WIRTSCHAFTSKAMMER ÖSTERREICH

Praxisleitfaden zur

Umsetzung der DSGVO

2., aktualisierte Auflage vom September 2023

HINWEIS:
Um eine leichtere Lesbarkeit des Textes zu gewährleisten, wurde im vorliegenden Leitfaden auf die explizit geschlechtsspezifische Schreibweise verzichtet. Hierfür wurde als Vereinfachung stellvertretend für alle Geschlechtsformen jeweils die kürzere männliche Schreibweise angewandt.

Einleitung

In heutiger Zeit ist es für uns alle selbstverständlich, unsere Daten im Internet bekannt zu geben und dort zu verarbeiten. So melden wir uns für die verschiedensten Online-Plattformen von sozialen Netzwerken bis zum Online-Shopping und -Banking an. Was aber genau mit unseren Daten geschieht, wem diese übermittelt werden, wo sie gespeichert sind und wie sicher sie aufbewahrt werden, ist häufig unklar.

Um diesem „Wildwuchs" an Datenverarbeitungen entgegenzuwirken, hat die EU beschlossen, die Verarbeitung personenbezogener Daten transparenter zu gestalten und den Betroffenen die Kontrolle über ihre Daten zu erleichtern.

Die Europäische Datenschutzgrundverordnung, kurz DSGVO, wurde zu diesem Zweck im April 2016 beschlossen. Sie ist seit Mai 2018 verbindlich und regelt den Umgang mit personenbezogenen Daten. Für alle Unternehmen, die in der EU tätig sind, gilt es daher, den Umgang mit personenbezogenen Daten genau zu regeln und achtsam mit diesen Daten umzugehen. Daraus ergibt sich konkreter Handlungsbedarf.

Der Schwerpunkt dieser Publikation liegt in der praktischen Umsetzung der Datenschutzvorschriften im Betrieb. **Eine Erläuterung der rechtlichen Bestimmungen finden Sie jeweils in der Randleiste bei den entsprechenden Kapiteln. Sie finden darin auch Hilfestellungen, die anhand von konkreten Beispielen beschrieben werden.**

Beachten Sie bitte jedoch:

- alle Inhalte bilden die derzeit aktuelle Rechtslage ab
- die rechtliche Detailinformation ist bei der konkreten Umsetzung jedenfalls zu beachten. Im Zweifel kontaktieren Sie bitte die Experten Ihrer Wirtschaftskammer
- Dieser Leitfaden soll einen generellen Weg bei der Umsetzung der DSGVO darstellen, der jedoch nicht alle denkbaren betrieblichen Erfordernisse berücksichtigen kann.

Die Umsetzungsfrist für die DSGVO endete mit 25. Mai 2018.
Seit diesem Zeitpunkt müssen alle Bestimmungen der DSGVO umgesetzt ein.

Wer muss die DSGVO umsetzen?

Alle Unternehmen, die in der EU tätig sind und Daten von Personen verarbeiten, müssen die Anforderungen der DSGVO jedenfalls umsetzen. Dabei spielt es keine Rolle, wo das Unternehmen seinen Sitz hat. Es kommt nur darauf an, ob das Unternehmen Daten von Bürgern in der EU verarbeitet.

Die DSGVO betrifft so gut wie alle Unternehmen.

Online Ratgeber - Datenschutz-Grund-verordnung

Anwendungsbereich der DSGVO

FAQ - Betrifft mich die DSGVO?

Was sind personenbezogene Daten?

Daten sind dann personenbezogen, wenn damit eine natürliche Person identifiziert oder identifizierbar ist. Das ist beispielsweise bei eindeutigen Kennungen wie einer Kreditkartennummer, einer Sozialversicherungsnummer, einer E-Mail-Adresse, aber auch bei einer Kombination von Adresse und Geburtsdatum möglich.

Ebenso personenbezogen sind Daten, die einer natürlichen Person zugeordnet sind. Typisches Beispiel sind Rechnungen, die Sie einer natürlichen Person zugeordnet haben oder auf denen der Sachbearbeiter vermerkt ist.

FAQ - Was sind personen-bezogene Daten?

Wichtige Begriffs-bestimmungen

Umsetzung der DSGVO im Überblick

Die DSGVO ist ein umfassendes Regelwerk mit einer Reihe von Anforderungen, die erfüllt und Aufgaben, die erledigt werden müssen. Auf den folgenden Seiten finden Sie eine Übersicht über die wichtigsten Schritte.

Erhebung aller Verarbeitungsvorgänge & personenbezogenen Daten

Stellen Sie fest, wo und wie Sie Daten natürlicher Personen (= betroffener Personen) in Ihrem Unternehmen verarbeiten. Üblicherweise handelt es sich bei den natürlichen Personen um Mitarbeiter, Kunden oder Lieferanten sowie Interessenten (Newsletter) oder Webseite-Besucher. Deren Daten werden beispielsweise für die Lohn- und Gehaltsverrechnung, die Kundenakquise & -betreuung sowie den Versand von Newslettern und den Betrieb der IT verwendet.

Im Zuge dieser Erhebung wird festgestellt,

- welche Daten im Detail Sie konkret verarbeiten,
- wo diese abgespeichert sind (z.B.: Personalverarbeitung, Mitarbeiter- oder Kundendatenbank, Online-Shop-System)
- ob es sich dabei um besondere Kategorien von Daten (z.B.: Gesundheitsdaten in der Personalverwaltung) handelt und
- ob Sie diese Daten auch tatsächlich benötigen.

Prüfung der Zweckbindung und Rechtmäßigkeit

Haben Sie festgestellt, welche Daten Sie verarbeiten, so ist zu überlegen, zu welchem Zweck Sie diese Daten verarbeiten. Sie dürfen Datenverarbeitungen nur zu einem definierten, rechtmäßigen Zweck durchführen. Dabei dürfen nur jene Daten verarbeitet werden, die Sie tatsächlich für diesen Zweck benötigen (Zweckbindung).

Darüber hinaus ist sicherzustellen, dass Sie auch berechtigt sind, die Daten zu verarbeiten, denn für jede Art der Verarbeitung von personenbezogenen Daten ist eine Rechtsgrundlage notwendig (z.B. der Vertrag mit der beschäftigten Person oder dem Kunden, das Gesetz oder auch eine Einwilligung).

Spezielles Augenmerk müssen Sie auf die Rechtmäßigkeit bei der Verarbeitung besonderer Kategorien personenbezogener Daten (z.B.: Gesundheitsdaten, Religions- und Gewerkschaftszugehörigkeit) legen.

Weitergabe der Daten

Auch wenn es einem Unternehmen oft nicht bewusst ist, so werden im betrieblichen Ablauf doch häufig Daten weitergegeben. Sie müssen also auch feststellen, welche personenbezogenen Daten Sie an wen weitergeben. Dabei kann es sich um Weitergabe an andere Unternehmen (z.B.: Dienstleister oder Lieferanten), Behörden (z.B.: ÖGK, Finanzamt) oder andere öffentliche Stellen (z.B.: Lehrlingsstelle) handeln.

Spezielles Augenmerk ist auf Übermittlungen in Länder außerhalb der EU bzw. internationale Organisationen (z.B.: Facebook, Microsoft, Google usw.) zu legen. Nicht immer ist den Unternehmen eine solche internationale Datenübermittlung bewusst.

Internationaler Datenverkehr

Speicherfrist

Personenbezogene Daten sind nur so lange aufzubewahren, wie diese für den eigentlichen Zweck benötigt werden. Entfällt dieser Zweck, so sind die Daten zu löschen, es sei denn, es gibt gesetzliche Aufbewahrungsfristen (z.B.: aus dem Steuerrecht).

Prüfen Sie daher, welche gesetzlichen Aufbewahrungsfristen es für die Daten in Ihrem Unternehmen gibt.

Speicher- und Aufbewahrungspflichten

Erstellung des Verzeichnisses der Verarbeitungstätigkeiten

Sobald Sie die Fragen aus den obigen Punkten beantwortet haben, dokumentieren Sie in einem nächsten Schritt diese Informationen im Verzeichnis der Verarbeitungstätigkeiten.

Verarbeitungsverzeichnis (inkl. Muster und Beispiele)

Auftragsverarbeiter und Verantwortlicher

Es muss außerdem geklärt werden, welche Auftragsverarbeiter Sie heranziehen. Dabei handelt es sich um Externe, die in Ihrem Auftrag personenbezogene Daten verarbeiten. Beispiele dafür sind IT-Dienstleister oder Cloud-Dienste-Anbieter.

Mit allen Auftragsverarbeitern ist eine Vereinbarung zu treffen, die schriftlich oder elektronisch dokumentiert werden muss.

Wer ist Auftragsverarbeiter und was ist dabei zu beachten?

Mustervertrag für eine Auftragsverarbeitung

Sicherung der Verarbeitung

Ein wesentlicher Bestandteil der DSGVO ist die Sicherheit der personenbezogenen Daten. Sie haben für die sichere Speicherung, Verwendung und Weitergabe zu sorgen. Häufig wird von „TOMs" gesprochen, das bedeutet „Technisch-organisatorische Maßnahmen".

Liste mit Datensicherheitsmaßnahmen

Umgang mit Betroffenenrechten

Alle natürlichen Personen, deren Daten Sie verarbeiten, haben aufgrund der DSGVO besondere Rechte – die sogenannten Betroffenenrechte. Zu den betroffenen Personen gehören beispielsweise Ihre Mitarbeiter sowie Ansprechpartner Ihrer Kunden und Lieferanten.

Sie müssen sicherstellen, dass die betroffenen Personen diese Rechte bei Ihnen einfordern können und Sie diese Anfragen innerhalb eines Monats (Verlängerung auf drei Monate in Einzelfällen möglich) beantworten können.

Übersicht Betroffenenrechte

Musterschreiben Auskunftserteilung

Dokumentationsvorlage Betroffenenrechte

Verhalten bei einem Sicherheitsvorfall

Sollte trotz der getroffenen Sicherheitsmaßnahmen eine Datenschutzverletzung auftreten, so gibt es eine Reihe von Maßnahmen, die Sie in einem solchen Fall durchführen müssen. So ist z.B.: innerhalb von 72 Stunden die Datenschutzbehörde von diesem Vorfall zu informieren, und je nach Schwere des Vorfalls auch die betroffenen Personen.

Der richtige Umgang mit Sicherheitsvorfällen und Dokumentenvorlagen für die Meldung muss also gut überlegt und vorbereitet werden.

Laufende Prüfung & Aktualisierung

Aus der DSGVO ergibt sich eine erhebliche Rechenschaftspflicht, im Rahmen derer Sie nachweisen müssen, dass Sie alle Anforderungen ausreichend erfüllt haben. Die erstellten Dokumentationen und Maßnahmen sind dazu laufend auf Aktualität sowie Wirksamkeit zu prüfen und gegebenenfalls zu aktualisieren.

Die nächsten Kapitel gehen im Detail auf die hier genannten Umsetzungsschritte ein und beschreiben praxisnahe Beispiele zur Umsetzung.

Meldung von Datenschutzverletzungen

Muster - Meldung an die Aufsichtsbehörde

Muster Benachrichtigung der betroffenen Person von Datenschutzverletzungen

Erhebung aller Verarbeitungsvorgänge & personenbezogenen Daten

Am Beginn der Umsetzung Ihres Datenschutzprojektes ist zu erheben, welche personenbezogenen Daten Sie überhaupt in Ihrem Unternehmen verarbeiten und warum (d.h. zu welchem Zweck) Sie dies tun.

Überlegen Sie, welche Vorgänge und Abläufe es in Ihrem Unternehmen gibt, bei denen personenbezogene Daten verarbeitet werden. Dabei ist es unerheblich, ob diese Verarbeitung computergestützt oder manuell erfolgt. Grundsätzlich umfasst die DSGVO alle personenbezogenen Daten, die strukturiert bzw. elektronisch aufbewahrt und verarbeitet werden.

Relevante Vorgänge sind beispielsweise die Lohn- und Gehaltsverrechnung, die Führung einer Geburtstagsliste aller Mitarbeiter oder Kunden, eine Kundenkartei, die Erstellung und der Versand von Rechnungen mit Daten einer natürlichen Person oder eine Videoüberwachung (z.B.: der Werkshalle oder des Parkplatzes) sowie die Webseite (mit Website-Analyse-Tool und Cookies) oder Online-Kontaktformulare und Webshops.

In weiterer Folge ist festzustellen, welche konkreten Daten(kategorien) im Rahmen dieser Verarbeitungsvorgänge verarbeitet werden. Beantworten Sie dabei die folgenden Fragen:

- Welche konkreten Daten benötige ich, um beispielsweise den Vertrag mit dem Kunden/Lieferanten oder den Dienstvertrag mit meinen Mitarbeitern zu erfüllen?
- Gibt es möglicherweise gesetzliche Vorschriften, die mich zur Verarbeitung von Daten verpflichten - z.B.: das Steuerrecht?
- Gibt es sonstige gute Gründe, warum ich die Daten benötige?

Möglicherweise werden Sie feststellen, dass Sie Daten speichern und verarbeiten, die für den Zweck eigentlich nicht notwendig sind. Zur Erfüllung des Dienstverhältnisses ist es z.B.: nicht notwendig, dass ein Mitarbeiterbild auf der Webseite des Unternehmens veröffentlicht wird. Gleiches gilt auch für Gruppenfotos gemeinsam mit Kunden oder Lieferanten. Dies ist zur Erbringung der vertraglichen Leistung nicht zwingend notwendig.

Im Sinne der Datenminimierung ist der Datenbestand auf das Notwendigste zu reduzieren, das bedeutet: alle Daten, die Sie nicht unbedingt benötigen, müssen Sie löschen.

Eine weitere Überlegung, die Sie in diesem Zusammenhang anstellen müssen: Wie lange speichern Sie diese Daten? Es ist klar, dass Sie die persönlichen Daten Ihrer Mitarbeiter speichern und verarbeiten, allerdings unterliegen nicht alle Daten der Mitarbeiter den gleichen Aufbewahrungsfristen. Und was passiert, wenn ein Dienstnehmer das Unternehmen verlässt? Müssen Sie die Daten weiter aufbewahren? Dürfen Sie das? Wenn ja, wie lange?

Überlegen Sie auch, in welcher Form Sie die Daten verarbeiten. Handelt es sich dabei um Datenbanken, Software-Programme, Excel-Listen oder analoge Karteien? Die DSGVO unterscheidet zwar bei der Art und Weise der Verarbeitung nicht, im Zuge der Datensicherheit sind aber angemessene Schutzmaßnahmen zu treffen, die unter anderem von der Methode der Verarbeitung abhängig sind.

Bestimmte personenbezogene Daten fallen unter die „besonderen Kategorien personenbezogener Daten" (auch „sensible Daten" genannt, z.B.: die Krankenstandsdaten von beschäftigten Personen). Diese Datensätze dürfen nur eingeschränkt verarbeitet werden und die Rechtmäßigkeit der Verarbeitung dieser muss besonders geprüft werden.

Wichtige Begriffsbestimmungen

Prüfen Sie, in welchen Bereichen Sie sensible Daten verarbeiten. Bei Krankenstandsdaten für sozialversicherungsrechtliche Zwecke in der Personalverwaltung wird das der Fall sein.

Sollte Ihre Analyse der Daten und Verarbeitungsvorgänge ergeben, dass Ihre Verarbeitungen mit einem hohen Risiko für die betroffenen Personen verbunden sind, müssen Sie noch weitere Schritte prüfen.

Brauche ich einen Datenschutzbeauftragten?

Einen Datenschutzbeauftragten brauchen Sie als Verantwortlicher nur unter ganz bestimmten Umtänden. Die Gründe für eine notwendige Benennung sind in den FAQs detailliert erläutert.

Was Sie in jedem Fall bei der Benennung vermeiden müssen, sind Interessenkonflikte zu den anderen beruflichen Tätigkeiten des Beauftragten. So würden beispielsweise die Aufgaben des IT-Leiters mit denen des Datenschutzbeauftragten kollidieren und die Benennung dieser Person ist damit nicht möglich. Natürlich ist auch die Benennung der Geschäftsleitung aus gleichen Gründen nicht möglich.

Ein Spezialfall ergibt sich dadurch auch bei EPUs. Sollten Sie einen Datenschnutzbeauftragten benötigen, so muss diese Rolle an eine externe Person ausgelagert werden.

Beachten Sie bei der Benennung des Beauftragten auch, dass diese Person die notwendigen fachlichen Qualifikationen mitbringt oder aufbaut und darüber hinaus auch die Mittel zur Umsetzung der gesetzlichen Aufgaben erhält.

Achtung: Der Datenschutzbeauftragte ist gegenüber der Datenschutzbehörde nicht Verantwortlicher und haftet somit auch nicht für die Nichteinhaltung der DSGVO-Anforderungen. Die Haftung bleibt weiterhin beim Unternehmen.

FAQ - Wann brauche ich einen Datenschutzbeauftragten

Der Datenschutzbeauftragte

Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung ist in der DSGVO gefordert, wenn es ein potentiell hohes Risiko für die Rechte und Freiheiten der betroffenen Personen gibt. Im ersten Schritt ist also zu definieren, ob ein solches hohes Risiko vorhanden ist.

Dabei ist zu bewerten, ob besondere Kategorien von Daten, Daten zu strafrechtlichen Verurteilungen oder die Überwachung öffentlicher Bereiche umfangreich durchgeführt wird. Ebenso relevant wird die Folgenabschätzung bei einer systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen, wenn die Daten bestimmten Zwecken dienen.

Die Datenschutzbehörde hat zwei Listen mit konkreten Verarbeitungsvorgängen erstellt: Die sog. „black list" führt Verarbeitungsvorgänge, bei denen auf jeden Fall eine Datenschutz-Folgenabschätzung durchzuführen ist, an.
Die „white list" beschreibt jene Verarbeitungsvorgänge, bei denen keine Datenschutz-Folgenabschätzung erforderlich ist. Vor der Durchführung einer Datenschutz-Folgenabschätzung sollten Sie daher auch diese Listen der Datenschutzbehörde prüfen.

In weiterer Folge müssen Sie feststellen, welches Risiko es für die Rechte und Freiheiten der betroffenen Personen gibt. Bei der Bewertung des Risikos sind folgende Aspekte zu berücksichtigen:

- Welche Daten verarbeiten Sie?
- Ist die Datenverarbeitung rechtmäßig? Wie ist diese Rechtmäßigkeit sichergestellt?
- Halten Sie bei der Verarbeitung die Grundsätze der DSGVO ein?
- Welches Risiko besteht hinsichtlich der Vertraulichkeit, Verfügbarkeit oder Integrität?
- Wie hoch ist dieses Risiko?
- Welche Maßnahmen haben Sie zur Minimierung des Risikos bzw. zum Schutz der Daten getroffen?

Die Bewertung des Risikos sollte möglichst objektiv und nachweisbar durchgeführt werden.

Datenschutz-Folgenabschätzung

Ratgeber: Muss ich eine Datenschutz-Folgenabschätzung durchführen?

Ablaufplan Datenschutz-Folgenabschätzung

„white list"

„black list"

Prüfung der Zweckbindung und Rechtmäßigkeit

Die Verarbeitung von personenbezogenen Daten darf nur dann erfolgen, wenn es dafür eine Rechtsgrundlage gibt, auf die Sie sich berufen können:

Mögliche Grundlagen für die rechtmäßige Verarbeitung sind:

- Die Erfüllung eines Vertrages mit der betroffenen Person (z.B.: Dienstvertrag, Kaufvertrag) oder die Anbahnung eines solchen durch Ihren Vertragspartner (Interessenten)
- Die Erfüllung einer rechtlichen Verpflichtung (z.B.: gesetzliche Nachweispflicht; steuerliche Aufbewahrungspflichten, gesetzliche Verpflichtungen zur Aufzeichnung der Arbeitszeiten)
- Der Schutz lebenswichtiger Interessen einer betroffenen Person oder eines Dritten
- Wahrnehmung einer Aufgabe im öffentlichen Interesse oder Ausübung öffentlicher Gewalt
- Zur Wahrung eines berechtigten Interesses Ihres Unternehmens, sofern nicht das Interesse oder Rechte der betroffenen Personen überwiegen
- Die (freiwillig erteilte und verständlich formulierte) Einwilligung, die jedoch jederzeit widerrufen werden kann

Grundsätze und Rechtmäßigkeit der Verarbeitung

Für besondere Kategorien personenbezogener Daten ergeben sich eingeschränkte Rechtsgrundlagen, die gesondert geprüft werden müssen.

Als konkreter Handlungsbedarf sind alle Abläufe und die Verwendung der jeweiligen Daten auf Rechtmäßigkeit zu prüfen. Sie müssen also folgende Fragen beantworten:

- Auf Basis welcher Rechtsgrundlage führe ich die Verarbeitung durch?
- Brauche ich genau die Daten für diesen Verarbeitungszweck zwingend?

Ein einfaches Beispiel ist die Verarbeitung von Daten Ihrer Mitarbeiter zum Zweck der Lohn- und Gehaltsverrechnung. Sie verarbeiten die dazu notwendigen Daten zur Erfüllung des Vertrages mit Ihren Beschäftigten sowie zur Erfüllung einer rechtlichen Verpflichtung (insbes. steuerliche Aufbewahrungspflichten und gesetzliche Aufzeichnungspflichten). Sie verarbeiten darüber hinaus Daten zur Erfüllung der vertraglichen Verpflichtung, indem Sie beispielsweise Zugänge zu betrieblichen Informationen oder Arbeitskleidung zur Verfügung stellen. Die beruflichen Kontaktdaten Ihrer Mitarbeiter (betriebliche E-Mail-Adresse und Telefonnummer) stellen Sie Ihrer gesamten Belegschaft zur Verfügung, was als berechtigtes Interesse angesehen werden kann, da es notwendig ist, diese Daten intern im Unternehmen zu verteilen, um die Arbeitsabläufe und Kontaktaufnahmen zu ermöglichen.

Alle Verarbeitungen, die nicht zwingend zur Erfüllung des Dienstvertrages sowie zur Einhaltung rechtlicher Verpflichtungen erforderlich sind oder im Rahmen des berechtigten Interesses stehen, bedürfen einer Einwilligung. Das bedeutet: Wenn Sie diese Daten verarbeiten möchten, müssen Sie

die betroffenen Personen um Ihre Erlaubnis fragen. Beispiel dafür wäre die Veröffentlichung von Mitarbeiterfotos auf der Webseite oder in sozialen Netzwerken. Bei Einwilligungen sind verschiedene Aspekte zu berücksichtigen, Details dazu finden Sie über den Link.

Einwilligungserklärung

Die gleichen Überlegungen sind für alle Verarbeitungsvorgänge und für alle betroffenen Personengruppen, also auch für Kunden, Lieferanten, Partner und andere notwendig.

Darf ich auch mit der DSGVO noch eine Videoüberwachung betreiben?
Wie bei allen anderen Verarbeitungen ist auch bei der Videoüberwachung die Rechtmäßigkeit sicherzustellen.

Bildverarbeitung/Videoüberwachung

Relevante Aspekte, die bei der Videoüberwachung berücksichtigt werden müssen, sind:

- **Zweck der Überwachung**
  Warum gibt es eine Videoüberwachung?
- **Gelinderes Mittel**
  Ist die Videoüberwachung wirklich notwendig, oder könnte sie auch durch eine andere Maßnahme ersetzt werden?
- Die **Aufbewahrungsfrist** der Videoaufnahmen beträgt in der Regel 72 Stunden.
- Der **Zugriff auf die Aufzeichnungen sollte eingeschränkt** sein und nur jenen Personen zur Verfügung stehen, die diesen benötigen bzw. die in einer etwaigen Einwilligungserklärung oder Betriebsvereinbarung genannt sind.

Gerade bei der Videoüberwachung ist die ausreichende Kennzeichnung (z.B.: durch Schilder oder Aufkleber) sowie weiterführende Datenschutzinformationen (z.B.: auf einer Webseite), auf die vor Ort mittels QR-Code oder dergleichen hingewiesen wird.

Über die Datenschutzpunkte hinaus sollten Sie bei der Videoüberwachung auch etwaige arbeitsrechtliche Aspekte (Betriebsvereinbarung!) beachten. Das gilt auch dann, wenn die Erfassung der Mitarbeiter gar nicht zielgerichtet beabsichtigt ist (z.B.: Überwachung des Eingangs).

Erstellung des Verzeichnisses der Verarbeitungstätigkeiten

Eine wichtige Neuerung in der DSGVO ist das Verzeichnis der Verarbeitungstätigkeiten, welches von jedem Unternehmen geführt werden muss.

Dabei handelt es sich um eine Liste der in Ihrem Unternehmen vorhandenen Verarbeitungsvorgängen. Diese Liste kann um einige zusätzliche, sinnvolle Informationen ergänzt werden. Folgende Aufzählung zeigt die zu dokumentierenden Informationen anhand des Beispiels „Bewerbungsverfahren“:

- **Zweck der Verarbeitung**
  Auswahl geeigneter und qualifizierter zukünftiger Mitarbeiter
- **Beschreibung der Kategorien betroffener Personen**
  Bewerber
- **Beschreibung der Kategorien personenbezogener Daten**
  Kontaktdaten, Lebenslauf, Qualifikationsnachweise, alles was der Bewerber sonst noch schickt
- **Kategorien von Empfängern**
  Personalvermittler
- **Übermittlungen in Drittländer oder an internationale Organisationen**
  keine
- **Fristen für die Löschung**
  6 Monate nach Ende Entscheidung über die Auswahl für die Stelle
- **Technische und Organisatorische Maßnahmen zum Schutz der Daten**
  Eingeschränkter Zugriff auf Bewerberdaten; Vernichtung nach Abschluss der Auswahl

Alle Verarbeitungsvorgänge sind inklusive dieser Punkte zu dokumentieren. Das Verzeichnis kann um zusätzliche Punkte, wie beispielsweise der bereits geprüften Rechtsgrundlage und die Quelle der Daten erweitert werden. Neben den von Ihnen direkt erhobenen Daten könnten z.B.: auch Daten von einer Personalvermittlung bei Ihnen gespeichert werden.

Um das Verzeichnis schnell und einfach zu erstellen, können einige Verarbeitungsvorgänge zusammengefasst werden. Dies kann beispielsweise sinnvoll sein, wenn der Zweck, die Kategorien der personenbezogenen Daten, die Kategorien der betroffenen Personen und die Kategorien der Empfänger gleich sind.

So können Sie beispielsweise die An- und Abmeldung von Mitarbeitern, die Lohn- und Gehaltsverrechnung, die Urlaubs- und Verwaltung der Krankenstände als Personalverwaltung zusammenfassen.

Die DSGVO schreibt nicht vor, in welcher Form oder in welchem Detailgrad das Verzeichnis zu führen ist. So können Sie dies auf Papier, in einem Word-Dokument, als Excel oder in einem Online-Tool erstellen.

Dokumentationspflicht - Verzeichnis von Verarbeitungstätigkeiten

Muster-Verarbeitungsverzeichnis für Verantwortliche

Wichtig im Zusammenhang mit dem Verzeichnis der Verarbeitungstätigkeiten ist, dass dieses im Anlassfall, wenn sich Verarbeitungen erweitern oder verändern, auf Aktualität geprüft und ggf. ergänzt bzw. korrigiert wird. Eine regelmäßige Prüfung wird also dringend empfohlen.

Bei der Erstellung kann es auch hilfreich sein, die bis 2018 im Datenverarbeitungsregister (DVR) gemeldeten Verarbeitungen als Basis heranzuziehen. Informationen zu den Datenkategorien und Empfängern finden Sie zudem in der (nicht mehr gültigen) Standard- und Musterverordnung.

Achtung: Auch als Auftragsverarbeiter müssen Sie ein Verzeichnis der Verarbeitungstätigkeiten für die Tätigkeiten im Auftrag des jeweiligen Verantwortlichen (= Ihr Kunde) führen.

Standard- und Musterverordnung

Muster-Verarbeitungsverzeichnis für Autragsverarbeiter

Auftragsverarbeiter und Verantwortlicher

Grundsätzlich können mehrere Stellen in die Datenverarbeitung Ihres Unternehmens eingebunden sein. Daher unterscheidet die DSGVO zwischen drei wesentlichen Parteien bei der Verarbeitung personenbezogener Daten.

- **Verantwortlicher**
  Unternehmen welches die Daten einer natürlichen Person verarbeitet und über die Mittel und den Zweck der Verarbeitung selbst entscheidet. Zum Beispiel verarbeiten Sie als Unternehmen die Daten Ihrer Mitarbeiter sowie Kunden und Lieferanten und sind somit Verantwortlicher.
- **Betroffene Personen**
  Natürliche Personen, deren Daten von einem Verantwortlichen verarbeitet werden. Im konkreten Beispiel also Ihre Mitarbeiter, Kunden und Lieferanten.
- **Auftragsverarbeiter**
  Eine natürliche oder juristische Person, Behörde oder öffentliche Stelle, die personenbezogene Daten einer betroffenen Person im Auftrag eines Verantwortlichen verarbeitet. Dazu gehören zum Beispiel IT-Dienstleister.

Zur Erfüllung der DSGVO sind von Ihnen alle Auftragsverarbeiter, die Daten in Ihrem Auftrag verarbeiten, zu identifizieren. Dabei kann es sich um IT-Dienstleister, Hosting-Provider, Werbeagenturen oder Anbieter spezifischer Cloud-Lösungen handeln, wenn von diesen in Ihrem Auftrag personenbezogene Daten verarbeitet werden.

Mit allen diesen Auftragsverarbeitern ist eine Auftragsverarbeitungsvereinbarung abzuschließen. Dabei handelt es sich um eine Vereinbarung, die den Auftragsverarbeiter zur Einhaltung der gesetzlichen Anforderungen verpflichtet. Diese Auftragsverarbeitervereinbarung ist schriftlich (oder in elektronisch dokumentierter Form) abzuschließen.

Achtung: Auch wenn Sie bestimmte Verarbeitungsvorgänge an einen Auftragsverarbeiter auslagern, bleiben Sie der Verantwortliche, und müssen sich z.B. um die Rechtsgrundlage der Verarbeitung selbst kümmern.

Verantwortlicher und Auftragsverarbeiter

Mustervertrag für die Auftragsverarbeitung

Sicherheit der Verarbeitung

Als Verantwortlicher sowie als Auftragsverarbeiter sind Sie verpflichtet, ausreichende, dem Stand der Technik entsprechende Sicherheitsmaßnahmen zum Schutz der von Ihnen verarbeiteten personenbezogenen Daten zu ergreifen („TOMs"). Die DSGVO verweist dabei auf die Angemessenheit der Maßnahmen vor allem im Hinblick auf das Risiko für die Rechte und Freiheiten der betroffenen Personen.

Beim Schutz der Daten geht es in erster Linie um den Schutz der **Vertraulichkeit, Integrität** und der **Verfügbarkeit** der Daten. Es ist also zu regeln, wie die personenbezogenen Daten vor unbefugtem Zugriff, Verlust und Manipulation geschützt werden.

Zu diesem Zweck gibt es eine nahezu endlose Reihe von möglichen Maßnahmen, die ergriffen werden können:

- Aufbewahrung von personenbezogenen Daten in pseudonymisierter Form
- Verschlüsselung, Speicherung und Weitergabe von personenbezogenen Daten
- Anfertigung von verschlüsselten Backups und Aufbewahrung an unterschiedlichen Orten
- Verwendung sicherer Passwörter, um den Zugriff auf IT-Systeme zu verhindern
- Verwendung von Schreddern oder verplombten Containern für die Entsorgung von Informationen und Daten
- Versperren von Büros und Dokumenten, wenn diese unbeaufsichtigt zurückgelassen werden („Clear-Desk")
- Einsatz und sichere Konfiguration einer Firewall
- Einsatz eines Anti-Viren-Schutzes

Diese Liste stellt nur eine kurze Übersicht über mögliche Maßnahmen dar und stellt keinen Anspruch auf Vollständigkeit. Zur Auswahl geeigneter Schutzmaßnahmen, können Sie sich an die verschiedenen Online-Ratgeber oder an die IT-Security Experts Group der WKO wenden.

Auch das Thema Weitergabe von Daten via E-Mail sollte beim Thema Datensicherheit berücksichtigt werden. Die Übermittlung von sensiblen Daten über unverschlüsselte E-Mails ist nicht sicher und nicht Stand der Technik. Wird ein E-Mail mit personenbezogenen Daten (z.B.: monatliche Lohnverrechnungsdaten an den Lohnverrechner) abgefangen, stellt dies einen unbefugten Zugriff auf Daten und somit eine Datenschutzverletzung dar.

Wichtig ist bei den getroffenen Sicherheitsmaßnahmen, diese auch zu dokumentieren. Dies muss zum Beispiel direkt im Verzeichnis der Verarbeitungstätigkeiten oder kann in einem Informationssicherheitshandbuch erfolgen. Eine umfassende Basis für ein solches Handbuch und mögliche Maßnahmen finden Sie im IT-Sicherheitshandbuch für kleine und mittlere Unternehmen der WKO.

Online-Ratgeber „it-safe"

IT-Safe (mit Checklisten, Broschüren, Ratgebern)

IT-Security Experts Group

Mustervertrag für die Auftragsverarbeitung mit TOMs im Anhang

IT-Sicherheits-Handbuch für KMU

Umgang mit Betroffenenrechten

Betroffene Personen verfügen gemäß DSGVO über definierte Rechte, die sie unter den gesetzlichen Bedingungen geltend machen können.

- **Recht auf Auskunft**
  Jede Person darf von Ihnen Auskunft darüber verlangen, ob bzw. welche personenbezogenen Daten Sie über sie gespeichert haben und was Sie damit machen.
- **Recht auf Berichtigung**
  Eine betroffene Person kann die Berichtigung bzw. Ergänzung der über sie verarbeitenden Daten verlangen.
- **Recht auf Löschung (Recht auf Vergessenwerden)**
  Betroffene Personen haben das Recht auf Löschung der sie betreffenden personenbezogenen Daten, vorausgesetzt es gibt keine zweckgebundene Notwendigkeit, die Daten weiter zu verarbeiten. So dürfen Sie beispielsweise keine personenbezogenen Daten löschen, die Sie aus gesetzlichen Gründen aufbewahren müssen. Ebenfalls von der Löschung ausgenommen sind personenbezogene Daten, die Sie zur Abwehr von drohenden Ansprüchen dritter Personen aufbewahren müssen (z.B.: Schadenersatzforderungen).
- **Recht auf Einschränkung**
  Eine Einschränkung kann gefordert werden, um die personenbezogenen Daten von der Verarbeitung auszunehmen, ohne jedoch eine Löschung zu verlangen.
- **Recht auf Datenübertragbarkeit**
  Im Zuge der Datenübertragbarkeit kann eine betroffene Person die Übermittlung der von ihr bereitgestellten personenbezogenen Daten an sich oder einen anderen Verantwortlichen verlangen, sofern die Verarbeitung auf einem Vertrag oder einer Einwilligung beruht. Die Übermittlung muss dabei in einem elektronischen, maschinenlesbaren Format (z.B.: CSV, Excel) erfolgen.
- **Widerspruchsrecht**
  Eine betroffene Person kann der Verarbeitung ihrer Daten widersprechen. Der Widerspruch löst bei Direktmarketing eine Verpflichtung zur Unterlassung der Datenverwendung sowie bei anderen Gründen eine Abwägung zwischen Interessen aus.

Alle diese Rechte kennen auch Ausnahmen, z.B.: wenn eine Auskunft die Rechtsposition des Verantwortlichen gefährden würde oder ein Löschantrag mit einer gesetzlichen Verpflichtung zur Aufbewahrung kollidiert.

Betroffenenrechte

Zum Recht auf Löschung ist anzumerken, dass im Sinne der Datenminimierung und -sparsamkeit, generell alle personenbezogenen Daten zu löschen sind, sobald es für diese keinen rechtmäßigen Verarbeitungszweck (mehr) gibt, d.h. die Daten nicht mehr benötigt werden (z.B.: Bewerberdaten = sechs Monate nach Ende des Bewerbungsprozesses; Daten aus einer Videoüberwachung = 72 Stunden).

Sie sollten sich daher firmeninterne Regelungen überlegen, wie Sie mit solchen Betroffenenanträgen umgehen. Dabei sollten eindeutige Zuständigkeiten und Verantwortlichkeiten festgelegt werden, die auch der gesamten Belegschaft bekannt sind. Denken Sie bei der Erstellung einer solchen Regelung auch an krankheits- bzw. urlaubsbedingte Abwesenheiten, denn für die Bearbeitung eines Ansuchens haben Sie einen Monat Zeit. Es ist notwendig, dass diejenigen Personen, die mit Daten im Unternehmen umgehen, wissen, wer bei einer Anfrage zuständig ist, um nicht unnötig Zeit bei der Beantwortung zu verlieren.

Wurden Daten auf Antrag einer betroffenen Person berichtigt, gelöscht oder eingeschränkt, hat der Verantwortliche jeden anderen, an den die Daten weitergegeben wurden, über die Geltendmachung dieser Ansprüche in Kenntnis zu setzen (**Mitteilungspflicht**).

Wie gehe ich mit Betroffenenanträgen um?

Es gibt keine Vorschrift, in welcher Form jemand von Ihnen Auskunft über seine Daten oder die Löschung ebendieser verlangen kann. Sie müssen damit rechnen, dass Sie schriftlich oder per E-Mail, am Telefon oder in einem persönlichen Gespräch ein solches Ansuchen bekommen.

Was Sie in jedem Fall bei der Benennung vermeiden müssen, sind Interessenkonflikte zu den anderen beruflichen Tätigkeiten des Beauftragten. So würden beispielsweise die Aufgaben des IT-Leiters mit denen des Datenschutzbeauftragten kollidieren und die Benennung dieser Person ist damit nicht möglich. Natürlich ist auch die Benennung der Geschäftsleitung aus gleichen Gründen nicht möglich.

Ein Spezialfall ergibt sich dadurch auch bei EPUs. Sollten Sie einen Datenschnutzbeauftragten benötigen, so muss diese Rolle an eine externe Person ausgelagert werden.

Beachten Sie bei der Benennung des Beauftragten auch, dass diese Person die notwendigen fachlichen Qualifikationen mitbringt oder aufbaut und darüber hinaus auch die Mittel zur Umsetzung der gesetzlichen Aufgaben erhält.

Achtung: Der Datenschutzbeauftragte ist gegenüber der Datenschutzbehörde nicht Verantwortlicher und haftet somit auch nicht für die Nichteinhaltung der DSGVO-Anforderungen. Die Haftung bleibt weiterhin beim Unternehmen.

Feststellung der Identität

Wichtigster Punkt zu Beginn: Überzeugen Sie sich von der Identität des Anfragers, da jede Person natürlich nur ein Auskunftsrecht bezüglich seiner eigenen Daten hat. Nichts wäre unangenehmer, als einer unberechtigten dritten Person die falsche gespeicherte Information weiterzugeben.

- Bei telefonischen Ansuchen: Weisen Sie den Anrufer darauf hin, dass - auch zu seinem eigenen Schutz - die Identität geprüft werden muss. Ersuchen Sie ihn um ein E-Mail bzw. ein persönliches Gespräch, auch Videotelefonie kommt in Betracht.
- Bei E-Mail Ansuchen: Wenn Sie keine Zweifel bezüglich der Identität des Anfragers haben, können Sie eine E-Mail zur weiteren Bearbeitung des Ansuchens akzeptieren. Ideal wäre es, wenn dieses E-Mail digital signiert wäre. Falls Sie Zweifel an der Identität des Anfragers oder der Echtheit der E-Mail-Adresse haben, verlangen Sie bitte eine genaue Identifikation wie am Telefon.
- Bei einem persönlichen Gespräch: Falls Sie die anfragende Person nicht kennen, ersuchen Sie um einen Ausweis.

Dokumentieren Sie, wie Sie die Identität festgestellt haben.

Dokumentationsvorlage Betroffenenrechte

Bearbeitung der Anfrage

Auskunft

Auf Anfrage müssen Sie die Person darüber informieren, welche Daten Sie über die betroffene Person verarbeiten und warum Sie dies tun.

Auskunftspflicht des Verantwortlichen

Im Idealfall haben Sie Ihr Verarbeitungsverzeichnis so strukturiert, dass Sie sehr schnell die benötigten Informationen zusammenstellen können.

Die wichtigsten sind:

- welche Daten werden verarbeitet
- für welchen Zweck
- wie lange werden sie gespeichert
- ob, und wenn ja, an wen diese Daten weitergegeben werden.

Sie müssen nun **alle** Informationen über die anfragende Person zusammenstellen. Dabei ist anzuraten, hier einen genauen Prozess in Ihrem Unternehmen festzulegen und den auch strikt einzuhalten. Sollten große Mengen an Informationen über die betroffene Person vorliegen, können Sie eine Präzisierung der Anfrage verlangen. Falls Sie sehr umfangreiche Datenmengen haben und Ihnen die betroffene Person unbekannt ist, könnten Sie sich nach deren Bezug zu Ihrem Unternehmen erkundigen (z.B.: Kunde, Lieferant, Anbieter, Messebesucher, Veranstaltungsteilnehmer, ehemaliger Mitarbeiter etc.).

Idealerweise haben Sie im Verzeichnis der Verarbeitungstätigkeiten auch dokumentiert, wo die personenbezogenen Daten gespeichert sind (z.B.: Excel-Liste, Kundendatenbank oä). Kopieren Sie die Daten aus den entsprechenden Speicherorten und übermitteln Sie diese an die betroffene Person. Gegebenenfalls sollte dabei auf Verschlüsselung gesetzt werden.

Berichtigung, Löschung, Einschränkung

Werden Sie zur Berichtigung oder Löschung der Daten bzw. zur Einschränkung der Datenverarbeitung aufgefordert, so führen Sie dies durch.

Pflicht zur Berichtigung, Löschung und Einschränkung

Werden Sie beispielsweise informiert, dass sich der Name der Person geändert hat, so passen Sie diesen nach erfolgreicher Identifikation an.

Im Falle einer Löschung sind die Daten aus Ihren Datenbanken, Netzlaufwerken und E-Mails zu löschen. Backups können nachrangig behandelt werden. Im Falle einer Datenwiederherstellung aus einem Backup ist aber sicherzustellen, dass bereits gelöschte Daten wieder entfernt werden.

Dokumentieren Sie die durchgeführte Handlung.

Widerspruch

Verarbeiten Sie Daten auf Basis eines berechtigten Interesses, steht den betroffenen Personen in ungewöhnlichen Sondersituationen grundsätzlich das Recht auf Widerspruch zu und Sie müssen die Verarbeitung der personenbezogenen Daten einstellen.

Widerspruch

Die Umsetzung des Widerspruchs ist zu dokumentieren.

Datenübertragbarkeit

Auf Wunsch sind die personenbezogenen Daten einer betroffenen Person, welche diese bereitgestellt hat, dieser zur Verfügung zu stellen. Dies hat in einem maschinenlesbaren Format (z.B.: CSV, Excel) zu erfolgen. Von diesem Recht ist auch die Übermittlung an einen anderen Verantwortlichen umfasst.

Datenübertragbarkeit

Die Übertragung ist zu dokumentieren.

Übermittlung der Information

In jedem Fall müssen Sie die betroffene Person über die durchgeführten Schritte informieren bzw. im Falle des Auskunftsrechtes die angeforderten Daten übermitteln.

Musterschreiben zur Auskunftserteilung

Bei der Übermittlung der Informationen sind folgende Punkte zu beachten:

- Die Übermittlung erfolgt in der Regel schriftlich, nur auf Wunsch des Anfragers kann sie auch mündlich erteilt werden.
- Sie dürfen natürlich nur der betroffenen Person Auskunft geben, also keine Übermittlung an allgemeine Unternehmensadressen.
  Falls Sie kritische Daten übermitteln, verwenden Sie zusätzliche Sicherheitsmaßnahmen (z.B.: E-Mail Verschlüsselung etc.)
- Die Auskunft muss in einfacher und klar verständlicher Sprache erfolgen. Eventuell müssen Sie vielleicht Ihre internen Datenbezeichnungen oder Verarbeitungsvorgänge bei der Beauskunftung an den Betroffenen noch überarbeiten.
- Sie müssen den Anfrager im Rahmen der Auskunft auch über seine weiterführenden Rechte wie Richtigstellung oder Löschung seiner Daten, Untersagen einer weiteren Verarbeitung sowie das Beschwerderecht bei der Aufsichtsbehörde informieren.
- Wenn Sie keine Daten über den Anfragenden gespeichert haben, schicken Sie ihm eine „Leermeldung", denn jede betroffene Person hat ein Recht, dass ihr bestätigt wird, ob ein Verantwortlicher überhaupt ihre personenbezogenen Daten verarbeitet.
- Wird der betroffenen Person die Geltendmachung eines Rechtes versagt, so ist ihr dies inklusive einer Begründung ebenso mitzuteilen.

Die Rückmeldung muss in der Regel innerhalb eines Monats ab Anfrage erfolgen. Protokollieren Sie den gesamten Vorgang der Anfragebeantwortung auch für Ihre Unterlagen. Dies sollte Aufgabe einer zentralen verantwortlichen Person für die Betroffenenrechte sein.

Dokumentationsvorlage Betroffenenrechte

Informationspflicht

Ein Spezialfall der Betroffenenrechte sind die Informationspflichten. Im Zuge der Erhebung personenbezogener Daten müssen Sie die betroffenen Personen über die Verarbeitung detailliert informieren. Es ist unerheblich, ob Sie die Daten direkt bei den betroffenen Personen oder über Dritte erheben.

Informationspflichten

Sie müssen also die Informationspflicht mit wenigen Ausnahmen und unabhängig von der Rechtsgrundlage der Verarbeitung erfüllen.

Online Ratgeber „Informationspflichten"

Am einfachsten kann der Informationspflicht in der Regel direkt im Zuge der Erhebung nachgekommen werden. Betreiben Sie beispielsweise einen Online-Shop, so informieren Sie die Personen im Zuge der Registrierung bzw. Bestellung ohne Konto über die Verwendung der Daten.

Bei **neuen Mitarbeitern** wird häufig ein **Personalbogen** ausgefüllt, um alle relevanten Daten abzufragen. Weisen Sie die Mitarbeiter im Zuge der Ausfüllung bereits auf die geplante Verarbeitung der Daten hin, indem Sie einen kurzen Passus zum Datenschutz ergänzen.

Nehmen Sie eine Klausel zum Datenschutz in die Dienst- oder andere Verträge mit auf und weisen Sie Mitarbeiter sowie Kunden und Lieferanten auf die den Zweck der Datenverwendung und die Betroffenenrechte hin. Dabei handelt es sich um eine Information, nicht um eine Einwilligung.

Bei der Informationspflicht gilt grundsätzlich:
je mehr Sie informieren, desto besser.

Informieren Sie Ihre betroffenen Personen daher über unterschiedliche Kommunikationswege, wie beispielsweise:

- Datenschutzerklärung auf der Webseite
- Datenschutzhinweise bei Online- und anderen Formularen
- Hinweis auf den Verarbeitungszweck auf Einwilligungserklärungen
- Datenschutzhinweise & -erklärungen in mobilen Apps
- Aushängen auf Messeständen und in Verkaufslokalen bzw. -geschäften

Es ist zulässig, dass Sie einen allgemeinen Hinweis im Rahmen der Korrespondenz (z.B.: E-Mail oder Schriftstücke) verwenden, in dem Sie auf die Verwendung der personenbezogenen Daten hinweisen, und auf eine Datenschutzerklärung auf der Webseite verweisen, wenn Sie annehmen können, dass die betroffenen Personen in der Lage sind, sich einfach und ohne große Mühen Kenntnis dieser Information zu verschaffen.

Bedenken Sie immer den Weg, auf dem der Kunde zu Ihnen kommt, und informieren Sie beim ersten Kontakt (z.B.: Aushang im Ladenlokal, Hinweis bei der Kassa, Hinweis beim Kontakt-Formular oder Online-Shop, Hinweistafel bei der Videoüberwachung).

Nicht immer ist es möglich, alle geforderten Informationen so darzustellen, dass sie der Betroffene auch rasch erfassen kann, so etwa ganz typisch bei Videoüberwachungen. Es ist zulässig, die Informationen auf mehreren Ebenen darzustellen, z.B.: Informationen zu den Verarbeitungszwecken, die Identität des Verantwortlichen, die Existenz der Rechte der betroffenen Person ergänzt um Informationen über die größten Auswirkungen der Verarbeitung und jene Verarbeitungen, mit denen die betroffene Person nicht rechnet, auf einem Hinweisschild und mit QR-Code auf eine Internetadresse mit den weiteren Informationen zu verweisen.

Tipp: Vermeiden Sie jeden Anschein, dass der Betroffene seine Zustimmung zur Datenschutzerklärung erteilt. Daher sollten Datenschutzerklärungen auf Papier keinesfalls unterschrieben oder (sowohl auf Papier als auch mittels Häkchen im Internet) „akzeptiert" werden. Hintergrund hierfür ist die Rechtsprechung des Obersten Gerichtshofs zu Allgemeinen Geschäftsbedingungen.

Verhalten bei einem Sicherheitsvorfall

Der Schutz der personenbezogenen Daten ist ein wesentlicher Bestandteil der DSGVO. Zur Datensicherheit gehört auch der Umgang mit Sicherheitsvorfällen - Situationen in denen der Schutz personenbezogener Daten verletzt wird.

Datenschutzverletzungen werden als „Data Breach" bezeichnet und treten unter anderem bei erfolgreichen Hacking-Angriffen auf Ihr Netzwerk oder Ihre Datenbanken, unbeabsichtigter Veröffentlichung von Daten aber auch beim Verlust eines Datenträgers (z.B.: Smartpone, Notebook oder USB-Stick) ein, wenn personenbezogene Daten betroffen sind.

Datenschutzverletzungen sind im Falle eines möglichen Risikos für die Rechte und Freiheiten natürlicher Personen innerhalb von 72 Stunden an die Datenschutzbehörde zu melden.

Verursacht die Datenschutzverletzung ein voraussichtlich hohes Risiko für die Rechte und Freiheiten für die betroffenen Personen, müssen Sie auch diese über die Datenschutzverletzung informieren. Dies hat unverzüglich zu erfolgen.

Die Herausforderung bei der Meldung sowohl an die Datenschutzbehörde als auch an die betroffenen Personen ist die Einschätzung des Risikos einer Datenschutzverletzung. Gelingt es beispielsweise einem Angreifer, sich Zugang zu den Passwörtern Ihrer Mitarbeiter zu verschaffen und berücksichtigt man dabei, dass die meisten Menschen in der Regel Passwörter mehrfach verwenden, so kann man hier bereits ein hohes Risiko sehen. Der Grund dafür ist ganz einfach: die unbefugte Person könne mit den Zugangsdaten auch Zugriff auf die privaten E-Mail-Konten, Online-Shopping-Portale und viele andere Plattformen erlangen.

Meldung von Datenschutzverletzungen (Data Breach Notification)

Muster - Meldung an die Aufsichtsbehörde

Muster - Benachrichtigung der betroffenen Personen

Laufende Prüfung & Aktualisierung

Einer der Grundsätze der DSGVO verpflichtet den Verantwortlichen zur nachweislichen Einhaltung der Anforderungen.

Konkret bedeutet dies, dass Sie die Wirksamkeit der von Ihnen getroffenen Maßnahmen regelmäßig kontrollieren und nachweisen müssen. Aus diesem Grund sollte ein regelmäßiger Kontrollprozess eingeführt werden.

So sollte zumindest **einmal pro Jahr** geprüft werden, ob Ihre **Datenschutzmaßnahmen und -dokumentationen** noch aktuell sind. Dabei sollten unter anderem folgende Punkte geprüft werden:

- Ist das Verzeichnis der Verarbeitungstätigkeiten noch aktuell?
- Entsprechen Ihre Maßnahmen zur Datensicherheit noch dem Stand der Technik?
- Sind die etablierten Datensicherheitsmaßnahmen wirksam?
- Funktioniert der Prozess zur Beantwortung von Betroffenenanträgen?
- Wurden bisherige Betroffenenansuchen dokumentiert?
- Gab es Datenschutzvorfälle / „Data Breaches"?

Ergänzend sollten auch Ihre Mitarbeiter zumindest jährlich im Umgang mit personenbezogenen Daten sensibilisiert werden.

Rechenschaftspflicht

Die DSGVO fordert nicht nur die Einhaltung der Anforderungen, sondern auch den Nachweis darüber. So müssen Sie die Wirksamkeit Ihrer Datenschutzmaßnahmen und die konforme Verarbeitung auch nachweisen können. Das ist nur durch Dokumentation der relevanten Maßnahmen und Tätigkeiten möglich.

So sollten Sie zumindest eine Dokumentation über folgende Themenschwerpunkte haben:

- Verzeichnis der Verarbeitungstätigkeiten
- Arbeitsschritte pro eingegangenem Betroffenenbegehren
- Vorhandene Sicherheitsmaßnahmen zum Schutz der personenbezogenen Daten
- Schriftliche Vereinbarung mit allen Auftragsverarbeitern

Generell ist empfohlen, dass alle Datenschutzmaßnahmen und Tätigkeiten rund um das Thema Datenschutz dokumentiert werden, sofern Ihnen darauf eine Nachweispflicht entstehen kann.

Weiterführende Informationen

wko.at/datenschutz

Diese Themenseite führt Sie durch alle Grundlagen der DSGVO

wko.at/datenschutzservice

Auf dieser Seite finden Sie alle Serviceangebote der Wirtschaftskammer wie Vertragsmuster, Online-Ratgeber, geförderte Beratungs- und Schulungsangebote, Webinare und Vieles mehr. Ebenso finden Sie hier die Kontaktdaten der Experten in Ihrer Wirtschaftskammer.

it-safe.at

Praxisnahe Informationen und Tools der Bundessparte „Information & Consulting" zur IT-Sicherheit, die besonders auf die Bedürfnisse kleiner Unternehmen abgestimmt sind.

Impressum

Medieninhaber und Herausgeber
Wirtschaftskammer Österreich, Wiedner Hauptstraße 63, 1045 Wien
wko.at

Autoren
Mag. Viktoria Haidinger, LL.M, Wirtschaftskammer Österreich

Auf Grundlage der 1. Auflage von:
Erik Rusek, MSc zert. DSBA (TÜV)
www.vace-sec.at

Dr. Thomas Schweiger, LL.M., CIPP/E, zert. DSBA (DATB, TÜV)
www.dataprotect.at

Produktion, Gestaltung, Infografiken
Inhouse GmbH der Wirtschaftskammern Österreichs

September 2023

wko.at/datenschutz