DSGVO leicht gemacht
für Event-ManagerInnen & VeranstalterInnen

1. Datenschutz-Grundverordnung

2. Begriffe, die Sie kennen sollten

3. Pflichten bei der Datenverarbeitung

4. Informationspflichten

5. Betroffenenrechte

6. Rechtsdurchsetzung und Strafen

7. Maßnahmen

1. Datenschutz-Grundverordnung

Die „Datenschutz-Grundverordnung“ (DSGVO, VO 2016/679) der Europäischen Union gilt ab 25. Mai 2018. Sie bringt auch für Österreich grundlegende und verbindliche Neuerungen, insbesondere im Zusammenhang mit der Verarbeitung personenbezogener Daten und deren Dokumentation. Die DSGVO erweitert die Rechte der Betroffenen und die Pflichten der Verantwortlichen und sieht viel strengere Strafen als nach der bisherigen Rechtslage vor. Ergänzt wird die DSGVO in Österreich durch das Datenschutzgesetz (DSG), das mit dem Datenschutz-Anpassungs-Gesetz und dem Datenschutz-Deregulierungs-Gesetz und weiteren gesetzlichen Regelungen an die DSGVO angepasst wird.

Ab 25. Mai 2018 müssen alle Änderungen im Hinblick auf die neue Rechtslage vollzogen sein. Jedes Unternehmen, das in irgendeiner Weise personenbezogene Daten verarbeitet (z.B. eine Kundendatei führt, Rechnungen ausstellt, Lieferantendaten speichert), ist betroffen. Damit kommen wesentliche Neuerungen auf Unternehmen zu.

Die nachstehenden Informationen geben in einem ersten Teil einen Einblick in die wichtigsten Neuerungen des Datenschutzrechts und beantworten oft gestellte Fragen. In einem zweiten Teil werden Maßnahmen erläutert, die von jedem Unternehmen zu setzen sind. Entsprechende Musterdokumente für die Erfüllung der wichtigsten rechtlichen Verpflichtungen wurden branchenspezifisch etwa für Betriebe der Tourismus- und Freizeitwirtschaft erstellt und sind unter wko.at/bstf/datenschutzimtourismus abrufbar. Die Dokumente sind jedenfalls noch an die Besonderheiten Ihres Unternehmens anzupassen.

Weiterführende allgemeine Informationen und Musterdokumente finden Sie auch unter wko.at/datenschutz.

Bei den in dieser Broschüre verwendeten personenbezogenen Bezeichnungen gilt die jeweils gewählte Form immer für beide Geschlechter.

Verarbeitung personenbezogener Daten

sensible Daten bzw. besondere Kategorien personenbezogener Daten

Verantwortlichkeit und Auftragsverarbeitung

2. Begriffe, die Sie ab sofort kennen sollten!

2.1. Die „Verarbeitung personenbezogener Daten“

Was sind personenbezogene Daten?

Personenbezogen sind Daten immer dann, wenn sie sich auf eine Person – den sog „Betroffenen“ – beziehen, die identifiziert oder auch nur identifizierbar ist. Nach österreichischer Rechtslage kommen als Betroffene nur natürliche Personen in Betracht, nicht jedoch juristische Personen. Außer bei den Betroffenenrechten hat dies jedoch wenig praktische Bedeutung.

Identifizierbarkeit liegt immer dann vor, wenn eine Person direkt oder indirekt, insbesondere mittels

- Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder
- zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind,

identifiziert werden kann.

Beispiele: Name, Adresse, Geburtsdatum, Bankdaten, Gesundheitsdaten, etc.

Die DSGVO gilt nicht für anonyme Informationen oder Daten, die so anonymisiert worden sind, dass eine betroffene Person nicht mehr identifiziert werden kann. Die DSGVO betrifft daher nicht die Verarbeitung anonymer Daten für statistische Zwecke oder Forschungszwecke.

Die DSGVO findet

- nicht nur Anwendung auf die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten,
- sondern auch auf die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem verwaltet werden.

Beispiele: Agenturinterne Kundendatei (elektronisch, aber auch in Papierform), vom Kunden beigestellte Listen mit Daten eingeladener Personen, Crewlisten mit Handynummern, Kontaktdaten von (Sub-)Lieferanten, die für den Kunden tätig sind

Häufige Fragen

Gelten Kontaktdaten der Geschäftspartner (z.B. Durchwahl, Handynummer oder Email-Adresse des Sachbearbeiters oder des Angestellten) auch als personenbezogene Daten?

Ja.

Gilt die Datenschutzgrundverordnung nur für digitale Daten oder auch für analoge (z.B. händisch beschriebene Kundenkarten)?

Ein Dateisystem ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind. Das unabhängig davon, ob diese Sammlung

zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird, z.B. alphabetisch geführte Ablagen.

Inwiefern betrifft der Datenschutz Teilnehmerlisten von Firmenveranstaltungen, Mitarbeiter-Events oder Hochzeiten?

Für solche Listen werden personenbezogene Daten natürlicher Personen verarbeitet. Diese Datenanwendung unterliegt daher der DSGVO, unabhängig davon, ob die Listen elektronisch oder auf Papier als Dateisystem geführt werden. Für die Verarbeitung dieser Daten besteht in aller Regel eine vertragliche Grundlage (siehe auch Punkt 3.2. Rechtmäßigkeit der Verarbeitung).

Komme ich mit einem Betrieb nach Beginn dieser Verordnung z.B. aus einem Beurteilungsportal wie Holidaycheck heraus? Bis jetzt war das ja nichtmöglich.

Nein. Das Interesse der Konsumenten und des Portals an der Bewertung einer Dienstleistung wird in der Regel ein Geheimhaltungsinteresse des Betriebs überwiegen. Gegen eine sachlich nicht gerechtfertigte Kritik können Sie sich gegebenen Falls wegen Kreditschädigung oder übler Nachrede wehren.

Wenn meine Website bei jimdo liegt: Muss ich selbst auch noch Informationen zum Datenschutz formulieren, obwohl Jimdo eine Datenschutzerklärung verwendet?

Jimdo stellt nur die technische Infrastruktur für Ihren Webauftritt bereit. Inhaltlich sind Sie selbst für die Einhaltung des Datenschutzrechts verantwortlich. Somit müssen Sie auch selbst auf Ihrer Website und darüber hinaus eine Datenschutzerklärung zur Verfügung stellen, die der DSGVO und den von Ihnen im Einzelfall zu verantwortenden Datenverarbeitungen entspricht.

Kann ich Fotos und Videos, die bei Events von Anwesenden gemacht werden, auf die Event-Site stellen, auf der sich der Kunde vorher angemeldet hat?

Auch Bildmaterial von Personen ist vom Schutzbereich der DSGVO erfasst. Wenn eine Person nicht erkennbar ist, liegt aber im Normalfall kein Personenbezug vor. Bedenken Sie, dass Fotos und Videos sehr unvorteilhaft sein können und sogar Persönlichkeitsrechte der Abgebildeten verletzen können.

Wir empfehlen Ihnen, schon im Zuge der Anmeldung zum Event vom Kunden Einwilligungen zu klar definierten Datenverarbeitungen und –veröffentlichungen einzuholen. Dies gilt auch für Veröffentlichungen in Social Media. Außerdem sollten Sie auch direkt beim Einlass zum Event deutlich sichtbar darüber aufklären, dass von dem Event zum Zweck der Dokumentation und der Veröffentlichung auf der Event-Site Bildaufnahmen gemacht werden und jeder Betroffene durch die Teilnahme einwilligt, dass diese Aufnahmen veröffentlicht werden dürfen.

Auch wenn Sie nicht selbst der Veranstalter des Events sind, sondern dieses „nur“ für den Veranstalter organisieren, müssen Sie sich DSGVO konform verhalten. Also z.B. auch dann, wenn Sie im Auftrag des Veranstalters über das Event in Medienveröffentlichungen und Newslettern berichten und dafür Daten der Eventteilnehmer verarbeiten.

Sind Daten von „Freunden der Agentur“ von der DSGVO betroffen?

Ja.

Dürfen meine Mitarbeiter auf dem Firmenhandy weiterhin Facebook, Instagram, Whatsapp & Co verwenden?

Davon raten wir derzeit ab. Wenn Sie Ihre eigenen Daten preisgeben wollen, ist das Ihre freie Entscheidung. Mitarbeiter- und Kundendaten sollten allerdings nicht ohne deren Einwilligung veröffentlicht werden.

Die genannten Plattformen und die damit bereit gestellten Dienste sind sehr populär. Die eingesetzten Praktiken sind aber oft nicht leicht zu durchschauen und die damit verbundenen datenschutzrechtlichen Fragen sind kaum gelöst (z.B. zur Datenweitergabe an andere Unternehmen, auch in Drittstaaten, zur Datensicherheit, zu den eingesetzten Techniken). Das hängt auch damit zusammen, dass mitunter unklar ist, welche Datenverarbeitungen mit solchen Services einhergehen und ob das in Ländern stattfindet, die einen Datenschutzstandard vorsehen, der dem in der EU vergleichbar ist.

Dies gilt auch für die Verwendung von WhatsApp im Unternehmensbereich. Da sehr viele große Anbieter im Moment ihre Dienste DSGVO konform ausgestalten bzw laufend daran arbeiten, sollte dieses Thema weiter beobachtet werden. Berücksichtigt sollte dabei werden, dass eine Datenweitergabe in das EU-Ausland zumindest in den Datenschutz-Richtlinien des Anbieters selbst ausgewiesen wird (vgl https://www.whatsapp.com/legal/ bzw. die WhatsApp Datenschutzrichtlinie https://www.whatsapp.com/legal/?eea=1#privacy-policy) und diese Datenweitergabe in das EU-Ausland an gewisse datenschutzrechtliche Voraussetzungen gebunden ist, die der Verantwortliche selbst zu prüfen hat (vgl auch WKO-Infoseite zum Thema https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Internationaler-Datenverk.html).

Was muss ich beachten, wenn ich Google Analytics verwende?

Sie müssen über die „Datensammlung“ informieren. Bereits jetzt sind Sie verpflichtet, über eingesetzte Cookies und Social Plug-Ins aufzuklären. Dies gilt auch für das Trackingtool Google Analytics., Näheres hierzu finden Sie auf der WKO-Infoseite zum Thema: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/datenverarbeitung-webshop-website.html.

Wann brauche ich einen Datenschutzbeauftragten?

Eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht für ein Unternehmen, wenn es im Rahmen seiner Kerntätigkeit Verarbeitungsvorgänge durchführt, die entweder aufgrund ihrer Art, ihres Umfanges und/oder ihrer Zwecke eine umfangreiche und systematische Überwachung von Betroffenen erforderlich machen oder in der umfangreichen Verarbeitung sensibler Daten oder von Daten über strafrechtliche Verurteilungen oder Straftaten bestehen. (vgl die WKO-Infoseite https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Der-Datenschutzbeauftragt.html).

Wann werden personenbezogene Daten verarbeitet?

Der Begriff der **Verarbeitung** ist sehr weit zu verstehen. Er umfasst nach dem Wortlaut der DSGVO eine Vielzahl von Vorgängen, die allesamt zu Ihrem unternehmerischen Alltag gehören, und zwar das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung,

Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten.

Beispiele: Erstellung einer Kundendatei, Aufnahme der Daten zur Erstellung einer Rechnung, Anlegen, Verwalten und Löschen der Mitarbeiterdatenbank

2.2. Was sind sensible bzw. besondere Kategorien personenbezogener Daten?

Die DSGVO sieht im Zusammenhang mit bestimmten Kategorien personenbezogener Daten verschärfte Schutzstandards vor: Deren Verarbeitung bedarf einer ausdrücklichen Einwilligung des Betroffenen. Dies gilt für Daten, die sich auf spezielle persönliche Eigenschaften des Betroffenen beziehen, und zwar insbesondere genetische Daten, biometrische Daten, die – z.B. in einem Reisepass – zur eindeutigen Identifikation gedacht sind, Gesundheitsdaten, Daten zum Sexualleben oder zur sexuellen Orientierung, aber auch seine rassische oder ethnische Herkunft, seine politische Meinung, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft.

Gesundheitsdaten beziehen sich auf die körperliche oder geistige Gesundheit einer natürlichen Person. Dies schließt die bei der Erbringung von Gesundheitsdienstleistungen erfassten Informationen über den Gesundheitszustand (auch wenn keine Krankheit vorliegt) mit ein.

Beispiele: Daten über Allergien, körperliche Einschränkungen oder sexuelle Vorlieben;

Häufige Fragen

Wir haben ein Online-Buchungstool für Events und verarbeiten dort neben den allgemeinen Personendaten (Name, Adresse, Telefon, E-Mail, etc.) auch spezielle Informationen, die uns die Kunden mitteilen, damit die Verpflegung beim Event entsprechend angepasst werden kann (zB Laktoseintoleranz, Vegetarier, halal und dergleichen). Zählen diese Daten bereits zu "sensiblen" Daten?

Ernährungswünsche oder -gewohnheiten ohne zwingende Verbindung zu einem religiösen Bekenntnis sind nicht zwangsläufig immer auch sensible Daten:

„Halal“ oder „kosher“ können einen Rückschluss auf die Religion zulassen, Informationen über Allergien, Lebensmittelunverträglichkeiten und dergleichen sind gesundheitsbezogen. Im konkreten Fall empfehlen wir bereits im Rahmen des Buchungsprozesses für solche Wünsche die Einholung der ausdrücklichen Einwilligung des betroffenen Kunden.

Gehört das Religionsbekenntnis zu den besonders berücksichtigungswürdigen „sensiblen“ Daten?

Ja. Wenn jemand z.B. als Gast an einer Trauung nach katholischem Ritus teilnimmt, können daraus aber noch keine Schlussfolgerungen auf sein Religionsbekenntnis gezogen werden.

2.3. Verantwortlichkeit und Auftragsverarbeitung

Der **Verantwortliche** (primär natürliche oder juristische Personen, Behörde und sonstige Rechtsträger) entscheidet über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten und muss sicherstellen, dass die Datenschutzbestimmungen eingehalten werden. Wenn die Zwecke und Mittel der Verarbeitung gesetzlich vorgegeben sind (z.B. durch EU- oder nationale Vorschriften), so können auch weitere Vorschriften, die den Verantwortlichen betreffen, damit geregelt sein.

Beispiele: Auftraggeber, Agentur

Auftragsverarbeiter sind Rechtsträger, die unter der Weisungsgewalt des Verantwortlichen personenbezogene Daten im Auftrag des Verantwortlichen bearbeiten. Sie sind insoweit nur ausführender Gehilfe unter dem Mantel des Verantwortlichen und verfolgen mit der Datenverarbeitung keinen anderen als den vom Verantwortlichen gewünschten Zweck.

Beispiele: externer Buchhalter, externe Dienstleister zur Bereitstellung von Web-Anmeldeplattformen, etc.

Der Auftragsverarbeiter wird dann selbst zum Verantwortlichen, wenn er im Rahmen der Datenverarbeitung eigenmächtig von dem vom Verantwortlichen vorgegebenen Zweck abweicht oder darüber hinausgeht.

Der Verantwortliche schließt mit dem Auftragsverarbeiter einen Dienstleistungsvertrag ab, in dem sich der Auftragsverarbeiter zur rechtskonformen Datenverarbeitung verpflichten muss. Die Berechtigung zur Sub-Auftragsvergabe samt Überbinden der entsprechenden Verpflichtungen muss ausdrücklich vorgesehen sein, ebenso sind Geheimhaltungspflichten zu verankern. Den Verantwortlichen trifft eine Verantwortung für die Auswahl eines geeigneten Auftragsnehmers. Diesen trifft wiederum die Pflicht zum sofortigen Widerspruch, wenn eine Weisung des Verantwortlichen rechtswidrig sein sollte.

Häufige Fragen

Müssen mit unseren Mitarbeitern und der externen Lohnverrechnung Vereinbarungen abgeschlossen werden, damit personenbezogene Daten übermittelt werden dürfen?

Ihre Mitarbeiter sind darüber aufzuklären, dass Sie die Daten weitergeben, eine Zustimmung ist wegen des Interesses an einer ordnungsgemäßen Lohnverrechnung nicht erforderlich. Mit dem externen Lohnverrechnungspartner müssen Sie eine DSGVO-konforme Auftragsverarbeitervereinbarung abschließen.

Wer sind sonst noch typische Auftragsverarbeiter im Eventmanagement? Mit wem muss ich hier eine schriftliche Vereinbarung zur Auftragsverarbeitung treffen?

Neben der externen Lohnverrechnung und Buchhaltung sind dies alle Unternehmen, die für Sie als Auftragnehmer personenbezogene Daten verarbeiten, etwa Unternehmen, die für Sie den Newsletter- und E-Mail-Versand abwickeln.

Darf ich Anfragen von Kunden zur Unterbringung im Rahmen eines Events ungefragt an andere Vermieter oder Unterkunftgeber weiterleiten, wenn mein Event-Hotel schon ausgebucht ist?

Nein, hierfür bedarf es der nachweisbaren Einwilligung des Kunden.

Grundpflichten

Rechtmäßigkeit der Verarbeitung

Pflichten des Verantwortlichen

3. Pflichten bei der Datenverarbeitung

3.1. Grundpflichten im Rahmen der Verarbeitung

Die folgenden Grundsätze sind die prägenden Säulen des neuen Datenschutzrechts. Ihre Einhaltung muss im Sinne einer umfassenden Rechenschaftspflicht nachgewiesen werden können und ihre Missachtung kann sehr unangenehme und auch teure Folgen haben:

3.1.1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Personenbezogene Daten müssen rechtmäßig verarbeitet werden.
Es geltend die Prinzipien der Fairness, der Transparenz und von Treu und Glauben. Die Verarbeitung muss in einer für die betroffene Person nachvollziehbaren Weise erfolgen.

Diese Transparenz und Fairness bedeutet, dass alle Informationen und Mitteilungen zur Verarbeitung der personenbezogenen Daten für den Betroffenen leicht zugänglich sind und rechtzeitig in klarer und einfacher Sprache erläutert werden. Dies betrifft insbesondere Informationen über die Identität des Verantwortlichen, die genauen Zwecke und die Dauer der Verarbeitung sowie die Auskunft darüber, welche personenbezogenen Daten verarbeitet werden.

3.1.2. Zweckbindung

Die Erhebung von personenbezogenen Daten ohne festgelegte, eindeutige und legitime Zwecke ist nicht zulässig.
Die Weiterverarbeitung in einer mit diesen Zwecken nicht zu vereinbarenden Weise ist ebenfalls nicht erlaubt. Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Zwecke oder für statistische Zwecke gilt aber nicht als unvereinbar mit dem ursprünglichen Zweck.

3.1.3. Datenminimierung

Die Datenverarbeitung soll auf das für den konkreten Zweck Notwendige beschränkt sein.
Das bedeutet zugleich, dass die Verarbeitung dem Zweck angemessen, erheblich sowie auf das notwendige Maß beschränkt sein muss. Dazu zählt auch, dass Verantwortliche durch technische Voreinstellungen sicherstellen müssen, dass sie und ihre Auftragsverarbeiter grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Zweck erforderlich ist, verarbeiten.

3.1.4. Richtigkeit

Falsche Daten sollen vermieden werden.
Verarbeitungen müssen aus diesem Grund mit Daten erfolgen, die sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind. Es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige personenbezogene Daten gelöscht oder berichtigt bzw. aktualisiert werden. (Für den Umgang mit Sicherungskopien gelten Erleichterungen.)

3.1.5. Speicherbegrenzung

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, allerdings nur so lange wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.
Das bedeutet zugleich, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Deshalb sollte der Verantwortliche Fristen für die Löschung oder regelmäßige Überprüfungen vorsehen. Ausnahmen sind nur eingeschränkt für ausschließlich im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke zulässig. Für den Umgang mit Sicherungskopien hat der österreichische Gesetzgeber Erleichterungen vorgesehen, wenn das aus wirtschaftlichen oder technischen Gründen erforderlich ist. Dies ist im Einzelfall zu prüfen.

3.1.6. Integrität und Vertraulichkeit

Die Grundsätze der Integrität und der Vertraulichkeit bedeuten, dass adäquate Schutzmaßnahmen erforderlich sind, um eine angemessene Sicherheit der personenbezogenen Daten zu gewährleisten.
Durch geeignete technische und organisatorische Maßnahmen soll insbesondere gewährleistet werden, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, von Unbefugten benutzt werden können.

Häufige Fragen

Stellen passwortgeschützte Zugänge zu Datenbanken, Firewalls und abgesperrte Büros ausreichende Schutzmaßnahmen dar?

Welche IT-Maßnahmen sind notwendig, um sensible Daten zu schützen?

Welcher Passwortschutz ist erforderlich?

Ist es erlaubt, dass auch ein IT-Administrator auf sensible Daten zugreifen kann?

Was im konkreten Einzelfall für die jeweils relevanten Datenkategorien ausreichend ist, ist nach dem Stand der Technik, den stattfindenden Datenverarbeitungen und damit verbundenen Risiken, aber auch nach Ihren finanziellen Möglichkeiten zu beurteilen.

Eine entsprechend konfigurierte Firewall zählt allerdings zu den Basismaßnahmen der IT-Sicherheit. Einen sehr guten Überblick über den Stand der Technik und Marktüblichkeit können Sie sich unter www.it-safe.at verschaffen. Informationen dazu finden Sie auch im IT-Sicherheitshandbuch für KMU www.wko.at/site/it-safe/sicherheitshandbuch.html

Grundsätzlich soll kein Mitarbeiter mehr Zugriffsrechte haben, als er für seine Tätigkeit braucht. Gibt es aber nachvollziehbare technische Gründe, warum der IT-Administrator Zugriff auch auf sensible Daten benötigt, wird dies im Regelfall auch erlaubt sein. Dies ist aber auf das Erforderliche zu beschränken und im Verarbeitungsverzeichnis zu dokumentieren. Das implementierte Organisationssystem muss sachlich ungerechtfertigte Zugriffe verhindern: Es ist kritisch zu hinterfragen, ob sich die Vergabe von Benutzerrechten an den organisatorischen Notwendigkeiten orientiert oder zu großzügig ist.

Wann ist eine end-to-end Verschlüsselung im E-Mail Verkehr erforderlich?

Die DSGVO verlangt nicht zwingend die Verschlüsselung, nennt diese aber im Rahmen der Datenschutzfolgenabschätzung als geeignete technische Maßnahme, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Verschlüsselung oder Pseudonymisierung erscheint insbesondere bei der Erfassung und Verarbeitung von Bankverbindungen, Kreditkartendaten, sensiblen Daten oder Daten über Straftaten sinnvoll.

Wie muss ich Daten/Adressen sichern, die in Papierform festgehalten werden?

Eine ausreichende Datensicherheit kann z.B. durch Nutzungsbeschränkung auf bestimmtes Personal, die Beschränkung von Zutritts- und Zugriffsberechtigungen zum Ablagesystem (Safe, versperrbare Kästen in Räumen mit Zugangssperren), geeignete Zutrittscodes und Passwörter, aber auch räumliche Trennungen erreicht werden.

Ich möchte Kundendaten und -wünsche (z.B. Hochzeitsdatum, Polsterwünsche, besondere Essenswünsche (Kosher, Allergien) für Werbezwecke oder den nächsten Besuch speichern, um den Kunden bestmöglich in Erinnerung zu behalten. Darf ich das?

Es ist derzeit unklar, wie lange derartige Daten gespeichert werden dürfen. Wenn seit dem letzten Besuch des Gastes mehr als ein Jahr vergangen ist, wird man von einer Löschpflicht ausgehen müssen, es sei denn, der Gast hat der längeren Speicherung ausdrücklich zugestimmt. Außerdem ist zu prüfen, ob eine Einwilligung zur Versendung von Werbemails gemäß § 107 Telekommunikationsgesetz erforderlich ist, wenn Sie Werbung via elektronischer Nachrichten (E-Mail, SMS, WhatsApp, …) verschicken möchten oder telefonisch Kontakt aufnehmen möchten.

Im Fall eines Erstkontakts ist für die telefonische oder elektronische Kontaktaufnahme zu Zwecken der Direktwerbung eine Zustimmung erforderlich. Bei bereits bestehenden Kunden kann per Mail Direktwerbung für ähnliche Produkte oder Dienstleistungen erfolgen. Der Kunde muss aber eine wirksame Möglichkeit zum Abbestellen des Mailversands haben. Liegt keine Einwilligung vor, können E-Mails an

Kunden ohne Beschränkung der Empfängerzahl versendet werden, wenn sämtliche der folgenden fünf Voraussetzungen vorliegen:

- die E-Mail-Adresse des Kunden wird beim Verkauf einer Ware oder einer Dienstleistung erhoben und
- der Kunde erhält bei Erhebung der E-Mail-Adresse die Möglichkeit, den Empfang kostenfrei und problemlos abzulehnen und
- der Kunde erhält bei jeder Zusendung die Möglichkeit, den Empfang kostenfrei und problemlos abzulehnen und
- die Zusendung erfolgt zur Direktwerbung für eigene, ähnliche Produkte und
- der Kunde ist nicht in die sog „ECG-Liste“ (auch „Robinson-Liste“) eingetragen.

Weitere Informationen hierzu finden Sie hier: www.wko.at/service/wirtschaftsrecht-gewerberecht/E-Mails_versenden_-_aber_richtig.html.

Wenn ein Kunde per E-Mail Information für ein Event-Angebot einholt – benötige ich dann eine Einwilligung, damit ich seine E-Mail-Adresse verwenden darf?

Für die Bearbeitung der Anfrage des Kunden und die allfällige Buchung bilden die Vertragsanbahnung und der Vertragsabschluss eine ausreichende Rechtsgrundlage.

Ist die Verarbeitung personenbezogener Daten von Kunden zur Versendung von Weihnachtspost zulässig?

Weihnachtspost gilt als Form der Direktwerbung. Analoge Werbung per Post ist zulässig, solange der Kunde nicht ausdrücklich widersprochen hat. Postalische Werbung ist datenschutzrechtlich bei einem aufrechten Kundenverhältnis aufgrund der berechtigten Interessen des Versenders zulässig. Für eine elektronische Nachricht ist zu prüfen, ob eine Einwilligung gemäß § 107 Telekommunikationsgesetz erforderlich ist (siehe oben).

Die meisten ERP-Systeme (Warenwirtschaftssysteme) sind nicht in der Lage Kundendaten zu löschen, solange es noch Sub-Datensätze (Rechnungen usw.) gibt. Was mache ich, wenn ein Kunde auf Löschung besteht?

Eine Verpflichtung zum Löschen besteht nicht, solange der Vertrag noch aufrecht ist (z.B., weil der Vertrag noch nicht vollständig erfüllt wurde, noch eine Rechnung offen ist, etc.) oder gesetzliche Aufbewahrungsfristen (zB Steuer 7 Jahre) maßgeblich sind und nur die für die Aufbewahrung wirklich notwendigen Daten gespeichert werden. Jedenfalls muss auf das Löschungsbegehren verordnungskonform reagiert und dem Kunden gegenüber begründet erklärt werden, warum die Daten noch nicht gelöscht werden können.

3.2. Rechtmäßigkeit der Verarbeitung

Damit personenbezogene Daten rechtmäßig verarbeitet werden, kommen unterschiedliche Rechtsgrundlagen in Betracht. Welche Rechtsgrundlage das ist hängt auch davon ab, ob die Daten „sensibel“ sind oder strafrechtlich relevant, weil für solche Daten Einschränkungen bestehen. Als Rechtsgrundlagen kommen insbesondere in Betracht:

3.2.1. Einwilligung

Die Einwilligung des Betroffenen muss rechtzeitig durch eine eindeutige bestätigende Handlung oder Erklärung erfolgen. Sie muss freiwillig, für den konkreten Fall und Zweck und in informierter Weise erfolgen. Es muss unmissverständlich bekundet werden, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden und über die Möglichkeit des Widerrufs informiert ist. Diese Einwilligung kann mündlich, schriftlich oder elektronisch erfolgen, etwa auch durch Anklicken eines Kästchens auf einer Internetseite (Opt In). Es bedarf im jeweiligen Kontext des eindeutigen Einverständnisses der betroffenen Person zur Datenverarbeitung. Stillschweigen, bereits vorangekreuzte Kästchen oder Untätigkeit stellen keine Einwilligung dar. Wenn die Verarbeitung mehreren Zwecken dient, ist für jeden Zweck der Verarbeitung eine gesonderte Einwilligung nötig.

Muster-Einwilligungserklärungen finden Sie unter wko.at/bstf/datenschutzimtourismus.

Häufige Fragen

Müssen wir den Kunden, der seine Teilnahme an einem Event bei einer Agentur bucht, bei der Erfassung seiner Daten (Name, Adresse, Telefonnummer etc.) unterschreiben lassen, dass er der Datenverarbeitung und -weitergabe an ein Hotel für eine von ihm gewünschte Zimmerbuchung zustimmt?

Ja. Beachten Sie in diesem Zusammenhang auch, dass die Vermittlung einer Unterkunft einer Reisebüroberechtigung bedarf (§ 126 Abs 1 Z 3 GewO). Selbst wenn sie im Nebenrecht erfolgt, braucht die Agentur eine „entsprechend ausgebildete und erfahrene Fachkraft".

Muss für die Veröffentlichung von Fotos auf der Homepage, auf denen Gäste erkennbar sind, eine schriftliche Einverständniserklärung eingeholt werden?

Hier sind Einwilligungen nach dem Datenschutz-, Urheberrecht und Persönlichkeitsrechten zu unterscheiden:

Eine datenschutzrechtliche Einwilligung kann grundsätzlich auch mündlich erteilt werden. Aus Beweisgründen empfiehlt sich allerdings entweder eine schriftliche Einwilligung oder jedenfalls die schriftliche Protokollierung der Einholung der mündlichen Einwilligung.

Ob die Veröffentlichung eines Fotos zusätzlich aus anderen Gründen (z.B. Persönlichkeitsrechte) zustimmungspflichtig ist, hängt von den Umständen des Einzelfalls und den berechtigten Interessen der abgebildeten Person ab. Für den Fall, dass eine Zustimmung eingeholt wird, empfehlen wir diese schriftlich einzuholen.

Muss ich vor jeder Kontaktaufnahme (telefonisch, postalisch, per Mail) mit dem Kunden zu Werbezwecken für die Datenverarbeitung eine gesonderte Einwilligung einholen?

Die für Postwerbung erforderliche Verarbeitung von Adressdaten ist in aller Regel durch die berechtigten Interessen des Unternehmers gedeckt. Der Kunde kann aber künftigen Zusendungen widersprechen.

Für Anrufe oder E-Mails gelten die Bestimmungen des Telekommunikationsgesetzes (§ 107). Im Fall eines Erstkontakts ist für die telefonische oder elektronische Kontaktaufnahme zu Zwecken der Direktwerbung eine Zustimmung erforderlich. Bei bereits bestehenden Kunden kann per Mail Direktwerbung für ähnliche Produkte oder

Dienstleistungen erfolgen. Der Kunde muss aber eine wirksame Möglichkeit zum Abbestellen des Mailversands haben.

Liegt keine Einwilligung vor, können E-Mails an Kunden ohne Beschränkung der Empfängerzahl versendet werden, wenn sämtliche der folgenden fünf Voraussetzungen vorliegen:

- die E-Mail-Adresse des Kunden wird beim Verkauf einer Ware oder einer Dienstleistung erhoben und
- der Kunde erhält bei Erhebung der E-Mail-Adresse die Möglichkeit, den Empfang kostenfrei und problemlos abzulehnen und
- der Kunde erhält bei jeder Zusendung die Möglichkeit, den Empfang kostenfrei und problemlos abzulehnen und
- die Zusendung erfolgt zur Direktwerbung für eigene, ähnliche Produkte und
- der Kunde ist nicht in die sog „ECG-Liste“ eingetragen.

Weitere Informationen hierzu finden Sie hier: www.wko.at/service/wirtschaftsrecht-gewerberecht/E-Mails_versenden_-_aber_richtig.html.

Wie geht man mit Daten eines Interessenten um, der eine herkömmliche Formularanfrage über eine Website an uns gerichtet hat, aber vielleicht nicht zum Kunden wird?

Wir empfehlen im Kontaktformular eine Opt-In Möglichkeit zu verwenden, mit der der Interessent zustimmt, dass die Daten bis auf Widerruf zum Versand und Erhalt elektronischer Werbung gespeichert und verarbeitet werden dürfen.

Berücksichtigen Sie auch die Kriterien des § 107 TKG in obiger Antwort.

Was ist bei einem Newsletter zu beachten, den ich für einen Kunden umsetzen soll?

Berücksichtigen Sie auch die Kriterien des § 107 TKG in obiger Antwort.

Kann ich Lieferanten oder Kunden in einer laufenden Geschäftsbeziehung zum Geburtstag gratulieren?

Das Geburtsdatum einer Person gehört zu den personenbezogenen Daten, sodass seine Verarbeitung zu Werbezwecken einer tauglichen Rechtsgrundlage bedarf. Bei Personen, mit denen eine laufende Geschäftsbeziehung besteht, spricht viel dafür, dass Ihre berechtigten Interessen als Unternehmer die Gratulation (=Datenverarbeitung) zulassen. Zu berücksichtigen ist auch, dass die Glückwünsche so übermittelt werden, dass Sie nur den Jubilar erreichen, und nicht auch Dritte.

Sollten bereits wirksame Einwilligungen eingeholt worden sein, dann bleiben diese auch nach dem 25.5.2018 wirksam, sofern sie nicht widerrufen werden. Gleiches gilt für Zustimmungserklärungen zum E-Mail-Versand gemäß § 107 Telekommunikationsgesetz.

3.2.2. Vertragserfüllung und/oder –vorbereitung

Wenn die betroffene Person einen Vertrag abschließt oder anstrebt, der eine Datenverarbeitung mit sich bringt, darf die Verarbeitung „nicht-sensibler“ Daten zum Zweck der Vertragserfüllung erfolgen. Das gilt nicht für die Verarbeitung der

Daten von Personen, die nicht selbst Vertragspartei sind, es sei denn, es liegt eine wirksame Stellvertretung vor.

3.2.3. Erfüllung einer Rechtspflicht durch den verantwortlichen Unternehmer

Die Verarbeitung ist weiters zulässig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung des verantwortlichen Unternehmers (z.B. arbeits(zeit)rechtliche oder steuerrechtliche Verpflichtungen) erforderlich ist.

3.2.4. Wahrung lebenswichtiger Interessen natürlicher Personen

Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

3.2.5. Öffentliche Aufgaben

Die Verarbeitung ist auch zulässig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage ist für privatwirtschaftlich agierende Unternehmer nur dann relevant, wenn sie mit hoheitlichen Aufgaben betraut und entsprechenden Befugnissen ausgestattet sind.

3.2.6. Berechtigte Interessen

Die Verarbeitung kann zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich sein, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (dies insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt). Als berechtigte Interessen kommen legale, ideelle und wirtschaftliche Interessen (z.B. Journalismus, Direktwerbung, arbeitsteilige Datenverarbeitung im Konzern, Wahrung eigener Ansprüche, Verteidigung eigenen Eigentums und Vermögens) in Betracht. Nur unverhältnismäßige Folgen für den Betroffenen sind zu vermeiden. Wenn ein Widerspruch gegen Direktwerbung vorliegt, sind berechtigte Interessen zur Fortsetzung der Direktwerbung ausgeschlossen.

3.2.7. Sonderbestimmungen für besondere („sensible“) Datenkategorien

Für die Verarbeitung sensibler Daten kommen weitere, sehr spezifische Rechtsgrundlagen (z.B. im Zusammenhang mit arbeits- und sozialrechtlichen Rechten und Pflichten, Gesundheitsvorsorge, Arbeitsmedizin, Verarbeitung durch Non Profit Organisationen) in Betracht.

Insbesondere dürfen sensible Daten bei einer ausdrücklichen Einwilligung der betroffenen Person und im Falle einer gesetzlichen Verpflichtung verarbeitet werden.

Darüber hinaus dürfen sensible Daten, die die betroffene Person offensichtlich öffentlich (z.B. ohne Einschränkung online oder in öffentlichen Registern) gemacht hat, verarbeitet werden. „Offensichtlich“ bedeutet, dass die betroffene Person diese Veröffentlichung freiwillig vorgenommen haben muss.

Häufige Fragen

Wenn ich von meinen Mitarbeitern das Religionsbekenntnis und die Gewerkschaftszugehörigkeit für die Lohnverrechnung abspeichere und verarbeite. Habe ich dann bereits sensible Daten? Was sind die Folgen?

Das sind sensible Daten. Für die Verarbeitung derartiger Daten brauchen Sie entweder eine ausdrückliche Einwilligung vom betroffenen Mitarbeiter oder das Erfordernis der Erfüllung gesetzlicher Verpflichtungen, insbesondere arbeits- und sozialrechtlicher Vorschriften.

Ersucht der Arbeitnehmer, den Gewerkschaftsbeitrag über die Lohnverrechnung abzurechnen, ist von einer Zustimmung zur Verarbeitung dieser Daten zu diesem Zweck auszugehen. Gleiches gilt, wenn das Religionsbekenntnis bekannt gegeben wird, um den Karfreitag als Feiertag im Sinne des Arbeitsruhegesetzes zu erhalten. Die Weiterverarbeitung dieser Daten zu Lohnverrechnungszwecken ist gesetzlich oder kollektivvertraglich geregelt.

3.3. Pflichten des Verantwortlichen und seines Auftragsverarbeiters

Die DSGVO ist von der Pflicht zur Transparenz und umfassenden Rechenschaft geprägt. Das bringt auch mit sich, dass man präzise, leicht auffindbar und verständlich sowie mitunter unentgeltlich aufklären muss. Der Verantwortliche muss dies rechtzeitig sicherstellen und den Nachweis erbringen können, dass die Verarbeitung entsprechend der DSGVO erfolgt. Zu seinen Pflichten gehören insbesondere die Folgenden:

- Der Verantwortliche muss betroffene Personen über erhebliche Aspekte der Datenverarbeitung informieren und entsprechende Auskunftsersuchen erfüllen. Bei begründeten Zweifeln an der Identität einer Person, die um Auskunft ersucht, kann man weitere Informationen verlangen (siehe unter Punkt 4. “Informationspflichten und Betroffenenrechte“).

- Der Verantwortliche darf nur mit geeigneten Auftragsverarbeitern zusammenarbeiten. Diese sind dem Verantwortlichen weisungsgebunden. Sie dürfen nur mit seiner Zustimmung Sub-Auftragsverarbeiter hinzuziehen und müssen mit dem Verantwortlichen Verträge abschließen, für die detaillierte Vorgaben mit Mindestinhalten gelten.

- Der Verantwortliche muss geeignete technische und organisatorische Maßnahmen umsetzen, um eine rechtmäßige Datenverarbeitung sicherzustellen. Dazu gehören nicht nur datenschutzfreundliche Voreinstellungen, um zu verhindern, dass überschießende Datenverarbeitungen stattfinden, sondern auch der Einsatz passwortgeschützter Datenträger (z.B. USB-Sticks) oder Bestätigungen über die erfolgte Löschung von Daten auf Datenträgern der Agentur. Er muss dies auch nachweisen können (siehe auch Punkt 7. 4. „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“).

- Der Verantwortliche (und ausnahmsweise auch seine Vertreter) sowie Auftragsverarbeiter müssen zudem ein Verzeichnis aller

Datenverarbeitungstätigkeiten (sog „VVT“), die ihrer Zuständigkeit unterliegen, führen.
Musterverarbeitungsverzeichnisse finden Sie unter wko.at/bstf/datenschutzimtourismus.

- Der Verantwortliche ist verpflichtet, mit der Aufsichtsbehörde auf Anfrage zusammen zu arbeiten.

Im Falle einer Datenschutzverletzung (z.B. Hack-Angriff, Leak, Verlust eines Datenträgers wie Smartphone, Notebook oder USB-Stick mit nach der DSGVO geschützten Daten) muss der Verantwortliche unverzüglich (spätestens binnen 72 Stunden) eine Meldung an die Aufsichtsbehörde durchführen. Die Meldung darf ausnahmsweise unterbleiben, wenn kein Risiko für die betroffene Person besteht. Zusätzlich hat er die betroffenen Personen, wenn für diese ein hohes Risiko besteht, direkt zu informieren. Ausnahmen von der Verständigungspflicht sind möglich. Ob Ausnahmen bestehen, ist im Einzelfall sorgfältig zu prüfen.

Wenn Datenanwendungen des Verantwortlichen zu einem wahrscheinlich hohen Risiko für betroffene Personen führen, muss im Einzelfall abgeklärt werden, ob zusätzlich eine sogenannte „Datenschutz-Folgenabschätzung“ vorzunehmen (beziehungsweise gegebenenfalls die Aufsichtsbehörde zu konsultieren) und ein Datenschutzbeauftragter einzusetzen ist.

Die Datenschutzbehörde hat eine Verordnung (DSFA-AV, BGBl II 108/2018 vom 25. 5. 2018) erlassen, mit der für einige Branchen und bestimmte Datenverarbeitungen die Verpflichtung zur Durchführung einer solchen Abschätzung eingeschränkt wurde. Solche Ausnahmen gelten nur in dem von der Datenschutzbehörde präzise festgelegten Rahmen, etwa für Kundenbetreuung und Marketing für eigene Zwecke, zur Videoüberwachung, für Bild- und Akustikdatenverarbeitung in Echtzeit oder zu Dokumentationszwecken. Im Einzelfall ist sorgfältig zu prüfen, ob die Vorgaben für Ausnahmen nach der Verordnung eingehalten werden.

Selbst wenn keine Datenschutz-Folgenabschätzung benötigt wird, müssen die übrigen Vorschriften der DSGVO und des DSG eingehalten werden. Oft werden Bild- und Videoaufnahmen von Events zu rein dokumentarischen Zwecken (z.B. Aufbau oder genereller Publikumsbesuch) angefertigt, ohne Personen gezielt identifizierend ins Bild zu setzen. Solche Aufnahmen bleiben dann vielfach firmenintern zur Dokumentation gespeichert. Derartige Verarbeitungsvorgänge fallen unter das Datenschutzgesetz und unterliegen strikten Vorgaben zur Kennzeichnung und Kontrolle des Zugangs und des Schutzes vor Veränderung. Sie sind im Datenverarbeitungsverzeichnis, für das ein unverbindliches Muster unter LINK EINFÜGEN abrufbar ist, zu dokumentieren und in aller Regel spätestens drei Jahre nach der Aufnahme zu löschen, sofern sie nicht gesetzeskonform berechtigt wurden.

Häufige Fragen

Kann ich als Geschäftsführer die Verantwortung für die Einhaltung der Datenschutzvorschriften an einen Mitarbeiter delegieren?

Nach § 9 VStG haften alle Geschäftsführer für die Einhaltung der Verwaltungsgesetze, d.h. auch des DSG. Wurde für einen Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person verhängt, so kann nach der derzeitigen Rechtslage neben der juristischen Person selbst nicht gleichzeitig ihr Vertreter bzw. der verantwortliche Beauftragte für denselben Verstoß bestraft werden.

Um zu vermeiden, dass im Fall einer Rechtsverletzung alle Geschäftsführer bestraft werden, sollte die Geschäftseinteilung vorsehen, dass nur einer der Geschäftsführer für Belange des Datenschutzes zuständig ist. Die Haftung des Geschäftsführers besteht unabhängig von der Bestellung eines Datenschutzbeauftragten oder eines Datenschutzkoordinators.

Jeder Einzelunternehmer und jede juristische Person muss ein gesondertes Verarbeitungsverzeichnis erstellen. Die Unternehmensbezeichnung muss der Firma entsprechen, um Verwechslungen zu verhindern.

Wie lange dürfen Bewerberdaten in Evidenz gehalten werden? Wie sieht es bei (Blind)bewerbungen bezüglich Archivierung/Speicherung aus, um beispielsweise später darauf zugreifen zu können? Wie geht man datenschutzkonform mit Initiativbewerbungen um?

Die Frist zur Geltendmachung von Ansprüchen nach §§ 15 Abs 1 und 29 GlBG wegen Diskriminierung bei Bewerbungen beträgt 6 Monate ab Ablehnung der Beförderung bzw der Bewerbung. Sollte eine Evidenzhaltung danach geplant sein, muss das im Einzelfall mit einem „berechtigten Interesse“ des Unternehmens begründet werden können oder man holt sich rechtzeitig die Einwilligung für die dauerhafte Evidenzhaltung ein.

Bei einer Initiativbewerbung/Blindbewerbung kann das Unternehmen/der Personalvermittler mit einer längeren Aufbewahrungsfrist argumentieren, da sich der Bewerber nicht für einen konkreten Posten bewirbt, sondern wohl (zumindest schlüssig) die Evidenzhaltung wünscht.

Gibt es die gesetzliche Pflicht, die Mitarbeiter nachweislich zu schulen?

Die Belehrung von Mitarbeitern über das Datengeheimnis wird in § 6 Abs 3 DSG angeordnet. Wie diese Belehrung auszusehen hat, bzw. welche Schulungsmaßnahmen sinnvoll sind, ergibt sich aus dem jeweiligen Unternehmen selbst. Tipps und Vergleiche können Sie sich unter www.it-safe.at holen!

Da der Begriff „Datenschutzbeauftragter“ nur dann verwendet werden soll, wenn dies nach der DSGVO erforderlich ist: Macht es Sinn, mich als „Datenschutz-Koordinator“ oder“-Manager“ zu bezeichnen?

Siehe hierzu Punkt 7.1.

Erhebung von Daten direkt bei der betroffenen Person

Erhebung von Daten nicht bei der betroffenen Person selbst

4. Informationspflichten

Informationspflichten setzen ein Informationsbedürfnis des Betroffenen voraus: Verfügt der Betroffene bereits nachweislich über sämtliche Informationen, besteht keine Informationspflicht.

4.1. Informationspflichten, wenn Daten der betroffenen Person erhoben werden

4.1.1. Bei der Erhebung direkt bei der betroffenen Person sind dieser folgende Informationen zu erteilen:

- **Name** und **Kontaktdaten** des **Verantwortlichen** (und gegebenenfalls seiner Vertreter) sowie allenfalls des Datenschutzbeauftragten.

- **Verarbeitungszwecke** und **Rechtsgrundlagen** der Verarbeitung.

- Im Falle einer Datenverarbeitung aufgrund **berechtigter Interessen** des Verantwortlichen bzw. eines Dritten sind die berechtigten Interessen, die vom Verantwortlichen oder einem Dritten verfolgt werden, zu nennen bzw. auszuweisen.

- Gegebenenfalls – auch interne – Empfänger der Daten.

- Falls die Absicht besteht, die Daten an ein **Drittland** oder eine internationale Organisation zu übermitteln, muss auch darüber informiert werden, ebenso wie über das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Europäischen Kommission. Weiters ist im Falle von Datenübermittlung an einen Empfänger in einem Drittland vorbehaltlich geeigneter Garantien oder aufgrund von verbindlichen internen Datenschutzvorschriften, bzw. generell aufgrund von besonderen Ausnahmebestimmungen eben auf diese geeigneten oder angemessenen Garantien zu verweisen oder zumindest die Information zu erteilen, wo eine Kopie erhältlich bzw. verfügbar ist.

  Entsprechende Muster-Datenschutzerklärungen finden Sie unter wko.at/bstf/datenschutzimtourismus.

- Die **Dauer** der Datenspeicherung, bzw wenn dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer.

- Die **Betroffenenrechte** auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch.

- Die Möglichkeit des **jederzeitigen Widerrufs** der Einwilligung, wobei die Verarbeitung bis zum Widerruf rechtmäßig bleibt.

- Das Bestehen eines **Beschwerderechts** bei der in Betracht kommenden Aufsichtsbehörde.

- Über die Rechtsgrundlage, also ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist,

die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte.

- Allenfalls über den Einsatz einer automatisierten Entscheidungsfindung und/oder von Profiling.

Es ist erneut umfassend aufzuklären, wenn zulässiger Weise erhobene Daten für einen anderen Zweck als den, für den sie ursprünglich erhoben wurden, verarbeitet werden sollen.

4.1.2. Bei Erhebung von Daten nicht bei der betroffenen Person selbst

In Fällen der Abschöpfung von Datenbeständen, die Dritte ohne Kenntnis oder gegen den Willen der betroffenen Person erhoben haben, oder im Fall der Erhebung durch Dritte treffen den Verantwortlichen Informationspflichten.

Die Informationen sind der betroffenen Person binnen eines Monats nach Erlangung zu erteilen, jedoch bereits davor, wenn mit diesen Daten mit der Person kommuniziert werden soll. Sollten die Daten einem anderen Empfänger offengelegt werden, spätestens zum Zeitpunkt der Offenlegung.

Die Informationspflicht umfasst:

- Den **Namen** und die **Kontaktdaten** des **Verantwortlichen** (und gegebenenfalls seiner Vertreter) sowie des Datenschutzbeauftragten.

- Die **Verarbeitungszwecke** und **Rechtsgrundlagen** der Verarbeitung.

- Die Kategorien personenbezogener Daten, die verarbeitet werden.

- Gegebenenfalls die – auch internen – Empfänger der Daten.

- Falls die Absicht besteht, die Daten an ein **Drittland** oder eine internationale Organisation zu übermitteln, muss auch darüber informiert werden, ebenso wie über das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Europäischen Kommission. Weiters ist im Falle von Datenübermittlung vorbehaltlich geeigneter Garantien oder aufgrund von verbindlichen internen Datenschutzvorschriften, bzw. generell aufgrund von besonderen Ausnahmebestimmungen eben auf diese geeigneten oder angemessenen Garantien zu verweisen oder zumindest, wo eine Kopie erhältlich wäre.

Im Sinne einer fairen und transparenten Verarbeitung ist ebenfalls bereits bei Erhebung über Folgendes zu informieren:

- Die **Dauer** der Datenspeicherung, bzw wenn dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer.

- Im Falle einer Datenverarbeitung aufgrund berechtigter Interessen des Verantwortlichen bzw eines Dritten sind die **berechtigten Interessen**, die vom Verantwortlichen oder einem Dritten verfolgt werden, zu nennen bzw. auszuweisen.

- Die **Betroffenenrechte** auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch.

- Die Möglichkeit des **jederzeitigen Widerrufs** der Einwilligung, wobei die Verarbeitung bis zum Widerruf rechtmäßig bleibt.

- Das Bestehen eines **Beschwerderechts** bei der in Betracht kommenden Aufsichtsbehörde.

- Aus welcher Quelle die personenbezogenen Daten stammen (zB öffentlich zugängliche Quelle).

- Allenfalls über den Einsatz einer automatisierten Entscheidungsfindung und/oder von Profiling.

Es ist erneut umfassend aufzuklären, wenn zulässiger Weise erhobene Daten für einen anderen Zweck als den, für den sie ursprünglich erhoben wurden, verarbeitet werden sollen.

Es gibt Ausnahmen von der Informationspflicht, etwa wenn gesetzliche oder berufliche Verschwiegenheitspflichten bestehen, die Erfüllung der Pflicht mit einem außergewöhnlich hohen Aufwand verbunden wäre oder die Rechte der betroffenen Person gewahrt bleiben. Das ist im Einzelfall sorgfältig zu prüfen. Auf das Bestehen einer Ausnahme sollte man sich niemals im Vorhinein verlassen.

Auskunftsrecht

Recht auf Berichtigung

Recht auf Löschung

Recht auf Einschränkung der Verarbeitung

Recht auf Datenübertragbarkeit

Widerspruchsrecht

5. Betroffenenrechte

5.1. Allgemein

Die DSGVO stärkt die Rechte der betroffenen Person erheblich. Diese hat

- ein Auskunftsrecht, ob sie betreffende Daten verarbeitet werden, und bejahendenfalls, ein Recht auf Erteilung von Informationen, die jenen bei Erhebung der Daten entsprechen,
- ein Recht auf Berichtigung und auf Löschung sowie ein Recht auf Einschränkung der Verarbeitung samt entsprechenden Mitteilungspflichten,
- ein Recht auf Datenübertragbarkeit, aber auch
- ein Widerspruchsrecht.

Nur der Verantwortliche hat Anträge des Betroffenen zu erledigen. D.h. nur dieser hat bspw. Auskunft zu erteilen oder die Daten zu löschen, zu berichtigen oder einzuschränken. Grundsätzlich ist die Auskunft schriftlich in einer kompakten, transparenten, verständlichen und leicht zugänglichen Form zu erteilen.

Der Verantwortliche hat den Antrag unverzüglich und zunächst einmal unentgeltlich zu beantworten, in jedem Fall aber binnen eines Monats ab Eingang. Ist die Beantwortung des Antrages komplex und liegen mehrfache Anträge vor, kann die Frist um zwei weitere Monate verlängert werden. Wenn der Verantwortliche nicht fristgemäß tätig wird, hat dieser den Auskunftswerber darüber zu informieren und ihn auch über die Möglichkeit einer Beschwerde an die Datenschutzbehörde aufzuklären.

Im Fall wiederholter oder exzessiver Anfragen können Kosten verrechnet oder die Auskunft bei schikanösen Anfragen sogar verweigert werden. Ob die Voraussetzungen dafür vorliegen, sollte im Einzelfall rechtzeitig und sorgfältig geprüft werden, um vermeidbare Auseinandersetzungen zu verhindern. Den Verantwortlichen trifft diesbezüglich die Beweislast.

Eine betroffene Person muss nur dann eine Bestätigung ihrer Identität liefern, wenn der Verantwortliche begründete Zweifel an der Identität des Auskunftswerbers hat (bspw. bei telefonischer Anfrage oder Fantasie-E-Mail Adressen). Werden große Mengen an Informationen über die betroffene Person verarbeitet, trifft sie eine Mitwirkungspflicht.

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. Eine Ausnahme besteht nur dann, wenn diese Mitteilungspflicht unmöglich oder mit einem unverhältnismäßig hohen Aufwand verbunden wäre. Die betroffene Person hat Anspruch auf Auskunft über diese Empfänger.

5.2. Zum Auskunftsrecht

In besonderen Ausnahmefällen kann aus Gründen des öffentlichen Interesses oder zur Wahrung von Betriebs- oder Geschäftsgeheimnissen die Erteilung der Auskunft

verweigert werden, ohne dies zu begründen. Dies ist im Einzelfall sorgfältig vorab zu prüfen.

5.3. Zum Recht auf Berichtigung

Voraussetzung für den Anspruch ist, dass die Daten unrichtig sind, also mit der Wirklichkeit nicht übereinstimmen (z.B. falsches Geburtsdatum) oder dass die Daten unter Berücksichtigung des Zwecks der Verarbeitung unvollständig sind. Den Beweis für die Richtigkeit muss der Verantwortliche, der die Verarbeitung unverändert auf dieser Grundlage fortsetzen will, erbringen.

5.4. Zum Recht auf Löschung ("Recht auf Vergessenwerden")

Die betroffene Person hat einen Anspruch auf Löschung, wenn einer der folgenden Gründe vorliegt:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Sie widerruft ihre Einwilligung zur Datenverarbeitung (und es liegt keine andere Rechtsgrundlage vor); das gilt insbesondere für Daten eines Kindes, die im Zusammenhang mit einem ihm angebotenen Dienst der Informationsgesellschaft (z.B. Online-Spiele) ermittelt worden sind.
- Die betroffene Person legt Widerspruch gegen die Verarbeitung ein (und es liegen keine vorrangigen berechtigten Gründe für die Fortsetzung der Verarbeitung vor).
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich.

5.5. Recht auf Einschränkung der Verarbeitung

Die betroffenen Personen haben einen Anspruch auf Einschränkung der Datenverarbeitung, wenn einer der folgenden Gründe vorliegt:

- Solange die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet und der Verantwortliche dies überprüft.
- Legt die betroffene Person Widerspruch gegen die Verarbeitung ein, besteht dieses Recht, solange nicht feststeht, ob berechtigte Gründe des Verantwortlichen jene des Betroffenen überwiegen.
- Wenn sich die Verarbeitung als unrechtmäßig erweist, die betroffene Person aber statt der Löschung die Einschränkung der Nutzung der personenbezogenen Daten verlangt.
- Wenn der Verantwortliche die personenbezogenen Daten nicht länger für die Zwecke der Verarbeitung benötigt, sie aber die betroffene Person ihrerseits zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt.

5.6. Recht auf Datenübertragbarkeit

Das Recht auf Datenübertragbarkeit ermöglicht der betroffenen Personen, „ihre“ Daten in einem branchenüblichen Format (Interoperabilität) zurückzuerhalten, damit sie an einen anderen Verantwortlichen ihrer Wahl zur fortgesetzten

Verarbeitung übermittelt sowie für ihre eigenen Zwecke und für verschiedene Dienste wiederverwendet werden können. Das Recht setzt voraus, dass die betroffene Person die Daten selbst zur Verfügung gestellt hat und die Verarbeitung mithilfe automatisierter Verfahren auf einer Einwilligung der betroffenen Person oder auf einem Vertrag mit der betroffenen Person beruht.

Für Daten, die in Papierform dokumentiert sind, gibt es das Recht nicht, weil es an einem automatisierten Verfahren mangelt.

5.7. Zum Widerspruchsrecht

Die betroffene Person kann in verschiedenen Fällen Widerspruch gegen die Verarbeitung ihrer Daten erheben. Sie ist im Vorfeld über dieses Recht aufzuklären. Der Widerspruch kann auch mit automatisiertem Verfahren erfolgen:

In Fällen, in denen die Verarbeitung aufgrund öffentlicher Interessen, berechtigter Interessen, die Profiling umfassen können, oder für Forschung oder Statistik stattfindet, kann die betroffene Person Gründe vorbringen, die sich aus ihrer besonderen Situation ergeben. Der Verantwortliche hat die Verarbeitung dann aufgrund des Widerspruchs zu unterlassen, sofern er keine zwingenden schutzwürdigen Gründe für die Fortsetzung der Verarbeitung geltend machen kann.

Im Fall des Widerspruchs gegen Direktmarketing kommt es zu keiner Interessensabwägung: Wenn die Daten der betroffenen Person zu Direktmarketing-Zwecken (einschließlich Profiling, wenn es damit in Verbindung steht) verarbeitet werden, führt der Widerspruch automatisch zu einer Pflicht, diese Datenverarbeitung zu stoppen.

1. Datenschutz-Grundverordnung

2. Begriffe, die Sie kennen sollten

3. Pflichten bei der Datenverarbeitung

4. Informationspflichten

5. Betroffenenrechte

6. Rechtsdurchsetzung und Strafen

7. Maßnahmen

Haftung und Recht auf Schadenersatz

Beschwerde bei der / Kontrolle durch die Datenschutzbehörde

Sanktionen

Strafen nach der DSGVO

Strafen nach dem DSG

6. Rechtsdurchsetzung und Strafen

6.1. Haftung und Recht auf Schadenersatz

Jeder an einer Verarbeitung beteiligte Verantwortliche, der bei der Verarbeitung von Daten gegen die Bestimmungen der DSGVO verstoßen hat, haftet für den dadurch entstandenen Schaden. Jede betroffene Person, die wegen eines Verstoßes gegen die DSGVO, das Grundrecht auf Datenschutz oder die der Durchführung der DSGVO dienenden Bestimmungen des DSG materiellen oder immateriellen Schaden erleidet, hat das Recht, vom Verantwortlichen oder dessen Auftraggeber, der sorgfalts- oder weisungswidrig gehandelt hat, Schadenersatz zu fordern. Es gelten die Regeln des allgemeinen Schadenersatzrechtes.

Der Verantwortliche und der Auftragsverarbeiter sind von der Haftung befreit, wenn sie nachweisen können, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich sind.

6.2. Beschwerde bei der / Kontrolle durch die Datenschutzbehörde

Kontaktdaten:

Österreichische Datenschutzbehörde
Wickenburggasse 8
1080 Wien

Telefon: +43 1 52152 2569
E-Mail: dsb@dsb.gv.at
Web: www.dsb.gv.at

Jede betroffene Person, die sich in ihren Rechten nach der DSGVO oder dem DSG 2018 als verletzt erachtet, hat das Recht, eine Beschwerde an die Datenschutzbehörde zu richten. Die Datenschutzbehörde hat den Beschwerdeführer binnen 3 Monaten ab Einbringung über den Stand und die Ergebnisse des Beschwerdeverfahrens zu informieren.

Die Datenschutzbehörde ist berechtigt, eigenständige Kontrollen einzuleiten. Einer Kontrolle muss keine Beschwerde vorangehen.

6.3. Sanktionen

Die Datenschutzbehörde ist angehalten, bei der Verhängung von Strafen die Verhältnismäßigkeit zu wahren und insbesondere bei erstmaligen Verstößen Verwarnungen auszusprechen. Bei der Verhängung einer Geldbuße und der Entscheidung über deren Höhe sind viele Faktoren ausschlaggebend wie:

- Die Kategorien personenbezogener Daten, die vom Verstoß betroffen sind.
- Die Art, Schwere und Dauer des Verstoßes.
- Die Zahl der von der Verarbeitung betroffenen Personen und das Ausmaß des von diesen erlittenen Schadens.
- Vorsatz oder Fahrlässigkeit des Verstoßes.

- Vorgenommene Maßnahmen zur Schadensminderung.

- Der Grad der Verantwortung des Verantwortlichen und des Auftragsverarbeiters unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen für die Datensicherheit.

- Etwaige einschlägige frühere Verstöße des Verantwortlichen oder Auftraggebers.

- Der Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern.

- Der Umfang und die Art der Meldung des Verstoßes an die Aufsichtsbehörde.

- Die Einhaltung genehmigter Verhaltensregeln oder Zertifizierungsfahren.

- Die durch den Verstoß erlangten Vorteile oder erlittenen Verluste.

6.4. Strafen nach der DSGVO

Die Strafhöhe beträgt bis zu EUR 10 Mio oder im Fall eines Unternehmens bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Betrag höher ist (z.B. Verletzung von Pflichten des Verantwortlichen und Auftragsverarbeitern, etwa zur Erarbeitung eines Verarbeitungsverzeichnisses oder die Verletzung der Datensicherheitsvorschriften).

Bei bestimmten besonders schwerwiegenden Verstößen können Geldbußen von bis zu EUR 20 Mio oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden, je nachdem, welcher Betrag höher ist (z.B. Verletzung fundamentaler Grundsätze für die Datenverarbeitung, Verletzung der Betroffenenrechte, Nichtbefolgung von Anweisungen der Aufsichtsbehörde).

Wird gegen mehrere Bestimmungen der DSGVO verstoßen, so darf der Gesamtbetrag der Geldbuße allerdings nicht den Strafbetrag für den schwerwiegendsten Verstoß übersteigen.

6.5. Strafen nach dem DSG

Wenn weder Strafbestimmungen der DSGVO noch andere Verwaltungsstrafbestimmungen, welche eine strengere Strafe vorsehen, zur Anwendung gelangen, kann von der Datenschutzbehörde noch immer eine Geldstrafe von bis zu EUR 50.000 verhängt werden, wenn

- sich jemand vorsätzlich widerrechtlichen Zugang zu einer Datenverarbeitung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält, oder

- Daten vorsätzlich in Verletzung des Datengeheimnisses übermittelt werden, insbesondere Daten, die ihm unter gewissen Voraussetzungen anvertraut wurden, vorsätzlich für andere unzulässige Zwecke verarbeitet werden, oder

- sich unter Vortäuschung falscher Tatsachen (Vortäuschen Verantwortlicher des öffentlichen Bereichs oder einer Hilfsorganisation zu sein, Katastrophenfall, Hilfeleistung für unmittelbar Betroffene, Auffindung und Identifizierung von Abgängigen und Verstorbenen, Information von Angehörigen) vorsätzlich personenbezogene Daten verschafft, oder

- eine Bildverarbeitung entgegen den gesetzlichen Bestimmungen betreibt oder

- die Einschau der Datenschutzbehörde in die Datenverarbeitungen und die diesbezüglichen Unterlagen verweigert.

- Strafbar ist auch der Versuch. Weiters kann auch der Verfall (behördliche Abnahme) von Datenträgern und Programmen sowie Bildübertragungs- und Bildaufzeichnungsgeräten ausgesprochen werden, wenn diese Gegenstände mit der Verwaltungsübertretung in Zusammenhang stehen.

Ansprechpartner benennen

Ist-Analyse und Erstellung Verarbeitungsverzeichnis

Einholung Einwilligungserklärungen

Datenschutz - Technikgestaltung und datenschutzfreundliche Voreinstellungen

Erfüllung der Informationspflichten

Umsetzung der Betroffenenrechte

Vorgang bei Datenschutzverletzungen festlegen

7. Maßnahmencheck: Sorgen Sie ausreichend vor?

7.1. Ansprechpartner benennen

Nennen Sie den Mitarbeiter Ihres Unternehmens, der in Datenschutzangelegenheiten für Ihr Unternehmen als Ansprechpartner fungiert und für Anfragen der Datenschutzbehörde oder von Betroffenen zuständig ist.

Bezeichnen Sie diesen Mitarbeiter nur dann als Datenschutzbeauftragten, wenn dies nach sorgfältiger Prüfung unbedingt erforderlich sein sollte. Andernfalls vermeiden Sie diese Bezeichnung bitte!

Ein Mitarbeiter, der intern für Datenschutzfragen verantwortlich sein sollte, wird aufgrund seiner Funktion nicht zum „Verantwortlichen" nach der DSGVO (siehe Punkt 2.3. Verantwortlichkeit und Auftragsverarbeitung).

7.2. Ist-Analyse und Erstellung Verarbeitungsverzeichnis

Das Verfahrensverzeichnis ist die Dokumentation über die tatsächlich stattfindenden Datenverarbeitungen in Ihrem Unternehmen. Überlegen Sie welche Kategorien an Daten Sie zu welchem Zweck erheben und an wen Sie diese Daten weitergeben und welche Fristen für die Löschung in Frage kommen.

Darauf basierend sollten die erforderlichen Umsetzungsschritte zur DSGVO, insbesondere die technischen und organisatorischen Maßnahmen im Rahmen der IT-Sicherheit, abgeleitet werden.

Auf wko.at/bstf/datenschutzimtourismus finden Sie branchenspezifische Muster-Verarbeitungsverzeichnisse, die Sie an Ihren Betrieb anpassen können.

7.3. Einholung Einwilligungserklärungen

Prüfen Sie, ob eine Rechtsgrundlage für eine Datenverarbeitung, wie bspw. ein Vertrag oder eine gesetzliche Verpflichtung, besteht. Ansonsten ist eine Einwilligungserklärung einzuholen.

Auf wko.at/bstf/datenschutzimtourismus finden Sie:

- Einwilligungserklärung zur Verarbeitung (sensibler) Daten samt zusätzlichen Angaben
- Einwilligungserklärung zu elektronischer Werbung
- Einwilligungserklärung zur Übermittlung von (sensiblen) Daten an „Drittanbieter" in unsicheren Drittstaaten

7.4. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Datenschutz durch Technologiegestaltung („privacy by design") ist primär Aufgabe der Software-Entwickler. Fragen Sie Ihre Entwickler bzw Lizenzgeber, wie der Grundsatz der Datenminimierung umgesetzt wurde.

Datenschutz durch datenminimierende Voreinstellungen („privacy by default") betrifft vor allem Benutzerschnittstellen im Internet und überall, wo Mitarbeiter

Daten von Kunden abfragen. Wir empfehlen eine systematische Überprüfung dieser Geschäftsbereiche, um die Abfrage nicht unbedingt nötiger Daten zu vermeiden.

Fragen Sie sich beispielsweise, ob wirklich jeder Mitarbeiter zu allen Daten Zugang haben muss, oder ob organisatorische Maßnahmen zur Vergabe von konkreten Benutzerrechten gesetzt werden können.

Siehe hier auch die Opt-In Varianten in den online abrufbaren Einwilligungserklärungen.

7.5. Erfüllung der Informationspflichten

Zur Erfüllung Ihrer Informationspflichten ist eine auf der eigenen Website leicht auffindbare (und nicht bloß im Impressum versteckte) Datenschutzerklärung eine häufig gewählte Lösung, ebenso eine zusätzliche Verlinkung in der E-Mail Signatur. Darüber hinaus kann die Datenschutzerklärung dem Betroffenen in Papierform (Informationsblätter) übergeben werden.

Branchenspezifische Beispiele für eine solche Datenschutzerklärung finden Sie auf wko.at/datenschutzimtourismus.

7.6. Umsetzung der Betroffenenrechte

Überlegen Sie sich wer in Ihrem Unternehmen der Ansprechpartner für Auskunfts-, Lösch- oder sonstige Anfragen Ihrer Gäste, Kunden oder sonstiger Betroffener ist. Wer kann und darf Anfragen beantworten?

Auskunftsersuchen sollten der Geschäftsführung und dem internen Datenschutzverantwortlichen sofort zur Kenntnis gebracht werden. Fristen für die Antwort sollten sofort erfasst und ein Zeitplan festgelegt werden. Die Form der Antwort (Schriftlichkeit) sollte definiert werden. Mündliche Auskünfte sollten selbst dann, wenn man überrumpelt wird, ausgeschlossen sein. Überlegen Sie: Wer leitet diese Prozesse im Alltagsbetrieb, wenn ein solcher Fall eintritt, und wer stimmt die Kommunikation intern und extern ab? Das setzt eine Vorbereitung der Geschäftsführung mit der IT-Abteilung und allenfalls auch Ihrem Rechtsberater voraus.

Es muss rechtzeitig definiert werden, in welchem Zeitraum mit welchen Informationen geantwortet wird. Testen Sie das richtige und rechtzeitige Reagieren! Legen Sie Prozesse und Verantwortlichkeiten fest, da ein Fehlverhalten leicht zu Anzeigen und damit verbundenen Strafen führen kann.

Mustervorlagen zur Auskunftserteilung finden Sie unter wko.at/datenschutzservice.

7.7. Vorgang bei Datenschutzverletzungen festlegen

Bei Datenschutzverletzungen muss umgehend, spätestens jedoch binnen 72 Stunden der Datenschutzbehörde und unter Umständen auch der betroffenen Person eine Erstmeldung erstattet werden. Weitere Meldungen können dann schrittweise erstattet werden (siehe Punkt 3.3. „Pflichten des Verantwortlichen und seines Auftragsverarbeiters). Ansonsten drohen Strafen, Reputationsverlust in der Öffentlichkeit und wirtschaftlicher Schaden. Es gilt daher vorab zu definieren wie Datenschutzvorfälle erkannt werden, einzustufen sind und wer im Team

verantwortlich ist, um im Notfall Entscheidungen zu treffen und die entsprechenden Schritte und Kommunikationen zu koordinieren. Sie hierzu auch:

Mustervorlagen für die Meldung an die Aufsichtsbehörde sowie für die Benachrichtigung der betroffenen Person ist abrufbar unter wko.at/datenschutzservice.