IN DIESEM KAPITEL

- lernen Sie Begriffe kennen, mit denen Sie protzen können
- erfahren Sie, wo Sie sich vertiefter mit diesen beschäftigen können
- können Sie feststellen, ob Sie bis zehn zählen können

Bonuskapitel
Mehr als 10 Begriffe, die Sie kennen sollten

Wenn Sie im Datenschutz mitreden wollen, müssen Sie bestimmte Begriffe kennen, sonst merkt jeder gleich, dass Datenschutz nicht gerade Ihre Stärke ist. Kennen Sie schon einmal die folgenden, haben Sie eine gute Basis, das Vorhandensein umfangreicher Datenschutzkenntnisse zu simulieren.

Die Grundprinzipien

Bei den *Grundprinzipien* – oder auch *elf Geboten* des Datenschutzes –, wie sie in diesem Buch genannt werden, handelt es sich um die Grundsätze nach Art. 5, die bei jeder Verarbeitung personenbezogener Daten immer und unbedingt eingehalten werden müssen:

- ✔ Grundsatz der *Rechtmäßigkeit*, Art. 5 Abs. 1 a)
- ✔ Grundsatz von *Treu und Glauben*, Art. 5 Abs. 1 a)
- ✔ Grundsatz der *Transparenz*, Art. 5 Abs. 1 a)
- ✔ Grundsatz der *Zweckbindung*, Art. 5 Abs. 1 b)
- ✔ Grundsatz der *Datenminimierung*, Art. 5 Abs. 1 c
- ✔ Grundsatz der *Richtigkeit*, Art. 5 Abs. d)
- ✔ Grundsatz der *Aktualität,* Art. 5 Abs. d)

- ✔ Grundsatz der *Speicherbegrenzung*, Art. 5 Abs. 1 e)
- ✔ Grundsatz der *Integrität,* Art. 5 Abs. 1 f)
- ✔ Grundsatz der *Vertraulichkeit*, Art. 5 Abs. 1 f)
- ✔ Grundsatz der *Rechenschaftspflicht*, Art. 5 Abs. 2)

Mit den Grundprinzipien können Sie sich ausführlicher beschäftigen in Kapitel 5 *Die elf Gebote der DSG*VO.

Personenbezogene Daten

Im Datenschutz werden nur *personenbezogene Daten* geschützt. Dabei handelt es sich kurz gesagt um alle Daten, über die sich ein Bezug zu einer *natürlichen Person*, also einem Menschen herstellen lässt. Manchmal ist das ganz einfach, nämlich dann, wenn es sich um den Namen einer Person handelt und Sie die Person auch kennen. Dann wissen Sie, dass zwischen dem Namen und der Person ein Bezug besteht. Dann gibt es aber auch solche Daten, bei denen das nicht auf den ersten Blick erkennbar ist. Wenn Sie eine Personalnummer sehen, nehmen Sie zunächst nur eine kryptische Zeichenabfolge wahr. Da sich der Mitarbeiter aber identifizieren lässt, der sich hinter der Personalnummer verbirgt, gehört auch diese zu den personenbezogenen Daten. Und dann gibt es noch Beziehungen von Personen zu anderen Personen oder zu Gegenständen. Das kann zum Beispiel ein Vertragsverhältnis sein oder das Eigentum an einem Fahrzeug. Auch solche Informationen gehören zu den personenbezogenen Daten und unterliegen daher dem Datenschutz.

Besondere Kategorien

Es gibt auch noch *besondere Kategorien* von personenbezogenen Daten. Das sind besonders sensible Daten, deren unbefugte Verwendung für die Betroffenen zu besonders schweren Folgen führen kann. Die DSGVO gibt diesen deshalb auch einen besonderen Status und schützt sie noch stärker als die übrigen personenbezogenen Daten. Grundsätzlich gilt, dass die besonderen Kategorien nur mit einer ausdrücklichen Einwilligung verarbeitet werden dürfen und die sonst üblichen Rechtsgrundlagen nicht genügen. Dabei handelt es sich um folgende Daten:

- ✔ Angaben über die rassische und ethnische Herkunft
- ✔ Angaben über politische Meinungen
- ✔ Angaben über religiöse oder weltanschauliche Überzeugungen
- ✔ Angaben zur Gewerkschaftszugehörigkeit
- ✔ Genetische Informationen

- ✔ Biometrische Informationen
- ✔ Angaben zur Gesundheit
- ✔ Informationen zum Sexualleben oder der sexuellen Orientierung

Wenn Sie sich intensiver mit *personenbezogenen Daten* und *besonderen Kategorien* beschäftigen wollen, blättern Sie einfach zurück zu Kapitel 2 *Personenbezogene Daten*.

Datenschutzbeauftragter

Der betriebliche *Datenschutzbeauftragte* hat die Aufgabe, darauf hinzuwirken, dass das Unternehmen sich an die Vorschriften des Datenschutzes hält. Er berät intern alle Abteilungen im Datenschutz, kontrolliert die Einhaltung der internen Datenschutzprozesse, schult Mitarbeiter und dient auch zugleich allen Mitarbeitern als vertrauliche Anlaufstelle. Deshalb unterliegt der Datenschutzbeauftragte auch der Schweigepflicht über alles, was ihm vertraulich mitgeteilt wurde. Der Datenschutzbeauftragte wird von dem Verantwortlichen benannt und muss einige fachliche und persönliche Voraussetzungen mitbringen, um den Job machen zu dürfen. Bei der Wahrnehmung seiner Aufgaben ist er *weisungsfrei*, berichtet aber in regelmäßigen Abständen über seine Tätigkeit und gewonnenen Erkenntnisse an die Geschäftsführung. Wenn das Unternehmen einen Datenschutzbeauftragten benannt hat, wozu es nicht immer verpflichtet ist, muss dieser an die zuständige Aufsichtsbehörde für den Datenschutz gemeldet werden.

Wann ein *Datenschutzbeauftragter* von einem Verantwortlichen benannt werden muss und was sonst noch alles wichtig ist im Zusammenhang mit dem Datenschutzbeauftragten, können Sie vertieft nachlesen in Kapitel 4 *Die Protagonisten* unter der Überschrift *Der Datenschutzbeauftragte*.

Verarbeitungsverzeichnis

Das *Verarbeitungsverzeichnis* hat viele Namen. In Art. 30 bezeichnet es der Verordnungsgeber etwas sperrig als *Verzeichnis von Verarbeitungstätigkeiten*. Gebräuchlich sind aber auch die Bezeichnungen *Verfahrensverzeichnis*, *Verarbeitungsübersicht*, *Verfahrensliste* und vielleicht noch mehr. Im Verarbeitungsverzeichnis müssen Verantwortliche alle *Verarbeitungstätigkeiten* auflisten, die im Unternehmen standardmäßig durchgeführt werden. Eine solche Verarbeitungstätigkeit kann zum Beispiel die *Erfassung von Arbeitszeiten* sein oder die *Abwicklung von Kundenbestellungen*. Im Verarbeitungsverzeichnis müssen Sie zu Ihren Verarbeitungstätigkeiten die folgenden Angaben machen:

- ✔ Namen und Kontaktdaten des *Verantwortlichen*
- ✔ Kontaktdaten des *Datenschutzbeauftragten*
- ✔ *Betroffenenkategorien*

- ✔ *Datenkategorien*
- ✔ *Verarbeitungszwecke*
- ✔ *Datenempfänger*
- ✔ *Drittlandübermittlung*
- ✔ *Löschfristen*
- ✔ Beschreibung *technisch-organisatorischer Maßnahmen*

Genaueres zum *Verarbeitungsverzeichnis* und wie Sie es am besten erstellen, erfahren Sie in Kapitel 10 *Datenschutzmanagement* unter der Überschrift *Wichtige Dokumente* und dort unter *Verarbeitungsverzeichnis*.

Einwilligung

Die *Einwilligung* ist eine von mehreren *Rechtsgrundlagen* des Art. 6, auf die Sie die Verarbeitung personenbezogener Daten stützen dürfen. An die Wirksamkeit von Einwilligungen sind strenge Bedingungen geknüpft. So muss die Einwilligung immer freiwillig sein, und vor der Abgabe der Einwilligungserklärung müssen die Betroffenen transparent informiert werden darüber, was mit ihren Daten geschehen wird. Einwilligungen müssen auch immer ausdrücklich erklärt werden. Ein Schweigen auf die Frage, ob eine Einwilligung abgegeben wird, kann zum Beispiel niemals als Zustimmung gewertet werden, und auch aus dem Verhalten Betroffener darf nicht voreilig der Schluss gezogen werden, dass damit auch zugleich eine Einwilligung abgegeben werden soll. Die Einwilligung muss auch inhaltlich bestimmte Anforderungen erfüllen. Voraussetzungen einer wirksamen Einwilligung sind

- ✔ Freiwilligkeit
- ✔ Bezugnahme auf einen bestimmten Fall
- ✔ *informierte* Abgabe
- ✔ unmissverständliche Formulierung
- ✔ eindeutig bestätigende Handlung
- ✔ Willensbekundung
- ✔ leicht zugängliche Form
- ✔ einfache und klare Sprache
- ✔ kein Widerruf
- ✔ keine Verwirkung

Welche *Rechtsgrundlagen* es außer der Einwilligung noch so alles gibt und was bei der Einholung von Einwilligungen genau beachtet werden muss, können Sie nachschlagen, wenn Sie zurückblättern zu Kapitel 6 *Nicht erlaubt ist auch verboten* zur Überschrift *Die einzelnen Erlaubnistatbestände* und dort unter *Einwilligung*.

TOM

Mit TOM meint man die sogenannten *technisch-organisatorischen Maßnahmen,* die ergriffen werden, um den Schutz personenbezogener Daten sicherzustellen. Diese Maßnahmen sollen sicherstellen, dass folgende Ziele erreicht werden können, nämlich eine wirksame

- ✔ Zutrittskontrolle,
- ✔ Zugangskontrolle,
- ✔ Zugriffskontrolle,
- ✔ Eingabekontrolle,
- ✔ Weitergabekontrolle,
- ✔ Verfügbarkeitskontrolle,
- ✔ Auftragskontrolle
- ✔ Intervenierbarkeit und
- ✔ Nichtverkettung.

Welche Maßnahmen konkret ergriffen werden können, um diese Ziele zu erreichen, können Sie vertieft nachlesen in Kapitel 9 *Technisch-organisatorische Maßnahmen* unter der Überschrift *Festlegung von TOM* und dort unter *Überblick über mögliche TOM*.

Datenschutzfolgenabschätzung

Bei der *Datenschutzfolgenabschätzung* handelt es sich um ein Instrument, das von der DS-GVO vorgegeben ist, um hohe Risiken, die Datenverarbeitungen für Betroffene bergen, in den Griff zu bekommen. Datenschutzfolgenabschätzungen fußen auf *Risikoanalysen*, bei denen die möglichen Schäden für Betroffene und die Wahrscheinlichkeit, dass diese sich realisieren, ermittelt werden. Stellt sich heraus, dass die Risiken für die Betroffenen hoch sind, muss die Datenschutzfolgenabschätzung durchgeführt werden. Der Verantwortliche muss dann überprüfen, ob die Verarbeitung tatsächlich erforderlich ist, und Abhilfemaßnahmen festlegen. Anschließend kommt es zu einer erneuten Risikoanalyse, und es wird untersucht, ob die Abhilfemaßnahmen in der Lage sind, das Restrisiko für die Betroffenen auf ein erträgliches Maß zu reduzieren. Datenschutzfolgenabschätzungen müssen immer

vor der Aufnahme der Datenverarbeitung durchgeführt werden. Kommt die Datenschutzfolgenabschätzung also zu dem Ergebnis, dass das hohe Risiko für die Betroffenen nicht auf ein erträgliches Maß reduziert werden kann, darf mit der Datenverarbeitung nicht begonnen werden. Es gibt dann jedoch die Möglichkeit, die Aufsichtsbehörde um Rat zu fragen, was getan werden kann.

Wenn Sie sich mit der *Datenschutzfolgenabschätzung* näher beschäftigen möchten, können Sie das, indem Sie zurückblättern zu Kapitel 9 *Technisch-organisatorische Maßnahmen* und dort zur Überschrift *Datenschutzfolgenabschätzung*.

Auftragsverarbeitung

Wenn Sie personenbezogene Daten von einem anderen in Ihrem Auftrag verarbeiten lassen, spricht man von einer *Auftragsverarbeitung*. Damit Auftragsverarbeitungen zulässig sind, müssen Sie mit Ihrem Auftragsverarbeiter einen Vertrag nach den Vorschriften des Art. 28 abschließen. Solche Verträge nennt man dann *Auftragsverarbeitungsverträge*. Auftragsverarbeiter zeichnen sich vor allem dadurch aus, dass sie die Daten, die Sie ihnen zur Verarbeitung überlassen, immer nur nach Ihrer ausdrücklichen *Weisung* verarbeiten und die Daten unter keinen Umständen für eigene Zwecke verwenden dürfen. Wenn ein wirksamer Auftragsverarbeitungsvertrag abgeschlossen wurde, wird der Auftragsverarbeiter so behandelt, als wäre er Teil des Verantwortlichen, für den er tätig ist. Man spricht in diesem Zusammenhang von der *Fiktion der Nichtübermittlung*.

Näheres zur Auftragsverarbeitung, wie sie sich von anderen Dienstleistungs- oder Geschäftsbesorgungsverhältnissen oder zur gemeinsamen Verantwortung abgrenzt und welche Anforderungen an Auftragsverarbeitungsverträge gestellt werden, können Sie noch einmal nachschlagen in Kapitel 7 *Zusammenarbeit von Unternehmen* unter der Überschrift *Die Auftragsverarbeitung*.

Pseudonymisierung

Bei der *Pseudonymisierung* werden personenbezogene Daten so verändert, dass sich der Personenbezug nur noch herstellen lässt unter Zuhilfenahme weiterer zusätzlicher Informationen. Denken Sie zum Beispiel an Ihre Steuer-Identifikationsnummer. Wer diese Nummer sieht, hat keine Ahnung, dass Sie sich dahinter verbergen. Außer Ihnen, dem Finanzamt und Ihrem Steuerberater weiß es zunächst einmal niemand. Im Finanzamt ist jedoch hinterlegt, dass die Steuernummer Ihnen gehört. Gleiches gilt zum Beispiel auch für Ihre Personalnummer. Die Pseudonymisierung ist eine *Maßnahme zum Schutz* personenbezogener Daten und soll nach dem Wunsch der DSGVO möglichst immer eingesetzt werden, wenn das mit einem verhältnismäßigen Aufwand machbar ist. Gehen pseudonymisierte Daten verloren oder werden diese anderen unbefugt offengelegt, handelt es sich immer noch um eine Datenschutzverletzung, denn auch pseudonymisierte Daten zählen noch zu den personenbezogenen Daten. Erst wenn der Personenbezug für niemanden mehr herstellbar wäre, spricht man von anonymisierten Daten, die dann auch nicht mehr dem Schutz der DSGVO unterliegen.

Datenschutzverletzung

Von einer *Datenschutzverletzung* oder auch *Datenpanne* spricht man immer dann, wenn personenbezogene Daten unbefugt vernichtet, zerstört oder verändert oder unbefugten Personen gegenüber offengelegt werden. Datenschutzverletzungen lösen die Meldepflicht nach Art. 33 und 34 aus und können zu Schadensersatzansprüchen der Betroffenen sowie Geldbußen führen. Haben Sie es gemerkt? Wir haben Ihnen noch einen elften Begriff untergejubelt.

Näheres zum Umgang mit Datenschutzverletzungen können Sie nachlesen in Kapitel 10 Datenschutzmanagement unter der Überschrift Datenschutzmanagement-System (PDCA), dort unter Projektplanung (Plan) / Einzelziele / Meldeverfahren bei Datenschutzverletzungen etabliert.