Wie erfülle ich die neue DSGVO?

Inhaltsverzeichnis

[I. Wo kommen wir her und wo gehen wir hin? 2](#_Toc501552370)

[II. Was versteht man unter einer Verarbeitung personenbezogener Daten? 3](#_Toc501552371)

[III. Wer sind die betroffenen Akteure? 4](#_Toc501552372)

[IV. Was sind die Pflichten dessen, der für die Verarbeitung verantwortlich ist? 5](#_Toc501552373)

[1) Transparent sein und informieren 5](#_Toc501552374)

[2) Eine gesetzeskonforme Datenverarbeitung 7](#_Toc501552375)

[3) Die Sicherheit und Rechtmäßigkeit der Datenverarbeitung gewährleisten 8](#_Toc501552376)

[4) Ein Register der verrichteten Arbeiten führen 9](#_Toc501552377)

[5) Über Verletzungen der Datensicherheit („Data Breaches“) informieren 10](#_Toc501552378)

[V. „Accountable“ sein? Eine erhöhte Dokumentationspflicht 11](#_Toc501552379)

[VI. Welche Rechte haben die betroffenen Personen? 13](#_Toc501552380)

[VII. Wann ist ein Datenschutzbeauftragter zu ernennen? 14](#_Toc501552381)

[VIII. Schlussfolgerung 15](#_Toc501552382)

# Wo kommen wir her und wo gehen wir hin?

Die DSGVO (Datenschutz-Grundverordnung) ist ein über 80 Seiten starkes, 99 verschiedenen Artikel umfassendes Dokument, das im Mai 2016 verabschiedet wurde. Das Format der Verordnung wurde demjenigen der Richtlinie vorgezogen, um den Anwendungsbereich möglichst zu vereinheitlichen. Im Gegensatz zur Richtlinie erfordert eine Verordnung keine Anpassungen auf nationaler Ebene – über die Verabschiedung einer Umsetzungsgesetzgebung – sondern findet unmittelbar Anwendung.

Niemand darf diesen Text ignorieren, der seit Mai 2018 gilt. Die Verordnung ist aus dem Willen entstanden, den Bürgern durch die Einführung einer Rechenschaftspflicht der Akteure, die personenbezogene Daten verarbeiten, eine größere Kontrolle über die Verwendung ihrer eigenen Daten zu verschaffen.

**Die Zeiten, in denen man den Schutz personenbezogener Daten folgenlos außer Acht lassen durfte, sind vorbei**. Zahlreiche Akteure haben nunmehr ein Interesse daran, sich gegebenenfalls zu beschweren: unzufriedene Kunden, Ihre Mitbewerber, Ihre Beschäftigten, die Kommission zum Schutz der Privatsphäre…

Weitestgehend **bestätigt** die neue Verordnung **bereits bestehende Grundsätze**. Die Verpflichtung zur Sicherung der Daten existiert schon seit fast 20 Jahren; die erste diesbezügliche Richtlinie datiert von 1995. Allerdings hat niemand das bis dato groß beachtet und die vorgesehenen Sanktionen wurden nur selten angewandt. Die Vorschriften sind also nicht neu, wurden aber in mehrerer Hinsicht verschärft und angepasst. Wenn Sie den ersten Zug verpasst haben, sollten Sie nun darauf achten, dass es kein zweites Mal geschieht!

Fortan wird nämlich eine **ganze Bandbreite von strikteren Strafmaßnahmen angewandt**. Bislang waren lediglich Geldstrafen vorgesehen, zu deren Verhängung allerdings ein Strafverfahren vor einer Gerichtsbarkeit eingeleitet werden musste – wodurch sich das Risiko, dass es tatsächlich dazu kam, erheblich verringerte. Heute ist die Kommission zum Schutz der Privatsphäre befugt, sehr hohe Verwaltungsstrafe zu verhängen – und sie kann dies wesentlich problemloser tun als früher. In den schwerwiegendsten Fällen ist eine Obergrenze von 20 Millionen Euro oder 4% des Gesamtumsatzes vorgesehen.

Neben hohen Bußgeldern kann Ihnen eine zeitweilige Aussetzung oder sogar die völlige Einstellung der Datenverarbeitung, sowie ein Verbot für die Zukunft auferlegt werden. Ganz zu schweigen von den möglichen Schäden für das Image und die Glaubwürdigkeit Ihres Unternehmens.

Diese Verordnung ist also mit gewissen Anforderungen verbunden; allerdings werden sich bestimmte Teile der DSGVO auf manche Organisationen schwerwiegender auswirken als auf andere. Die DSGVO bedeutet also keine Revolution, sondern vielmehr eine Weiterentwicklung der heutigen Realität.

# Was versteht man unter einer Verarbeitung personenbezogener Daten?

Personenbezogene Daten verstecken sich in sehr vielen, völlig alltäglichen Arbeitsvorgängen. Jedes Unternehmen verarbeitet personenbezogene Daten in großem Umfang – manchmal, ohne sich dessen bewusst zu sein.

Unter **„personenbezogenen Daten“** versteht man alle Informationen, auf deren Grundlage eine Person direkt oder indirekt identifiziert oder identifizierbar wird, wie Name, Adresse, Nationalregister-Nummer, Lohndaten, Online-Profil, Anmeldedaten, IP-Adresse, eine Bewerbung, Videoüberwachungsdaten, eine Einkaufshistorie, ein Klickverhalten, Positionsdaten usw.

Als Reisebus- oder Autobusunternehmen verarbeiten Sie hauptsächlich die Daten Ihrer Reisenden, die Ihrer Kunden und die Ihrer Zulieferer.

Der Begriff der **„Verarbeitung“** wird so weitgefasst definiert, dass praktisch **jeglicher Umgang mit personenbezogenen Daten als Datenverarbeitung betrachtet wird**. Entsprechend umfasst die Datenverarbeitung die Erhebung, die Speicherung, die Aufbewahrung, die Aktualisierung, die Abänderung, das Einsehen, die Verwendung, die Übertragung, die Verbreitung, die Streichung, den Abruf usw. Die Verarbeitung beginnt also mit der Erhebung und endet mit dem Löschen der Daten.

*Beispiel: Es handelt sich folglich um Daten, die Sie tagtäglich über ein Online-Formular auf Ihrer Webseite, über ein Kontaktformular, in das der Benutzer nur eine E-Mail-Adresse einträgt, über einen Beschreibungsbogen oder ein Teilnahmeformular erheben. Andere sehr gängige Formen von Datenverarbeitung sind die Personalverwaltung und die Lohnbuchhaltung, der Download von Fahrtenschreiber-Daten, die Positionsbestimmung der Fahrer, ein unternehmensinternes Telefonverzeichnis, die Buchhaltung, das Kundenmanagement, die Überwachung (Video, Alarm, Zugangskontrolle…).*

Einzige Bedingung ist eine zumindest teilweise Automatisierung der Datenverarbeitung oder, wenn dies nicht zutrifft, allein der Umstand, dass personenbezogene Daten dazu bestimmt sind, in eine Datei aufgenommen zu werden.

*Beispiel: Während Ihres gesamten Berufslebens sammeln Sie Visitenkarten von Fachkräften, mit denen Sie zusammentreffen. Wenn Sie diese Karten lose in einer Schreibtischschublade aufbewahren, handelt es sich nicht um eine Datenverarbeitung und der Schutz der DSGVO greift hier nicht. Falls Sie diese Karten jedoch strukturiert und nach alphabetischer Reihenfolge klassieren, um eine bestimmte Person und ihre Daten leichter wiederfinden zu können, bedeutet dies eine Verarbeitung personenbezogener Daten und unterliegt folglich ganz genauen Rechtsvorschriften.*

Die einzige Ausnahme bilden Datenverarbeitungsvorgänge im Rahmen einer rein persönlichen Tätigkeit, die mit einer beruflichen oder gewerblichen Aktivität in keinem Zusammenhang steht. *Beispiel: Das Telefonverzeichnis Ihres persönlichen Handys (und nicht Ihres Firmenhandys!)*

# Wer sind die betroffenen Akteure?

**Der Datenverarbeitungsverantwortliche**

Jedes Unternehmen, jeder Selbständige, jeder Berufstätige bewahrt personenbezogene Daten auf: die seiner Kunden, die seiner Lieferanten, die seiner Mitarbeiter usw.

Keine Firma, ungeachtet ihrer Größe oder ihres Tätigkeitsbereiches, kein Berufstätiger kann sich den Auswirkungen der neuen Gesetzgebung entziehen. Die Risiken und das Ausmaß der zu ergreifenden Maßnahmen fallen je nach den betroffenen Akteuren unterschiedlich aus, aber alle Unternehmen laufen Gefahr, zum Opfer von Datendiebstahl oder Datenangriffen zu werden.

Unter der DSGVO trägt die für die Behandlung der Daten zuständige Person die wichtigste Verantwortung und bestimmt die Mittel und Zwecke der Datenverarbeitung. Wichtigstes Kriterium sind ihre Rechtsfähigkeit und ihre Organisationskapazität.

In den meisten Fällen **ist der Arbeitgeber für die Datenverarbeitung verantwortlich**. Es ist aber auch möglich, dass es mehrere für die Behandlung der Daten zuständige Personen gibt, die gemeinsam die Zwecke und Mittel der Datenverarbeitung festlegen.

**Der Auftragsverarbeiter**

Für die Verarbeitung bestimmter personenbezogener Daten können Sie einen externen Auftragsverarbeiter bestimmen. Dieser ist *„eine natürliche oder juristische Person, eine Behörde, eine Dienststelle oder eine andere Einrichtung, die im Auftrag des Datenverarbeitungsverantwortlichen personenbezogene Daten verarbeitet“*.

*Beispiele für Auftragsverarbeiter: Es kann sich um ein Sozialsekretariat handeln, um einen Reiseveranstalter, einen Personalvermittler, eine Web- oder Marketing-Agentur, einen Dienstleister im Bereich der elektronischen Archivierung, eine Behörde, einen Cloud-Service, eine Sicherheitsfirma, eine Versicherungsgesellschaft oder einen externen IT-Service.*

Wenn Sie auf Auftragsverarbeiter zurückgreifen, müssen Sie sich vergewissern, dass diese genügend Garantien dafür anbieten, dass sie Daten unter Einhaltung der DSGVO verarbeiten. Als Datenverarbeitungsverantwortlicher müssen Sie den Vertrag, den Sie mit jedem Auftragsverarbeiter abgeschlossen haben, in Bezug auf seinen Umfang, seine Laufzeit und die Verarbeitungszwecke, die betroffenen Personalkategorien, Ihre Rechte und Pflichten usw. analysieren. In den Verträgen mit Ihren Auftragsverarbeitern müssen Sie alle DSGVO-relevanten Klauseln anpassen, vor allem in Bezug auf die gemeinsame Verantwortung oder die Pflicht, jegliche Verletzung des Privatlebens zu melden. Vergewissern Sie sich, dass Sie mit „sicheren“ Partnern zusammenarbeiten.

*Beispiel: Ein zuverlässiger Auftragsverarbeiter wird einen von der Kommission zum Schutz der Privatsphäre genehmigten Verhaltenskodex anwenden. Fragen Sie zumindest Ihren Auftragsverarbeiter nach seiner Datenschutzpolitik.*

Die Verarbeitung muss nach Ihren Anweisungen erfolgen. Der Auftragsverarbeiter muss sein Eingreifen auf den Auftrag beschränken, den Sie ihm erteilt haben. Ihre Anweisungen können z.B. über ein Lastenheft oder über Anhänge zum Vertrag dokumentiert werden. Indem er diesen Rahmen überschreitet und Daten zu anderen Zwecken als denen im Vertrag vorgesehenen verwendet, wird der Auftragsverarbeiter selbst zum Datenverarbeitungsverantwortlichen und muss die Konsequenzen tragen, die sich aus diesem Status ergeben, d.h. er muss eine größere Verantwortung übernehmen.

Diesbezüglich sei darauf hingewiesen, dass es durchaus möglich ist, beide Kappen zu tragen: die des Verantwortlichen und die des Auftragsverarbeiters.

Aufgabe: Ihre Verträge mit Ihren Auftragsverarbeitern analysieren und revidieren.

**Die Kommission für den Schutz der Privatsphäre**

Die Kommission für den Schutz der Privatsphäre ist eine unabhängige Kontrollinstanz, die über die Anwendung der Verordnung wacht. Die Befugnisse dieser Kommission sind nun ausgeweitet worden. Sie kann (in schwerwiegenden Fällen) leichter Bußgelder erheben, als früher. Im Anschluss an eine Ermittlung oder Beschwerde ist die Kommission außerdem befugt, verschiedene Maßnahmen zu ergreifen, beispielsweise eine Verwarnung, eine Abmahnung, ein Mängelbeseitigungsverlangen, eine zeitweilige oder endgültige Beschränkung der Verarbeitung… Bevor es zum Bußgeld kommt, gilt es einen ganzen Prozess zu durchlaufen.

Ferner erteilt sie interpretative Guidelines zu bestimmten Begriffen und Grundsätzen der Verordnung.

# Was sind die Pflichten dessen, der für die Verarbeitung verantwortlich ist?

Ab dem Moment, wo Sie personenbezogene Daten erheben, müssen Sie eine Reihe von Verpflichtungen einhalten. Die Verordnung greift die alten Verpflichtungen der Richtlinie auf und fügt ihnen neue hinzu.

## Transparent sein und informieren

Transparenz ist ein Grundsatz, der sich durch die gesamte Verordnung zieht. Wenn Sie personenbezogene Daten erheben, müssen Sie dies immer auf eine transparente Art und Weise tun, d.h. sie müssen die betroffenen Personen in einer **klaren und verständlichen Sprache** über diese Tatsache informieren.

Sie sind verpflichtet, anzugeben, welche Art von Daten Sie sammeln und zu welchem Zweck sie dies tun, wie lange diese Daten aufbewahrt werden sollen, an wen sie weitergeleitet werden dürfen und welche Rechte Ihre Kunden in Bezug auf die eigenen Daten haben.

All diese Informationen müssen in ein verfügbaren Dokument gefasst werden, das von Ihren Kunden jederzeit eingesehen und abgespeichert werden kann; idealerweise sollten Sie es, wenn möglich, auf Ihre Webseite stellen. Es handelt sich um ein „Privacy Statement“ oder eine „Privacy Policy“, eine Datenschutzerklärung.

Aufgabe: Prüfen Sie die Informationen und passen Sie Ihre Datenschutzerklärung bei Bedarf den neuen Vorschriften an oder erstellen Sie eine Datenschutzerklärung.

## Eine gesetzeskonforme Datenverarbeitung

Die Verordnung behält die **Zustimmung** als Rechtsgrundlage bei, knüpft diese jedoch an **strengere Bedingungen**. Die Zustimmung muss aus freien Stücken, auf der Grundlage hilfreicher und unmissverständlicher Informationen erteilt werden, die in einer klaren und verständlichen Sprache abgefasst sind. Jeder Datenverarbeitungsverantwortliche muss gegebenenfalls nachweisen können, dass ihm die Zustimmung zur Verwendung der Daten erteilt wurde (wir sprechen hier von einer ausdrücklichen Zustimmung). Dies bedeutet, dass die Person, deren Daten verarbeitet werden, dieser Datenverarbeitung ausdrücklich und aus freien Stücken zustimmen muss.

Um dieser Anforderung gerecht zu werden, können Sie beispielsweise ein anzukreuzendes Kästchen vorsehen (Vorsicht, keine standardmäßig angekreuzten Kästchen verwenden!), indem Sie auf Ihre Datenschutzerklärung verweisen, die über eine Verlinkung direkt eingesehen werden kann.

Die Person, deren Daten verarbeitet werden, hat außerdem das Recht, ihre Zustimmung jederzeit zu widerrufen. Diese Widerrufung der Zustimmung ändert rückwirkend nichts an der Rechtskonformität der ursprünglichen Datenverarbeitung, sondern bezieht sich nur auf die weitere Datenverarbeitung. Die Daten dürfen künftig also nicht mehr auf der Grundlage dieser Zustimmung verarbeitet werden.

Aufgabe: Überprüfen Sie alle Formulare, mit denen Sie um die Mitteilung personenbezogener Daten bitten.

Eine Datenverarbeitung gilt auch als rechtskonform, wenn sie **zur Erfüllung des Vertrages notwendig ist**. *Beispiele:*

* *Um Ihre Arbeitnehmer bezahlen zu können, benötigen Sie deren Bankverbindung.*
* *Um im Rahmen eines Schülertransports Kinder zu Hause abholen zu können, brauchen Sie deren Adresse. Den Beruf der Eltern müssen Sie dagegen nicht kennen.*

Die Datenverarbeitung kann auch notwendig sein, um **eine Verpflichtung einzuhalten,** die der Verantwortliche per Gesetz, per Dekret oder auch per Gerichtsbeschluss erfüllen muss. *Beispiel: Die Einbehaltung der Sozialversicherungsbeiträge oder des Steuervorabzugs.*

**Das allgemeine Interesse** stellt ebenfalls eine Rechtsgrundlage dar. Dieses kann jedoch nur im Rahmen von Aufträgen der Daseinsvorsorge oder von Aufgaben, die in den Befugnisbereich von amtlichen Stellen fallen, geltend gemacht werden. Die Branche der Linien- und Reisebusse kann sich im Prinzip also nicht auf diese Rechtsgrundlage beziehen. Allerdings sind Unternehmen wie TEC oder De Lijn in diesem Zusammenhang sehr wohl berechtigt, ein Verzeichnis ihrer Abonnementinhaber zu führen.

Auch zum Schutz **lebenswichtiger Interessen** dürfen die personenbezogenen Daten eines Menschen verarbeitet werden. In diesem Fall muss es um Leben und Tod gehen und es muss im Interesse dieser Person gehandelt werden. *Beispiel: Jemand wird auf einer Reise in Ihrem Bus von einem Unwohlsein befallen und Sie müssen die Familie kontaktieren, um den Rettungsdiensten bestimmte Informationen mitteilen zu können.*

Schlussendlich gibt es noch eine letzte Rechtsgrundlage: **das berechtigte Interesse**. Diese Rechtsgrundlage kommt im Fall der Verwendung von personenbezogenen Daten zu Zwecken des Direktmarketings zum Tragen. Die betroffenen Personen um ihre Zustimmung zu bitten, erscheint hier als eine gute Option; wenn Sie jeden um seine ausdrückliche Zustimmung bitten, wird die Antwortquote jedoch höchstwahrscheinlich sehr gering ausfallen. Eine Zustimmung darf aber nicht aus Stillschweigen abgeleitet werden. Somit dürften Sie einen Großteil Ihrer Kontakte nicht mehr verwenden. Darum können Sie unter gewissen Bedingungen ein „berechtigtes Interesse“ geltend machen, insofern Ihre Kommunikation zum Ziel hat, Produkte oder Dienstleistungen zu bewerben, die sich von den zuvor vom Kunden erworbenen nicht grundlegend unterscheiden.

* Zwischen den Interessen des Unternehmens und denjenigen der Verbraucher muss ein Gleichgewicht bestehen. Insofern müssen Sie sich vergewissern, dass die betroffene Person eine nötige Information erhalten hat und vernünftigerweise damit rechnen kann, zu kommerziellen Zwecken von Ihrem Unternehmen kontaktiert zu werden.
* Das Interesse muss real und präzise definiert sein: Ihr Unternehmen strebt mit der Kommunikation über seine Waren und Dienstleistungen beispielsweise eine Optimierung seines Absatzes an.
* Die Verarbeitung personenbezogener Daten (das Versenden von Werbeangeboten an eine Datenbank) muss notwendig sein, um die berechtigten Interessen des Unternehmens zu verfolgen. Dies bedeutet im Gegenzug, dass es keine anderen Lösungen geben darf.

*Beispiel: Ein Kunde, der bereits eine Busreise gebucht hat, dürfte auch über die zukünftigen Angebote des Reisebusunternehmens informiert werden.*

Es ist im Interesse Ihres Unternehmens, Ihr Reiseangebot unter ihren Stammkunden zu bewerben, genauso wie es auch für Ihre Kunden von Interesse ist, über neue Reisen oder über die Existenz bestimmter Sonderangebote informiert zu werden.

Was so genannte **sensible Daten** angeht – also Daten in Verbindung mit der Rasse, der politischen, philosophischen oder religiösen Meinung, der Zugehörigkeit zu einer Gewerkschaft, der Gesundheit, der Biometrie, der sexuellen Orientierung, der eventuell begangenen Gesetzesverstöße oder der strafrechtlichen Verurteilungen – so ist es im Prinzip verboten, diese zu verarbeiten; von wenigen Ausnahmen abgesehen.

## Die Sicherheit und Rechtmäßigkeit der Datenverarbeitung gewährleisten

Ab dem Moment, wo Sie personenbezogene Daten erheben, müssen Sie **technische und organisatorische Maßnahmen** ergreifen, um diese Daten bestmöglich zu sichern und die Gesetzgebung einzuhalten. Sie selbst können, je nach Art und Menge der erhobenen Daten, nach dem Zweck der Datenverarbeitung oder nach den potenziellen Risiken bei Datenverlust oder -diebstahl, die Maßnahmen wählen, die Ihnen geeignet scheinen.

Unter technischen Maßnahmen versteht man Maßnahmen auf Ebene des unternehmenseigenen IT-Systems, die es zum Beispiel ermöglichen, den internen Zugriff auf die Daten zu beschränken oder diese zu verschlüsseln, zu anonymisieren[[1]](#footnote-1) bzw. zu pseudonymisieren[[2]](#footnote-2).

Die organisatorischen Maßnahmen sind Maßnahmen im Zusammenhang mit der internen Datenverwaltung. Sie können die Form einer internen Datenverarbeitungspolitik annehmen und beinhalten unter anderem die Sensibilisierung und die Schulung Ihrer Mitarbeiter, die mit Aufgaben der Datenverarbeitung betraut werden, die Sicherung des internen Netzes oder der Server, die Absicherung der Räumlichkeiten oder der Gebäude und das Verbot, nicht kontrollierbare EDV-Netze mit dem internen Netz in Verbindung zu bringen. Zu diesen Maßnahmen gehört aber z.B. auch die Anschaffung eines Schredders oder die Sperrung der USB-Anschlüsse an den Computern, so dass keine unternehmenseigenen Daten nach außen mitgenommen werden können.

Aufgabe: Nehmen Sie Kontakt zu Ihrem Lieferanten, Berater oder IT-Service auf.

## Ein Register der verrichteten Arbeiten führen

Dabei handelt es sich um eine Art Logbuch, ein Arbeitsblatt, auf dem unter anderem vermerkt wird, welche personenbezogenen Daten verarbeitet werden, aus welchem Grund, für welchen Zeitraum, für wen, wem sie weitergeleitet und wie sie geschützt werden. Dieses Register muss am Gesellschaftssitz des Unternehmens schriftlich aufbewahrt werden.

Seit Inkrafttreten der Verordnung müssen **alle Unternehmen mit mindestens 250 Beschäftigten** in schriftlicher oder elektronischer Form **ein Register aller Arbeiten führen, die unter ihrer Verantwortung verrichtet wurden.**

Zählt **ein Unternehmen weniger als 250 Beschäftigte**, muss ein solches Register nur dann erstellt werden, wenn die Verarbeitung personenbezogener Daten ein potenzielles **Risiko für die Rechte und Freiheiten der betroffenen Personen umfasst, wenn die Datenverarbeitung nicht nur gelegentlich erfolgt oder wenn sensible (medizinische oder gerichtliche) Daten verarbeitet werden.**

Die Tragweite einer Verarbeitung, „die nicht nur gelegentlich erfolgt“ bedarf noch der Klärung, denn es ist schwierig zu entscheiden, wo zwischen gängiger Praxis und gelegentlichen Vorgängen die Grenze verläuft. Für die Kommission zum Schutz der Privatsphäre sind typische Verarbeitungen, die nicht gelegentlich erfolgen (sondern regelmäßig stattfinden), Vorgänge der Verarbeitung von Kunden-, Personal- oder Lieferantendaten.

Eine Datenverarbeitung, die mit Risiken für die Rechte und Freiheiten der betroffenen Personen verbunden ist, bezieht sich auf Situationen, die beispielweise zu einer Diskriminierung, zu einem Identitätsdiebstahl oder -betrug oder zu einem finanziellen Verlust führen können.

*Beispiel: Auf manchen Webseiten muss man ein Konto mit Benutzerkennung einrichten. Wenn Sie solche Informationen aufbewahren, ist dies mit Risiken für die Rechte und Freiheiten der Personen verbunden. Es kommt nämlich häufig vor, dass auf unterschiedlichen Plattformen der gleiche Benutzername und das gleiche Passwort verwendet werden. Wenn diese Daten, die Sie speichern, von Hackern gestohlen werden, ist es sehr wahrscheinlich, dass die Hacker unter anderem auch Zugriff auf Finanzdaten erhalten.*

Aus Gründen der Sicherheit und der Vorsicht ist es sicher nicht wertlos, alle Verarbeitungsvorgänge aufzuzeichnen, die Sie durchführen. Wir empfehlen Ihnen auf jeden Fall, ein Register der verrichteten Arbeiten zu führen, denn im Fall einer Kontrolle kann dies immer hilfreich sein, um nachzuweisen, dass Ihnen der Schutz des Privatlebens Ihrer Kunden am Herzen liegt und dass Sie die neue europäische Gesetzgebung kennen.

Genauere Informationen zu Inhalt und Form dieses Registers finden Sie hier: <http://economie.fgov.be/fr/modules/publications/general/cybersecurite-votre_entreprise_est-elle_prete.jsp> und <https://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement>.

Wir werden ein vereinfachtes, branchenspezifisches Register erstellen, das Sie demnächst auf unserer Webseite finden können.

Aufgabe: Ein Register erstellen

## Über Verletzungen der Datensicherheit („Data Breaches“) informieren

Im Fall eines Problems mit den Daten, beispielsweise Verlust, Diebstahl oder Zerstörung (irrtümlich oder infolge eines unbefugten Zugriffs auf das EDV-System des Unternehmens), muss der Datenverarbeitungsverantwortliche, **sobald er von dem Problem erfährt, die Kontrollbehörde binnen 72 Stunden darüber unterrichten.**  *Beispiel: Es wurde ein Laptop gestohlen, auf dem personenbezogene Daten gespeichert waren oder eine E-Mail, die personenbezogene Daten enthielt, wurde irrtümlicherweise an eine falsche Adresse geschickt.*

Der Verantwortliche muss ferner **die betroffenen Personen schnellstmöglich** über die Verletzung der Sicherheit ihrer Daten **informieren**, wenn damit ein hohes Risiko für deren Privatleben verbunden ist. Die Verletzung der Datensicherheit könnte *beispielsweise einen Identitätsdiebstahl, eine Diskriminierung, eine Schädigung des Rufes, einen finanziellen Verlust usw. zur Folge haben.*

Aufgabe: Einen Krisenplan und ein Verfahrensprotokoll erarbeiten.

# „Accountable“ sein? Eine erhöhte Dokumentationspflicht

**Das Prinzip der *accountability* (Rechenschaftspflicht)** bedeutet, dass Sie sich nicht nur darauf beschränken dürfen, sich an die Grundsätze und Pflichten der DSGVO zu halten, sondern dass Sie auch in der Lage sein müssen, zu beweisen, dass Sie dies tun. Ab sofort findet also die Verpflichtung zu Rückverfolgbarkeit und Transparenz den Behörden gegenüber Anwendung. Dieses Prinzip liegt der Abfassung aller Unterlagen zugrunde.

In der Vergangenheit musste der Kommission zum Schutz der Privatsphäre jegliche Datenverarbeitung gemeldet werden. In der Praxis meldeten viele Unternehmen diese Vorgänge jedoch nicht; daher wurde das System geändert.

Jetzt müssen Sie nachweisen können, dass Sie technische und organisatorische Maßnahmen ergriffen haben, um die Einhaltung der Gesetzgebung zu gewährleisten. Diese Maßnahmen müssen dokumentiert werden, um zu zeigen, dass Sie die nötigen Analysen durchgeführt, die geeigneten Hilfsmittel verwendet haben usw.

*Beispiel: Es reicht nicht mehr aus, zu sagen, dass Sie eine bestimmte Software gekauft haben. Sie müssen erklären, warum Sie gerade diese und keine andere Software ausgewählt haben. Außerdem müssen Sie über Updates die Weiterentwicklung Ihres Systems gewährleisten.*

*Auch Verhaltens- und Unternehmensführungskodizes, Zertifizierungen usw. können beweisen, dass der Unternehmer alle nötigen Schritte unternimmt, um den Datenschutz zu gewährleisten.*

Aufgabe: In diesem Sinne Maßnahmen ergreifen und jeden Schritt dokumentieren.

Daneben führt die Verordnung zwei neue Prinzipien ein, die es zu beachten gilt: den Grundsatz des Datenschutzes durch Technik („**Privacy By Design“**) und den Grundsatz der datenschutzfreundlichen Voreinstellungen („**Privacy By Default“**)

Der *Datenschutz durch Technik* steht für die Notwendigkeit, den Schutz des Privatlebens Ihrer Kunden schon bei der Entwicklung eines neuen Projektes, einer neuen Entwicklung, eines neuen Produktes oder einer neuen Dienstleistung zu berücksichtigen. Sie müssen also Produkte oder Dienstleistungen gestalten, die *per se* schon datenschutzfreundlich sind. *Beispiel: Alle Daten pseudonymisieren oder die erfassten Daten von vornherein auf ein Mindestmaß beschränken.*

*Datenschutzfreundliche Voreinstellungen* bedeuten, dass Sie spontan auf den Schutz des Privatlebens Ihrer Kunden achten, ohne abzuwarten, von diesen darauf hingewiesen zu werden. Standardmäßig muss der größtmögliche Schutz gewährleistet werden. Zu jedem spezifischen Zweck werden nur die wirklich benötigten Daten verarbeitet. *Zum Beispiel dürfen die Voreinstellungen einer Webseite nicht so sein, dass einer unbestimmten Anzahl von Personen der Zugang ermöglicht wird (soziale Netzwerke).*

Aufgabe: Die Parameter für jeden Verarbeitungsvorgang überprüfen.

Jeder, der personenbezogene Daten verarbeitet, ist verpflichtet, die Vertraulichkeit, Unversehrtheit und Verfügbarkeit der Daten zu gewährleisten. Auf der Grundlage des Registers ist für jeden Verarbeitungsvorgang eine Risikoanalyse vorzusehen. Sie können Ihr Register sogar um zwei Spalten erweitern, in denen Sie die Risiken formulieren, die mit jedem spezifischen Verarbeitungsvorgang verbunden sind, sowie die Maßnahmen, mit denen Sie diese Risiken einschränken möchten.

Dabei sollten Sie sich folgende Fragen stellen:

- Wenn ich Papierakten bearbeite, befinden sich diese auf meinem Schreibtisch oder in einem Schrank? Ist der Schrank abschließbar? Wer hat Zugang zu meinem Büro? Bleibt die Tür offen oder wird sie abgeschlossen?

- Wenn ich mit Dateien arbeite, ist mein Computer durch ein Passwort geschützt? Wer kennt dieses Passwort? Speichere ich die vertraulichen Informationen in einem Ordner, der durch ein weiteres Passwort geschützt ist? Lasse ich meinen Laptop im Auto liegen?

- Wenn ich einen Server betreibe, wer hat Zugriff auf die Daten? Ist es notwendig, dass alle Zugang dazu haben? Führe ich Back-ups durch? Wenn ja, wo werden diese aufbewahrt?

- Wenn ich Daten in der Cloud speichere, wo befinden sie sich und wer hat Zugriff darauf? Gibt mein Cloud-Anbieter mir Garantien?

- Wenn ich Kamerabilder aufnehme, werden diese gespeichert und aufbewahrt? Wer darf sie einsehen und unter welchen Umständen?

*Beispiel: Sie verfügen über die Listen von Personen, die an einer einwöchigen Busreise nach Spanien teilgenommen haben. Einer Ihrer Mitarbeiter erkennt darauf den Namen seines Nachbarn. Er weiß, dass seinem Nachbarn in Zusammenhang mit einer Arbeitsunfähigkeit Ausgangsverbot erteilt wurde. Folglich könnte er seinem Nachbarn schaden, indem er ihn bei seinem Arbeitgeber denunziert. Um die Daten Ihrer Kunden zu schützen, darf diese Liste daher nur einer begrenzten Anzahl von Personen zugänglich sein. Um nicht in eine Situation wie die oben beschriebene zu geraten, müssen Sie derartige Verhaltensweisen vorwegnehmen und verhindern. Insofern ist eine Risikoanalyse durchaus sinnvoll.*

Neben dieser klassischen Risikoanalyse macht die DSGVO den Unternehmen, die bestimmte Datenkategorien nutzen oder deren Haupttätigkeit in der Verarbeitung personenbezogener Daten besteht, strengere Auflagen. In diesem Zusammenhang verweist die Verordnung erneut auf Verarbeitungsvorgänge, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen bergen, ohne jedoch genauer darauf einzugehen. Die Verordnung nennt einige Beispiele, wie die systematische Überwachung oder die umfangreiche Verarbeitung sensibler Daten. In gewissen Fällen ist vor der Verarbeitung eine formelle Datenschutz-Folgenabschätzung durchzuführen, die der Kommission zum Schutz der Privatsphäre vorgelegt werden muss.

Aufgabe: Vor jedem Datenverarbeitungsvorgang prüfen, ob eine Folgenabschätzung erforderlich ist.

# Welche Rechte haben die betroffenen Personen?

Die Verordnung greift die Rechte auf, die bereits in der Richtlinie verankert waren, und fügt diesen noch zwei neue hinzu: das Recht auf Vergessen und das Recht auf die Übertragbarkeit der Daten. Jedes Recht ist an Bedingungen geknüpft. Sie verfügen ab dem Datum der Antragstellung über eine einmonatige Frist, um die Auflagen zu erfüllen.

**Recht auf Auskunft**: Die betroffene Person hat jederzeit das Recht, Sie zu fragen, ob ihre Daten erhoben wurden. Falls ja, müssen Sie in der Lage sein, ihr bestimmte Informationen zu erteilen: Welche Daten sind betroffen, wem werden diese Daten weitergeleitet, wie lange werden sie gespeichert und welche Rechte hat die Person. Die Person darf Sie auch bitten, ihr eine Kopie ihrer Daten in elektronischem Format zur Verfügung zu stellen.

**Recht auf Berichtigung**: Falsche oder unvollständige Daten müssen auf Anfrage der betroffenen Person hin jederzeit berichtigt oder ergänzt werden können.

**Recht auf Einschränkung der Verarbeitung**: In gewissen Fällen kann die betroffene Person um eine Einschränkung der Verarbeitung ihrer Daten ersuchen. Dies bedeutet, dass die entsprechenden Daten in Ihrem EDV-System „markiert“ werden müssen und dass sie vom Unternehmen für einen bestimmten Zeitraum nicht mehr verwendet werden dürfen.

**Recht auf Löschung der Daten (auch „Recht auf Vergessen“)**: In gewissen, von der Verordnung vorgesehenen Fällen, hat die betroffene Person das Recht, die Löschung ihrer personenbezogenen Daten zu fordern. Voraussetzung dafür sind die Widerrufung der Zustimmung und das Fehlen einer Rechtsgrundlage für die Verarbeitung. In diesem Fall sind Sie verpflichtet, die Daten ohne eine unzumutbare Wartezeit zu löschen. *Beispiel: Das Recht auf Vergessen kann geltend gemacht werden, um von Google zu verlangen, jeglichen Link zu einer personenbezogenen Information, die sich online befindet, zu löschen.* Allerdings gibt es von dieser Verpflichtung eine Reihe von Ausnahmen.

**Recht auf Datenübertragbarkeit**: Bei einer automatisierten Datenverarbeitung, die auf Zustimmung fußt oder die zur Erfüllung eines Vertrages notwendig ist, kann die betroffene Person Sie um die Übermittlung ihrer personenbezogenen Daten in einem „strukturierten, gängigen, maschinenlesbaren und interoperablen Format“ ersuchen. In gewissen Fällen darf sie den Verantwortlichen sogar darum bitten, dass er einem neuen Datenverarbeitungsverantwortlichen die Daten selbst übermittelt. *Zum Beispiel könnte ein Facebook-Nutzer von Facebook verlangen, alle seine Daten einem anderen sozialen Netzwerk zu übertragen, oder ein Luminus-Kunde könnte von Luminus verlangen, alle seine Daten an Engie zu übertragen. Genauso könnte ein Inhaber einer Mailbox darum bitten, alle Mails, die er über diese Mailbox erhalten oder verschickt hat, sowie die Liste der Kontakte, die er erstellt hat, in einem digitalen Format zu erhalten.*

Das Recht auf Datenübertragbarkeit hat zum Ziel, den natürlichen Personen eine gewisse Kontrolle über ihre Daten zurückzugeben. Es verankert gleichzeitig die Rechte auf Zugänglichkeit, Transparenz und Löschung der Daten. Natürlich ist das Recht auf Datenübertragbarkeit mit gewissen technischen Auswirkungen verbunden.

Aufgabe: Protokolle verabschieden, die es ermöglichen, auf alle Anfragen fristgerecht einzugehen.

# Wann ist ein Datenschutzbeauftragter zu ernennen?

Die DSGVO räumt einem neuen Akteur auf dem Gebiet des Schutzes personenbezogener Daten einen zentralen Stellenwert ein: dem Datenschutzbeauftragten, nach dem englischen Begriff „Data Protection Officer“ auch häufig „DPO“ genannt.

In diesem Zusammenhang sei darauf hingewiesen, dass die Bezeichnung eines DPO, sowohl für die Verantwortlichen als auch für die Auftragsverarbeiter, in gewissen Fällen vorgeschrieben ist:

- Wenn sie dem öffentlichen Dienst angehören;

- Wenn ihre Kerntätigkeit in Verarbeitungsvorgängen besteht, die eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang erfordern;

- Wenn ihre Kerntätigkeit in der (ebenfalls umfangreichen) Verarbeitung „besonderer“ Kategorien von personenbezogenen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht.

Die Umstände, welche die Bezeichnung eines DPO zwingend vorschreiben, sind in der Verordnung verhältnismäßig weit gefasst und bedürfen einer Auslegung: Was versteht man insbesondere unter einer „regelmäßigen und systematischen“ Überwachung oder was ist eigentlich „umfangreich“? Diese Begriffe müssen von der Kommission zum Schutz der Privatsphäre ausgelegt werden.

Der Datenschutzbeauftragte kann ein Arbeitnehmer sein, aber auch ein unabhängiger Dienstleistungsanbieter. Er übt eine Beratungs- und Kontrollfunktion aus und fungiert als Ansprechpartner der Kontrollbehörde. Er überwacht also innerhalb des Unternehmens, dass alle Daten gesetzeskonform verarbeitet werden. Er muss in der Lage sein, **innerhalb des Unternehmens unabhängig zu handeln**. Er muss auf höchster Management-Ebene Bericht erstatten und darf nicht aus Gründen im Zusammenhang mit der Ausübung seiner Funktion entlassen werden.

Der DPO muss ein Experte auf dem Gebiet der Datenschutzgesetzgebung sein, aber auch das Unternehmen, seine Funktionsweise und sein Marktumfeld sehr genau kennen. Abgesehen davon ist es wichtig, Interessenkonflikte zu vermeiden. *Zum Beispiel ist es in den meisten Fällen nicht empfehlenswert, einen EDV-Verantwortlichen zum DPO zu machen, denn als solcher muss er die Schutzmaßnahmen kontrollieren, die von seinem eigenen Team ergriffen wurden.*

Die DSGVO enthält keine Vorschriften über Diplome oder Bescheinigungen, die ein DPO besitzen muss und macht auch keine genauen Angaben dazu, welche Kenntnisse oder welche Erfahrung zur Ausübung seiner Funktion besonders wichtig sind.

Die anderen Unternehmen haben jedoch immer die Möglichkeit, einen DPO zu ernennen. Es ist in jedem Fall empfehlenswert.

Aufgabe: Wenn nötig einen DPO ernennen.

# Schlussfolgerung

Leider fühlen sich KMU von alldem noch allzu oft nicht betroffen, weil sie meinen, für Hacker uninteressant zu sein. Was gestern noch stimmte, trifft heute nicht mehr zu. Es ist vielmehr so, dass Hacker sich heute verstärkt für KMU interessieren, denn die großen Unternehmen, die bereits zum Ziel von Angriffen wurden, haben inzwischen Schutzmaßnahmen ergriffen. Bei KMU ist dies häufig noch nicht der Fall.

Die DSGVO einzuhalten, bedeutet, eine Reihe von Maßnahmen zu ergreifen, Verfahren einzuleiten, Zeit aufzuwenden und sowohl personelle als auch finanzielle Ressourcen zu mobilisieren. Dies sind aber keine unüberwindlichen Hindernisse. Betrachten Sie die neue Gesetzgebung als Wettbewerbsvorteil oder als Werbemittel, mit dem Sie bei Ihren Kunden und Lieferanten punkten können. Die zahlreichen Rechtsmittel, sowie die Maßnahmen und Sanktionen, die verhängt werden können, sollten Sie überzeugen, sich mit dem Gesetz in Einklang zu bringen.

Egal, wie viele Firewalls oder Virenschutzprogramme Sie haben – es gibt gesetzliche Verpflichtungen, denen sich niemand entziehen darf. Es ist die Gelegenheit, Informationen und die IKT besser zu schützen und ein Mindestmaß an Methode in Ihr Management zu bringen.

Natürlich stehen wir Ihnen bei Fragen jederzeit gerne zur Verfügung! Zögern Sie bitte nicht, uns zu kontaktieren.

1. Bei einer Anonymisierung werden die personenbezogenen Daten so verändert, dass die Person, auf die sie sich beziehen, nach der Verarbeitung nicht mehr zu identifizieren ist. Dieser Prozess muss irreversibel sein. Es darf nicht möglich sein, eine Anonymisierung rückgängig zu machen. [↑](#footnote-ref-1)
2. Die Pseudonymisierung ermöglicht, die Daten, die eine direkte Identifizierung ermöglichen, von den übrigen, nicht sachdienlichen Daten zu trennen. Im Zuge dieses Prozesses wird ein Identifizierungsschlüssel erstellt, mit dessen Hilfe sich zwischen den verschiedenen personenbezogenen Informationen eine Verbindung herstellen lässt. Diese Identifizierungsschlüssel müssen sicher aufbewahrt und mit einer robusten Zugangskontrolle geschützt werden. Auf diese Weise sind die gespeicherten Daten zwar nicht anonym, aber trotzdem nicht identifizierbar. Es handelt sich beispielsweise um die letzten 4 Ziffern einer Kreditkartennummer, die bei Online-Zahlungen am Bildschirm eingeblendet werden. [↑](#footnote-ref-2)