrundlage speichern. Ein anderes Ergebnis dürfte auch dem gesunden Menschenverstand widersprechen, da es in der Natur einer Online-Bestellung liegt, dass diese Daten benötigt werden. Eindeutig nicht zur Erfüllung des Vertrags erforderlich wäre dagegen beispielsweise die Verwendung dieser Daten zu Werbezwecken.

Sind die infrage stehenden Datenverarbeitungen nicht zur Erfüllung eines Vertrages erforderlich, so stellt die Einwilligung der Betroffenen die wichtigste Rechtsgrundlage für den Verantwortlichen

dar, da die Datenverarbeitung dem Willen des Betroffenen entspricht und die Voraussetzungen wenig Auslegungsspielraum bieten. Trotzdem ist die Einholung einer Einwilligung des Betroffenen nicht trivial. Diese muss insbesondere freiwillig, das heißt ohne äußeren Zwang erfolgen.

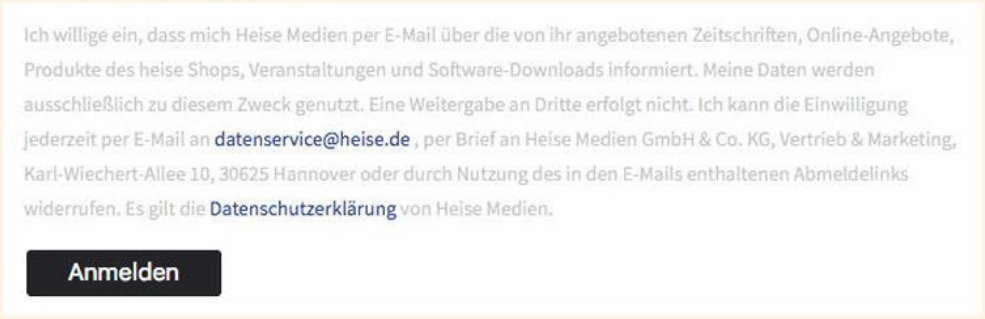
Dieses Erfordernis mündet zum einen im Kopplungsverbot: Der Datenerhebende darf eine bestimmte Leistung nicht von der Einwilligung des Betroffenen abhängig machen. Ein Online-Shop, der einen Kauf nur dann zulässt, wenn der Kunde der Weitergabe seiner Daten an Dritte zustimmt, würde daher rechtswidrig handeln.

Das Merkmal der Freiwilligkeit muss aber auch dann genauer betrachtet werden, wenn die Einwilligung im Rahmen eines Über-/Unterordnungsverhältnisses eingeholt werden soll, das heißt, wenn ein besonders großer wirtschaftlicher oder sozialer Unterschied zwischen den Betroffenen und dem Verantwortlichen besteht.

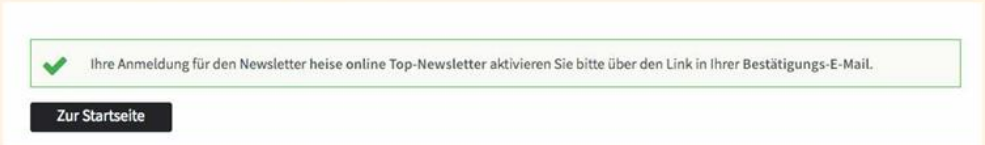
Bei der Einwilligung muss der Verantwortliche darüber hinaus im Zweifel durch entsprechende Dokumentation nachweisen können, dass sie tatsächlich eingeholt wurde. Bei Online-Einwilligungen, beispielsweise bei Newsletter-Abos, macht es daher Sinn, mit einem Double-Opt-In-Verfahren zu arbeiten: Setzt der Kunde beziehungsweise Nutzer das „Einwilligungs-Häkchen“, wird er in einer nachfolgenden E-Mail nochmals zur Bestätigung seiner Einwilligung aufgefordert. Im Kasten unten wird das Double-Opt-In-Verfahren anhand des heise.de-Newsletters verdeutlicht.

## Online-Einwilligung als Double-Opt-In

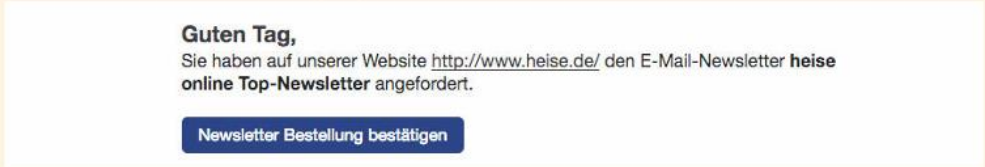
1. Erstes Opt-In auf der Website




2. Hinweis auf die Bestätigungs-E-Mail




3. Zweites Opt-In in der Bestätigungs-E-Mail



Die Einholung einer Einwilligung ist jedoch nicht immer praktikabel und teilweise sogar unmöglich. So kann zum Beispiel der Betreiber von öffentlichen U-Bahn-Stationen unmöglich die Einwilligung aller Fahrgäste einholen, diese filmen zu dürfen.

Ein weiteres Problem stellt das Erfordernis der informierten Einwilligung dar. Der Betroffene muss im Zeitpunkt der Abgabe der Einwilligung ausreichend über die Datenverarbeitungen, denen er zustimmen soll, informiert sein. Er soll vollständig im Bilde darüber sein, was mit seinen Daten geschieht, um auf dieser Grundlage seine Entscheidung treffen zu können. Vage Angaben wie etwa „Ihre Daten werden zur Bereitstellung unseres Dienstes verarbeitet“ reichen nicht aus. Insbesondere bei komplexen Online-Diensten wie Social-Media-Plattformen ist eine informierte Einwilligung oft kaum möglich. Die Datenverarbeitungsstrukturen solcher Dienste sind in der Regel so komplex, dass sie vom Nutzer nicht oder nur unter großem Aufwand erfasst werden können.

In solchen Konstellationen können Datenverarbeitungen mitunter auf die berechtigten Interessen des Datenerhebenden gestützt werden. Voraussetzung ist aber nicht nur, dass die Interessen des Verantwortlichen berechtigt, also in gewisser Weise schützenswert sind. Es muss weiterhin eine gründliche Abwägung mit den schutzwürdigen Interessen und Rechten der Betroffenen vorgenommen werden. Hat diese Abwägung zum Ergebnis, dass die Interessen der Betroffenen nicht überwiegen, so kann die Datenverarbeitung auf die berechtigten Interessen gestützt werden und ist damit rechtmäßig.

Diese Abwägung ist in den meisten Fällen jedoch alles andere als trivial und kann daher große Unsicherheiten mit sich bringen. In der Regel sollte daher das Ergebnis der Abwägung durch einen Rechtsanwalt überprüft werden. Bei manchen Szenarien sind sich Juristen jedoch darüber einig, dass das berechtigte Interesse der datenverarbeitenden Stelle in der Regel überwiegen dürfte. Zum Beispiel steht es den Rechten und Interessen der Betroffenen in der Regel nicht entgegen, wenn Kundendaten nach der Erhebung innerhalb eines Konzerns an andere konzernangehörige Unternehmen weitergegeben werden. Weiterhin dürften die Betroffeneninteressen auch dann nicht überwiegen, wenn diese im öffentlichen Raum – etwa vor einem Bargeldautomaten – von einer Videokamera erfasst werden, die dazu dient, Straftäter abzuschrecken oder diese gegebenenfalls zu verfolgen.

## Zweckbindungsgrundsatz

Der Zweckbindungsgrundsatz dürfte, neben dem eingangs erläuterten Grundsatz des Verbots mit Erlaubnisvorbehalt, das zweitwichtigste Grundprinzip des Datenschutzes darstellen. Auch dieser Grundsatz war bereits lange vor Inkrafttreten der DSGVO fest im Datenschutzrecht verankert. Er besagt, dass man die Zwecke der Verarbeitung bereits vor deren Beginn festlegen muss. Eine nachträgliche Verarbeitung zu anderen Zwecken als dem ursprünglich festgelegten ist unrechtmäßig. So dürfen eben beispielsweise IP-Adressen, die aus Gründen der IT-Sicherheit im Rahmen von Logfiles erhoben wurden, nicht für Werbung genutzt werden.

Damit wird beabsichtigt, dass der Betroffene stets Kenntnis darüber hat, was mit den ihn betreffenden Daten geschieht. Eng mit dem Zweckbindungsgrundsatz verknüpft ist daher auch die Pflicht des Datenverarbeitenden, den Betroffenen bereits vor Beginn der geplanten Verarbeitungen über die damit verfolgten Zwecke zu informieren. Wie Sie Ihre Informationspflichten mit der Datenschutzerklärung erfüllen können, erfahren Sie ab Seite 36.

Der Zweckbindungsgrundsatz ist besonders im Zusammenhang mit Big-Data-Prozessen immer wieder heftig diskutiert worden. Big-Data-Prozessen ist es immanent, dass der ursprüngliche Erhebungszweck nachträglich geändert wird, wenn Daten aus verschiedenen Quellen zusammengeführt und analysiert werden. Unter Juristen wird jedoch teils die Meinung vertreten, dass Big-Data-Prozesse jedenfalls dann rechtmäßig sein können, wenn die dadurch aggregierten Datensätze keinen Personenbezug mehr aufweisen und gewährleistet wird, dass dieser auch nachträglich nicht mehr hergestellt werden kann.

## Grundsatz der Datenminimierung

Ein weiterer zentraler Grundsatz des Datenschutzrechts ist die Datenminimierung. Der Gesetzgeber spricht in Artikel 5 davon, dass die Datenverarbeitungen „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige

Maß beschränkt" sein sollen. Die Einhaltung des Datenminimierungsgrundsatzes gewährleistet man auf verschiedene Arten und Weisen.

Zunächst sollte bereits *bei der Erhebung* der Daten darauf geachtet werden, dass man ausschließlich die tatsächlich für die Verarbeitungszwecke notwendigen Daten abfragt. Ein simples Beispiel hierfür ist das Kontaktformular auf einer Website: Wird die Anfrage vom Website-Betreiber ohnehin per E-Mail beantwortet, braucht er Daten wie die Telefonnummer oder die Anschrift des Anfragenden nicht zur Verwirklichung des (jedenfalls zunächst) ausschließlichen Erhebungszwecks „Bearbeitung und Beantwortung der Anfrage".

*Nach der Erhebung* von personenbezogenen Daten gewährleistet man die Datenminimierung insbesondere durch Anonymisierung oder Pseudonymisierung. So sollte man zum Beispiel bei Analysetools zur Reichweitenmessung im Onlinebereich stets die erhobene IP-Adresse kürzen und damit anonymisieren. Ein Pseudonymisierungsverfahren macht dagegen Sinn, wenn man die Klardaten nicht für alle geplanten Zwecke benötigt. Ein gängiges Beispiel hierfür ist die Erstellung von Käuferprofilen durch größere Unternehmen, um gezielt Werbung auszusteuern. Hier müssen die Klardaten der einzelnen Käufer, beispielsweise Name und Anschrift, zunächst durch eine pseudonyme ID ersetzt werden, bevor sie mit anderen Daten, etwa Alter und Postleitzahl, zu einem Profildatensatz zusammengefügt werden.

## Privacy by Design und Privacy by Default

Der Grundsatz *Privacy by Design* kann übersetzt werden als „Datenschutz durch Technikgestaltung". Gemeint ist damit, dass man bei der Entwicklung von Produkten oder der Vorbereitung von Projekten den Datenschutz bereits bei der Planung berücksichtigt. Beispielsweise sollte man bei größeren Datenbank-Projekten von vorn herein technisch sicherstellen, dass Daten im Bedarfsfall restlos und unter geringem Aufwand gelöscht werden können.

*Privacy by Default* meint hingegen die Implementierung datenschutzfreundlicher Voreinstellungen und ist daher eng mit dem Grundsatz der Datenminimierung verknüpft. Durch solche Voreinstellungen kann man zum Beispiel Nutzer von Online-Diensten schützen, die technisch nicht so versiert sind. So sollte in Browsern möglichst voreingestellt sein, dass Cookies, die das Nutzerverhalten tracken, geblockt werden. Ebenso sollte bei sozialen Netzwerken voreingestellt sein, dass dort eingestellte Inhalte nicht öffentlich, sondern vorzugsweise nur für „Freunde" sichtbar sind.

## Besonders sensible Daten

Ein weiteres wichtiges Prinzip ist die Unterscheidung zwischen normalen personenbezogenen Daten und solchen, die besonders sensibel und damit auch besonders schützenswert sind.

Dabei handelt es sich um Daten, die der Intimsphäre der Betroffenen zuzuordnen sind. Die DSGVO spricht in Artikel 9 von „besonderen Kategorien personenbezogener Daten" und nennt als solche „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." Der besondere Schutz dieser Informationen ist deshalb notwendig, weil diese ein hohes Risiko für die Persönlichkeitsrechte der Betroffenen darstellen. Besonders sensible Daten können die Grundlage von Diskriminierung bilden.

In gewissen Bereichen ist offensichtlich, dass es sich um sensible Daten handelt, beispielsweise bei einer Patientenakte oder der Angabe von sexuellen Vorlieben. Oftmals fällt aber erst bei genauerem Hinsehen auf, dass bestimmte Dokumente oder Datensätze auch sensible Informationen enthalten oder enthalten können. So kann zum Beispiel eine einfache Lohnabrechnung Auskunft über die Religionszugehörigkeit einer Person geben, wenn dort die Abführung von Kirchensteuer vermerkt ist. Ebenso könnte die Abbuchung eines Vereinsbeitrags auf dem Kontoauszug die politische Gesinnung einer Person erkennen lassen, wenn der Verein entsprechend bekannt ist.

Im Bereich dieser besonderen Art von Daten sind daher vor allem die Anforderungen an die Rechtsgrundlagen wesentlich höher. Die Verarbeitung kann hier nicht auf berechtigte Interessen oder die Durchführung eines Vertrages gestützt werden.

Des Weiteren steigen auch die Anforderungen an die Datensicherheit. Es gilt die Faustformel: Je sensibler ein Datum, desto höher sind die Anforderungen an die zu treffenden Sicherheitsmaßnahmen. (anm) c't


# Datenschutz-beauftragte

Von Brian Scheuch

## Neue Benennungspflichten

**Wer muss einen Datenschutzbeauftragten benennen?**

Das neue Datenschutzrecht verschärft die Anforderungen, ab wann ein Datenschutzbeauftragter (DSB) zu benennen ist, deutlich. Gemäß § 5 BDSG-neu benötigen öffentliche Stellen nun immer einen Datenschutzbeauftragten.

Für nicht-öffentliche Stellen, also Unternehmen, Vereine und andere Organisationen, ist gemäß § 38 BDSG-neu und Artikel 37 DSGVO ein Datenschutzbeauftragter unter anderem zu bestellen, wenn:

- in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind
- personenbezogene Daten geschäftsmäßig für Zwecke der Markt- oder Meinungsforschung verarbeitet werden
- Verarbeitungen vorgenommen werden, die einer Datenschutz-Folgenabschätzung unterliegen
- die Kerntätigkeit des Unternehmens in der umfangreichen regelmäßigen und systematischen Überwachung von Personen besteht
- die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten (Gesundheitsdaten, Religionsdaten, ethnische Herkunft usw.) gemäß Art. 9 DSGVO besteht

Die genannten Voraussetzungen müssen nicht kumulativ vorliegen, das heißt, die Benennungspflicht tritt ein, wenn mindestens eine dieser Alternativen gegeben ist.

Wie viele Personen an der automatisierten Verarbeitung beteiligt sind, ist dabei manchmal schwierig zu beurteilen. Wenn beispielsweise das Unternehmen insgesamt 15 Personen beschäftigt, wovon allerdings 6 Personen gar keine Daten verarbeiten, wie etwa Reinigungskräfte, dann ist kein Datenschutzbeauftragter zu benennen. Es kommt auch nicht darauf an, ob Mitarbeiter in Vollzeit oder Teilzeit arbeiten. Auch Teilzeitmitarbeiter zählen grundsätzlich als vollwertige Mitarbeiter und nicht anteilig.

## Fachliche Eignung

**Welche Voraussetzungen muss ein Datenschutzbeauftragter erfüllen?**

Artikel 37 Abs. 5 DSGVO verlangt, dass der Datenschutzbeauftragte auf Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf Grundlage seiner Fähigkeiten zur Erfüllung seiner Aufgabe benannt wird.

Eine explizite Definition, was unter berufliche Qualifikation und Fachwissen zu verstehen ist, kann man dem Gesetz nicht entnehmen. Im besten Fall verfügt der Datenschutzbeauftragte über eine Zertifizierung oder hat an einem entsprechenden Lehrgang teilgenommen.

Grundsätzlich kann sich ein angehender Datenschüt-

zer das nötige Fachwissen auch autodidaktisch aneignen. Die Datenschutzaufsicht in Nordrhein-Westfalen vertritt beispielsweise die Auffassung, dass sich das erforderliche Niveau des Fachwissens nach den durchgeführten Verarbeitungsvorgängen und dem erforderlichen Schutzbedarf der personenbezogenen Daten richtet.

Danach gilt: Je komplexer die Datenverarbeitung und je größer die Menge der verarbeiteten Daten, insbesondere sensibler Daten, desto höhere Anforderungen sind an das notwendige Fachwissen des Datenschutzbeauftragten zu stellen.

## Interessenskonflikte verhindern

**Wer darf Datenschutzbeauftragter werden?**

Der Datenschutzbeauftragte darf auch Beschäftigter des eigenen Unternehmens sein. Im Prinzip kann daher jeder Mitarbeiter, der über die entsprechende Qualifikation verfügt, als Datenschutzbeauftragter benannt werden.

Man darf jedoch niemanden benennen, der hierdurch in einen Interessenskonflikt geraten kann. Dazu gehören im Unternehmen regelmäßig folgende Gruppen:

- Geschäftsführung
- Leiter IT
- Leiter Personal
- Betriebsleiter

Diese Personengruppen können die Tätigkeit des Datenschutzbeauftragten nicht frei und unabhängig ausführen. Der IT-Leiter hat beispielsweise regelmäßig ein großes Interesse an Backups, das klassischerweise mit dem Recht auf Löschung kollidiert.

## Aufgaben

**Welche Aufgaben hat der Datenschutzbeauftragte?**

Dem Datenschutzbeauftragten unterliegen gemäß Artikel 39 und § 7 BDSG-neu mindestens folgende Aufgaben:

- Unterrichtung und Beratung des Unternehmens sowie der Beschäftigten hinsichtlich der Pflichten aus europäischen und nationalen Datenschutzvorschriften
- Überwachung der Einhaltung der Datenschutzvorschriften
- Schulung und Sensibilisierung der Mitarbeiter
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung
- Zusammenarbeit mit den Aufsichtsbehörden
- Anlaufstelle für die Aufsichtsbehörden, einschließlich vorheriger Konsultation gemäß Artikel 36 DSGVO

Der Datenschutzbeauftragte hat mit der Einführung der DSGVO eine Fülle an Aufgaben bekommen. Die Position des Datenschutzbeauftragten ist sowohl für ihn selbst, aber auch für das Unternehmen, das ihn benennt, nicht zu unterschätzen. Es ist keineswegs zu empfehlen, einen Datenschutzbeauftragten lediglich in der Datenschutzerklärung zu benennen, der ansonsten aber eher passiv tätig bleibt, wie es in der Vergangenheit oftmals geschehen ist.

Zu den wichtigsten Aufgaben gehören die Beratung, Schulung und Sensibilisierung des Unternehmens und der Mitarbeiter. Das Unternehmen und die Mitarbeiter sollen eine Anlaufstelle haben, um sich für Fragen des Datenschutzes entsprechend Rat einzuholen.

## Unternehmenspflichten

**Welche Pflichten haben Unternehmen gegenüber dem Datenschutzbeauftragten?**

Nicht nur der Datenschutzbeauftragte hat eine Fülle an Aufgaben. Auch die Unternehmen haben ihm gegenüber einige Pflichten. Unternehmen müssen sicherstellen, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in allen Fragen in Bezug auf den Schutz personenbezogener Daten eingebunden wird.

Ferner müssen Unternehmen den Datenschutzbeauftragten auch unterstützen, indem sie die zur Erfüllung seiner Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen zur Verfügung stellen.

Um seine Aufgaben ordnungsgemäß wahrzunehmen, benötigt der Datenschutzbeauftragte zunächst Arbeitszeit. Das Unternehmen muss ihm

hierfür abseits seiner Haupttätigkeit ein angemessenes Stundenkontingent einräumen. Je nach Menge der Datenverarbeitung kann dies so umfangreich sein, dass diese Tätigkeit nicht nur beiläufig zum Hauptjob erledigt werden kann. Sowohl das Unternehmen als auch der Datenschutzbeauftragte selbst sollten sicherstellen, dass ein angemessenes Stundenkontingent für die Tätigkeit zur Verfügung steht.

Um Zugang zu den einzelnen Verarbeitungsvorgängen zu erhalten, muss er darüber hinaus abteilungsübergreifend in entsprechende Prozesse mit eingebunden werden. Damit sein Anspruch auf Erhaltung seines Fachwissens erfüllt wird, müssen Unternehmen eine regelmäßige Fortbildung ermöglichen.

Der Datenschutzbeauftragte muss weisungsfrei sein. Geschäftsführer und / oder Abteilungsleiter dürfen dem Datenschutzbeauftragten keine Anweisung geben, wie er seine Aufgabe zu erledigen hat. Andernfalls könnte er nicht auf die Einhaltung datenschutzrechtlicher Vorschriften hinwirken. Die Weisungsfreiheit gilt jedoch nicht bei seiner gegebenenfalls weiter ausgeführten Haupttätigkeit.

Der Datenschutzbeauftragte berichtet direkt an die höchste Managementebene. Unternehmen müssen daher sicherstellen, dass der Datenschutzbeauftragte auch entsprechend berichten kann. In kleinen und mittelständischen Unternehmen ist dies in der Regel keine Herausforderung. In großen Konzernen sind die Wege zum höchsten Management regelmäßig sehr weit, dennoch sind gerade Konzerne verpflichtet, einen entsprechenden Prozess zur Berichterstattung zu implementieren.

## Kündigungsschutz

**? Kann dem internen Datenschutzbeauftragten gekündigt werden?**

! Der Datenschutzbeauftragte genießt gemäß § 6 BDSG-neu Kündigungsschutz. Das bedeutet: Eine ordentliche Kündigung des Datenschutzbeauftragten scheidet grundsätzlich aus, sodass diesem nur aus wichtigem Grund gekündigt werden kann. Damit der Datenschutzbeauftragte wirklich weisungsfrei arbeiten kann, darf ihm bei Monierung von Datenverarbeitungsprozessen oder bei der Kommunikation mit den Aufsichtsbehörden keine Kündigung drohen. Auch wenn der Datenschutzbeauftragte seine Tätigkeit niederlegt, besteht der Kündigungsschutz noch ein Jahr fort.

## Benennung

**? Wie wird der Datenschutzbeauftragte benannt?**

! Nach dem alten BDSG hatte die Bestellung des Datenschutzbeauftragten schriftlich zu erfolgen. Mit der Einführung der DSGVO ist dies nicht mehr zwingend notwendig. Die Benennung sollte trotzdem dokumentiert werden. Die DSGVO verlangt, dass die Kontaktdaten des Datenschutzbeauftragten veröffentlicht und der Aufsichtsbehörde mitgeteilt werden. Fast alle Aufsichtsbehörden bieten mittlerweile die Möglichkeit an, den Datenschutzbeauftragten bequem online oder per Post zu melden.

## Kontaktdaten

**? Wo sind die Kontaktdaten des Datenschutzbeauftragten anzugeben?**

! Liegt die Verpflichtung zur Benennung eines Datenschutzbeauftragten vor, so sind dessen Kontaktdaten auch zu veröffentlichen. Die Kontaktdaten sollten einerseits auf der Website des Unternehmens – in der Regel in der Datenschutzerklärung –, aber auch im unternehmensinternen Intranet veröffentlich werden. Umstritten ist derzeit noch, was alles zu den Kontaktdaten gehört. Einigkeit besteht jedoch darin, dass mindestens die E-Mail-Adresse des Datenschutzbeauftragten zu veröffentlichen ist. Eine namentliche Nennung ist hingegen nicht erforderlich.

## Externer DSB

**? Kann ich auch einen externen Datenschutzbeauftragten benennen?**

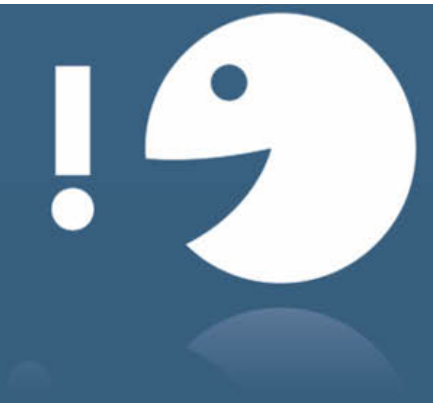
! Oftmals wird es schwierig sein, im eigenen Betrieb eine geeignete qualifizierte Person zu finden, die man als Datenschutzbeauftragten benennen kann. Dann kann man auch einen Externen als Datenschutzbeauftragten benennen. Man schont hiermit die eigenen personellen Ressourcen und kann Fortbildungskosten sparen. Ein weiterer Vorteil

kann in der Neutralität bestehen, da der externe Datenschutzbeauftragte in keinem abhängigen Arbeitsverhältnis steht. Ein Nachteil besteht jedoch darin, dass dieser teilweise nicht vollumfänglich in die internen Prozesse mit eingebunden wird und Ansprechpartner sowie Betriebsabläufe nicht gut genug kennt.

Entscheidet sich das Unternehmen für die externe Lösung, sollte es auch hier darauf achten, dass je nach Umfang der Verarbeitungstätigkeiten ein ausreichendes Stundenkontingent zur Verfügung steht. Im Internet gibt es unzählige Pauschalangebote, um einen externen Datenschutzbeauftragten zu benennen. Diese gehen von der reinen Benennung bis hin zu einem festen Beratungskontingent. Man sollte sich gut überlegen, ob man einen Datenschutzbeauftragten benennen möchte, der nur in der Datenschutzerklärung auftaucht, oder einen, der auch aktiv mitwirkt. Mit der passiven Lösung kommt man nur seiner Benennungspflicht nach. Dies führt aber regelmäßig dazu, dass man nicht vollumfänglich zum Datenschutz beraten wird und dieser auch nicht konsequent umgesetzt wird.

Lange Zeit war übrigens auch umstritten, ob der externe Datenschutzbeauftragte eine juristische Person (GmbH, AG, etc.) sein kann oder eine natürliche Person sein muss. Nach dem alten BDSG war auch die Bestellung einer juristischen Person möglich. Mit der DSGVO überwiegt nun die Ansicht, dass als Datenschutzbeauftragter immer eine natürliche Person benannt werden muss. (anm) c't

# Datenschutz-erklärung



**Jeder kennt sie, doch kaum einer macht sich die Mühe, sie zu lesen: die Datenschutzerklärung. Trotzdem gehört der auch Privacy Policy genannte Text für Unternehmen zum datenschutzrechtlichen Standard-Repertoire. Wer hier schlampt, begeht einen der offensichtlichsten Datenschutzverstöße.**

Von Nick Akinci und Joerg Heidrich

Jedes Unternehmen muss unabhängig von seiner Größe alle Betroffenen darüber informieren, wie es ihre personenbezogenen Daten verarbeitet. Hierzu ist es gängige Praxis, auf der Unternehmenswebsite eine Datenschutzerklärung zu veröffentlichen. Die DSGVO schlägt diese Vorgehensweise in den Erwägungsgründen auch ausdrücklich vor.

Im Internet findet sich mittlerweile eine Fülle an Musterdatenschutzerklärungen, die vermeintlich alles abdecken, was in den Datenschutzhinweisen enthalten sein muss. Ebenfalls erfreuen sich Datenschutzerklärungs-Generatoren großer Beliebtheit. Der Nutzer wird dabei meist aufgefordert, bestimmte Informationen über seine Website, wie das Vorhandensein eines Kontaktformulars oder von Tracking-Software, in eine Maske einzugeben. Am Ende erhält er – so wird es versprochen – eine auf seine Belange abgestimmte individuelle Datenschutzerklärung.

Hier ist jedoch Vorsicht geboten. Jede Website ist anders aufgebaut und kann Besonderheiten aufweisen, die in den Mustererklärungen nicht oder falsch dargestellt werden. Außerdem wird regelmäßig vergessen, dass im Zweifel nicht nur über die auf der Website stattfindenden Datenverarbeitungen zu informieren ist (siehe Seite 84), sondern auch über alle sonstigen datenschutzrelevanten Vorgänge im Unternehmen.

In der Regel ist es am sinnvollsten, die Betroffenen in einer abschließenden Datenschutzerklärung umfassend gleich über alle im Unternehmen und auf der Website stattfindenden Datenverarbeitungsvorgänge unterrichtet zu halten. Sucht man Unterstützung bei der Erstellung der Datenschutzerklärung, kann es daher ratsamer sein, einen auf Datenschutzrecht spezialisierten Juristen zu Rate zu ziehen.

## Zentrale Regelung

Für den Regelfall, dass personenbezogene Daten bei der betroffenen Person erhoben werden, regelt die DSGVO die Informationspflichten zentral und abschließend in Artikel 13. Die Vorschrift unterscheidet dabei zwischen Pflichtinformationen auf der einen Seite (Abs. 1) und „weiteren Informationen“

auf der anderen (Abs. 2). Letztere sind dem Betroffenen nur dann mitzuteilen, wenn sie „notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten". Aufgrund des großen Interpretationsspielraums, den diese Formulierung zulässt, wird es jedoch schwierig oder gar unmöglich sein, diese Unterscheidung rechtssicher zu treffen. Es ist daher dringend angeraten, auch diese weiteren Informationen zu vermitteln, weshalb im Folgenden nicht zwischen den beiden Kategorien unterschieden wird.

In zeitlicher Hinsicht müssen die Betroffenen bereits ab dem Zeitpunkt der Erhebung informiert werden. Die Erfüllung der Informationspflichten ist nur entbehrlich, „wenn und soweit die betroffene Person bereits über die Information verfügt".

## Verantwortlicher und Datenschutzbeauftragter

Zunächst sind dem Betroffenen der Name und die Kontaktdaten des datenschutzrechtlich Verantwortlichen mitzuteilen. Dies ist in der Regel das Unternehmen, in dem die Datenverarbeitungen stattfinden. Es sollte hier zumindest der Unternehmensname inklusive der Rechtsform beziehungsweise der Name des Einzelunternehmers, die Anschrift und eine E-Mail-Adresse genannt werden.

Ist im Unternehmen ein Datenschutzbeauftragter vorhanden, so sind ebenso dessen Kontaktdaten aufzuführen. Dieser muss jedoch nicht namentlich benannt werden – es reicht aus, wenn eine E-Mail-Adresse genannt wird, unter welcher der Datenschutzbeauftragte direkt erreichbar ist.

## Rechtsgrundlage und Verarbeitungszwecke

Weiterhin ist dem Betroffenen mitzuteilen, zu welchen Zwecken die einzelnen Datenverarbeitungen stattfinden. Der Betroffene soll wissen können, wozu seine Daten verarbeitet werden, um sich ein Bild darüber verschaffen zu können, was mit den ihn betreffenden Informationen geschieht.

Eine weitere wesentliche Pflicht besteht in der Nennung der Rechtsgrundlage für die Datenverarbeitung(en). Als wichtigste Rechtsgrundlagen sind bereits im Artikel ab Seite 14 die Verarbeitung zur Erfüllung eines Vertrages mit dem Betroffenen, die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten und die Einwilligung des Betroffenen genannt worden. Die Rechtsgrundlage muss dabei für jeden einzelnen Datenverarbeitungsvorgang präzise benannt werden.

Beruft sich das Unternehmen zur Nutzung von Informationen auf eigene berechtigte Interessen, hat es nicht nur die entsprechende Rechtsgrundlage anzugeben, sondern auch die Interessen, die es mit der Verarbeitung verfolgt. Im Falle der vorübergehenden Speicherung von IP-Adressen wäre das berechtigte Interesse etwa die Betriebssicherheit der Website.

## Weitergabe der Daten

Bei der Weitergabe von personenbezogenen Daten an unternehmensexterne Dritte ist der Betroffene über die Empfänger der erhobenen Daten zu benachrichtigen. Nutzt beispielsweise der Betreiber eines Online-Shops einen externen Zahlungsdienstleister für die Abwicklung der Bezahlung der Waren, so ist der Käufer darüber zu informieren, dass der Dienstleister die erforderlichen Zahlungsdaten erhält.

Außerdem ist auch darüber zu informieren, ob der Verarbeitende die Daten an Server im Nicht-EU-Ausland übermitteln will (siehe auch Seite 60). Hinzuweisen ist dabei ebenfalls darauf, ob für das konkrete Empfängerland ein Datenschutzabkommen existiert – wie das sogenannte Privacy-Shield-Abkommen für die USA.

## Speicherdauer und Betroffenenrechte

Darüber hinaus soll der Nutzer erfahren, wie lange Daten über ihn gespeichert werden. Es gilt die Faustregel: Benötigt man die Daten nicht mehr, sind sie zu löschen. Die aus Sicherheitsgründen nötige Nutzer-IP-Adresse sollte man beispielsweise nicht länger als 14 Tage speichern. Kann man keinen festen Zeitraum angeben, sind die Kriterien für die Speicherdauer zu nennen.

Der Betroffene muss weiterhin auch über alle ihm nach der DSGVO zustehenden Rechte „belehrt"

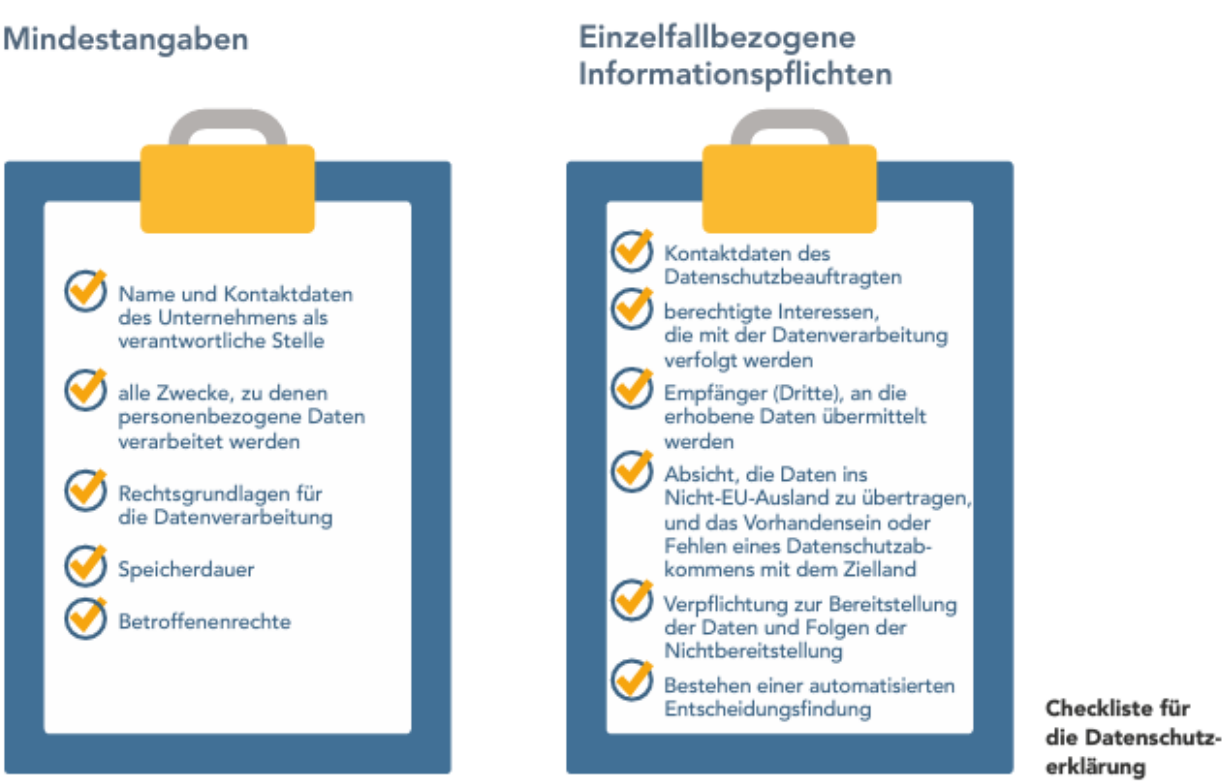
werden, die umfassend im dritten Kapitel der DSGVO geregelt sind. Details zu den Betroffenenrechten finden Sie ab Seite 18. Dabei ist es grundsätzlich ausreichend, schlicht auf das Bestehen der verschiedenen Rechte hinzuweisen. So ist es zum Beispiel beim Beschwerderecht nicht notwendig, dass auch die zuständige Datenschutzbehörde benannt wird. Beim Widerspruchsrecht gilt die Besonderheit, dass die Information darüber von den anderen getrennt zu erfolgen hat. Eine optische Hervorhebung durch Rahmung oder Fettdruck sollte hierbei aber ausreichend sein.

## Verständlichkeit steht an erster Stelle

Für alle vorgenannten Informationspflichten gilt der Grundsatz, dass die Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln" sind. Der Link zur Datenschutzerklärung sollte gut sichtbar auf der Startseite des Webauftritts stehen.

Im Text sollten juristische Fachbegriffe vermieden oder zumindest erklärt werden. Der Text muss in Deutsch und – je nach Kundenkreis – auch in weiteren Sprachen abgefasst sein. Das bedeutet, dass beispielsweise ein deutscher Online-Shop, der neben der deutschen auch in englischer Sprache verfügbar ist und einen Versand in das Vereinigte Königreich anbietet, sowohl eine deutsche, als auch eine englische Version der Datenschutzerklärung zum Abruf bereithalten muss.

Bezüglich des Textumfangs muss die Datenschutzerklärung in der Praxis mitunter einen Spagat zwischen umfassender Information und Verständlichkeit meistern. Je nachdem, welche und wie viele Datenverarbeitungen im Unternehmen stattfinden, kann sie schnell mehrere Seiten lang werden. Der Text sollte bei einer besonders umfangreichen Datenschutzerklärung klar und übersichtlich gegliedert sein. Es bietet sich dann auch




**Checkliste für die Datenschutzerklärung**

an, Details aus dem Haupttext auszugliedern und über Links für interessierte Kunden und Nutzer an separater Stelle vorzuhalten.

Eine Verletzung der Informationspflichten kann mit empfindlichen Geldbußen geahndet werden. Als Obergrenze legt die DSGVO 20 Millionen Euro respektive vier Prozent des gesamten weltweit erzielten Jahresumsatzes fest, je nachdem was höher ist. Es ist jedoch davon auszugehen, dass die Aufsichtsbehörden diesen Spielraum bei Verstößen gegen die Informationspflichten nicht voll ausschöpfen werden, da hierdurch in der Regel keine nennenswerten Schäden entstehen.

## Informationspflichten ernst nehmen

Weiterhin drohen bei Verstößen unter Umständen Abmahnungen von Konkurrenten oder „Abmahnvereinen“. Es ist – auch etliche Monate nach Wirksamwerden der DSGVO-Bestimmungen – immer noch heftig umstritten, ob eine fehlende oder unzureichende Datenschutzerklärung als Wettbewerbsverstoß durch Mitbewerber kostenpflichtig abgemahnt werden kann. Nur wenige Instanzgerichte haben sich bisher mit dieser Problematik beschäftigt und sind dabei zu unterschiedlichen Ansichten gelangt.

Unternehmen sollten daher genau prüfen, ob und wie sie personenbezogene Daten verarbeiten. Bei der Anpassung der Datenschutzerklärung kann man sich direkt am Gesetzestext orientieren, da Art. 13 der DSGVO die Informationspflichten nunmehr zentral katalogisiert aufführt. Darüber hinaus können die auf der linken Seite abgebildeten Checklisten dabei helfen, die Datenschutzerklärung zu vervollständigen. (anm) c't