Datenschutz

Dieses Dokument wurde erstellt am 18.10.2019

Inhaltsverzeichnis

- Beschwerde bei der Datenschutzbehörde
- Online-Ratgeber und -Rechner
- Weiterführende Links
- Rechtsgrundlagen

Datenschutz

Aktuelle Informationen über Datenschutz, Datenschutz-Grundverordnung, DSGVO, Pflichten von Unternehmen, Datenverarbeitungsverzeichnis etc.

Information für Einsteiger

Seit 25. Mai 2018 gelten **umfassende neue Bestimmungen zum Datenschutz**. Bis zu diesem Datum mussten Unternehmen **alle Datenanwendungen an die neue Rechtslage anpassen**.

Unter anderem sind Verantwortliche und Auftragsverarbeiter verpflichtet, ein sogenanntes "Datenverarbeitungsverzeichnis" zu führen und verschiedene Maßnahmen zum Schutz personenbezogener Daten zu treffen.

In diesem Thema finden sich ausführliche Informationen zur geltenden Rechtslage.

Stand: 01.01.2019

Abgenommen durch:

- USP-Redaktion

Allgemeine Informationen zum Datenschutz

Hintergrund der geltenden Datenschutzbestimmungen ist, dass durch eine **EU-Verordnung** ein **einheitliches Datenschutzrecht für alle EU-Mitgliedstaaten** geschaffen wurde. Die EU-Verordnung räumt den Gesetzgebern der einzelnen Mitgliedstaaten einen gewissen Regelungsspielraum ein. In Österreich wurde dieser (unter anderem) durch den Beschluss des "Datenschutz-Anpassungsgesetzes 2018" und des "Datenschutz-Deregulierungs-Gesetzes 2018" ausgenützt.

In Österreich gelten die

- **EU-Datenschutz-Grundverordnung** (**DSGVO** – Verordnung (EU) 2016/679) sowie das
- österreichische **Datenschutzgesetz** (**DSG** – in der Fassung des Datenschutz-Anpassungsgesetzes 2018 und des Datenschutz-Deregulierungs-Gesetzes 2018).

HINWEIS Bei Verstößen gegen die Datenschutzbestimmungen, drohen hohe Geldstrafen.

Betroffene Unternehmen

Die neuen Datenschutzbestimmungen gelten für **alle Unternehmen**, die

- in irgendeiner Art und Weise personenbezogene Daten **verarbeiten** (Auftragsverarbeiter) oder
- über die **Zwecke und Mittel** der Verarbeitung solcher Daten **entscheiden** (Verantwortlicher).

Personenbezogene Daten sind z.B. Name, Adresse oder Geburtsdatum einer natürlichen Person.

Die Regelungen gelten **unabhängig von der Größe des Unternehmens** und daher sowohl für Ein-Personen-Unternehmen als auch für KMU und Großunternehmen.

Wesentliche Neuerungen

Im Folgenden werden die wichtigsten Neuerungen auszugsweise aufgelistet:

- **Keine DVR-Meldungen** (Datenverarbeitungsregister-Meldungen) mehr bei der Datenschutzbehörde
- Stattdessen **nachträgliche Kontrolle durch die Datenschutzbehörde**
- **Verstärkte Eigenverantwortung von Unternehmen** durch Regelung u.a. folgender Pflichten:
  - Führung eines Verzeichnisses von Verarbeitungstätigkeiten (sogenanntes

"Datenverarbeitungsverzeichnis")
    - **Maßnahmen** zum Schutz personenbezogener Daten (z.B. Verschlüsselung der Daten)
    - Zahlreiche **Informationspflichten**
    - **Meldung von Datenschutzverletzungen**
    - Bestellung eines **Datenschutzbeauftragten** (in bestimmten Fällen, z.B. bei umfangreicher Verarbeitung "sensibler Daten" als Kerntätigkeit des Unternehmens)
    - **Datenschutz-Folgenabschätzung** bei Verarbeitungen mit voraussichtlich hohem Risiko für die Rechte und Freiheiten natürlicher Personen
    - Ausführliche Informationen zum Thema "Pflichten von Unternehmen" finden sich auf USP.gv.at.
- Umfassende **Rechte von Betroffenen** (Recht auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Widerspruchsrecht etc.)
- Androhung **sehr hoher Strafen bei Verstößen** (Geldbußen von bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Konzernumsatzes, je nachdem, welcher Betrag höher ist)

Online-Ratgeber und -Rechner

- ≫ Datenschutz-Grundverordnung (DSGVO)
- ≫ Informationsverpflichtungen nach der Datenschutz-Grundverordnung

Weiterführende Links

- ≫ Kompakter Folder Datenschutz-Grundverordnung (WKO)
- ≫ EU-Datenschutz-Grundverordnung DSGVO (WKO)
- ≫ Checkliste zur DSGVO (WKO)

Rechtsgrundlagen

- ≫ Datenschutz-Grundverordnung (DSGVO)
- ≫ Datenschutzgesetz (DSG)
- ≫ Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (BGBl. II Nr. 108/2018)

Zum besseren Verständnis und zur leichteren Lesbarkeit gilt in diesem Text bei allen personenbezogenen Bezeichnungen die gewählte Form für beide Geschlechter.

Stand: 12.04.2019

Abgenommen durch:

- USP-Redaktion

Begriffsbestimmungen – Datenschutz

Die Datenschutzbestimmungen gelten für **alle Unternehmen**, die

- in irgendeiner Art und Weise **personenbezogene Daten verarbeiten** (Auftragsverarbeiter) oder
- über die Zwecke und Mittel der Verarbeitung solcher Daten **entscheiden** (Verantwortliche).

Zum besseren Verständnis werden nachfolgend die wichtigsten Begriffe aus der Datenschutz-Grundverordnung (DSGVO) erklärt.

Personenbezogene Daten

Als personenbezogene Daten gelten alle Informationen, die sich **auf eine identifizierte oder identifizierbare natürliche Person (sogenannte "betroffene Person") beziehen**.

Beispiele: Name, Adresse, Geburtsdatum, E-Mail-Adresse, IP-Adresse, Kontonummer, Kfz-Kennzeichen, Interessen und Vorlieben etc., aber auch Fotos von Personen

Die genannten Beispiele zählen zur **allgemeinen Kategorie** personenbezogener Daten.

Daneben gibt es auch besondere Kategorien personenbezogener Daten (sogenannte **"sensible Daten"**). Die DSGVO versteht darunter Daten, aus denen z.B. die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie z.B. Gesundheitsdaten oder Daten zur sexuellen Orientierung einer natürlichen Person. Diese Daten unterliegen einem besonderen Schutz.

Beispiele: Fingerabdruck, Krankengeschichte

Strafrechtsrelevante Daten dürfen nur unter sehr engen Voraussetzungen verarbeitet werden (z.B. unter behördlicher Aufsicht).

Beispiele: Strafurteil, Waffenverbot

Verarbeitung

Verarbeitung ist **jeder Umgang mit personenbezogenen Daten**. Dies kann sowohl mit als auch ohne Hilfe automatisierter Verfahren erfolgen. Verarbeitungsvorgänge sind z.B. das Erheben, Erfassen, Speichern, Verändern, Abfragen, Löschen oder Vernichten personenbezogener Daten.

Beispiele für die Verarbeitung: Erstellung und Wartung einer **Mitarbeiterdatenbank**, Erstellung und Wartung einer **Kundendatei**

Auftragsverarbeiter

Als Auftragsverarbeiter gilt jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten **im Auftrag des Verantwortlichen verarbeitet**. Nach dem derzeit geltenden Datenschutzrecht werden diese Personen als "Dienstleister" bezeichnet.

Verantwortlicher

Verantwortlicher ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die über die **Zwecke und Mittel** der Verarbeitung personenbezogener Daten **entscheidet**. Nach dem derzeit geltenden Datenschutzrecht werden diese Personen als "Auftraggeber" bezeichnet.

Pseudonymisierung

Der Begriff "Pseudonymisierung" steht für Datenverarbeitung in einer Weise, dass die personenbezogenen Daten ohne zusätzliche Informationen **nicht mehr einer bestimmten betroffenen Person zugeordnet werden können**. Die zusätzlichen Informationen müssen gesondert aufbewahrt werden und Maßnahmen unterliegen, die gewährleisten, dass die Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Beispiel: Namen von Kunden werden durch Zufallscodes ersetzt

Online-Ratgeber und -Rechner

- ≫ Datenschutz-Grundverordnung (DSGVO)
- ≫ Informationsverpflichtungen nach der Datenschutz-Grundverordnung

Weiterführende Links

- ≫ Kompakter Folder Datenschutz-Grundverordnung (WKO)
- ≫ EU-Datenschutz-Grundverordnung DSGVO (WKO)
- ≫ Checkliste zur DSGVO (WKO)

Rechtsgrundlagen

- ≫ Datenschutz-Grundverordnung (DSGVO)
- ≫ Datenschutzgesetz (DSG)

Zum besseren Verständnis und zur leichteren Lesbarkeit gilt in diesem Text bei allen personenbezogenen Bezeichnungen die gewählte Form für beide Geschlechter.

Stand: 12.04.2019

Abgenommen durch:

- USP-Redaktion

Rechtmäßige Datenverarbeitung und Grundsätze für die Verarbeitung – Datenschutz

Rechtmäßige Datenverarbeitung

Laut Datenschutz-Grundverordnung (DSGVO) ist eine Verarbeitung personenbezogener Daten **nur zulässig**, wenn **zumindest eine der folgenden Rechtsgrundlagen** vorliegt:

- **Einwilligung**
  Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden Daten gegeben.
  Beispiel: Zustimmung zum Erhalt eines Newsletters
  Ausführliche Informationen zum Thema "Einwilligung in die Datenverarbeitung" finden sich auf USP.gv.at.
- **Erfüllung eines Vertrags**
  Die Datenverarbeitung ist für die Erfüllung eines Vertrags mit der betroffenen Person erforderlich.
  Beispiel: Kundendatenbank eines Unternehmens
- **Erfüllung einer rechtlichen Verpflichtung**
  Die Datenverarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.
  Beispiele: Arbeitsrechtliche Pflichten des Arbeitgebers; Verpflichtungen einer Bank aufgrund des Bankwesengesetzes
- **Berechtigte Interessen des Verantwortlichen oder eines Dritten**
  Eine Datenverarbeitung ist auch dann rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Datenverarbeiters erforderlich ist außer die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (dies ist insbesondere bei Kindern anzunehmen). Es muss daher eine Interessenabwägung vorgenommen werden.
  Beispiel: Einholung einer Bonitätsauskunft durch eine Bank

HINWEIS Die DSGVO sieht neben den genannten Rechtsgrundlagen noch weitere vor.

Grundsätze für die Datenverarbeitung

Folgende Grundsätze müssen bei der Verarbeitung personenbezogener Daten immer beachtet werden:

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Personenbezogene Daten müssen **auf rechtmäßige Weise, nach Treu und Glauben** und in einer für die betroffene Person **nachvollziehbaren** Weise verarbeitet werden.

Zweckbindung

Eine **Erhebung** von Daten darf nur **für festgelegte, eindeutige und legitime Zwecke** erfolgen. Eine Weiterverarbeitung der Daten ist nur in einer mit diesen Zwecken zu vereinbarenden Weise erlaubt.

Datensparsamkeit ("Datenminimierung")

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sein. Darüber hinaus verlangt die DSGVO, dass sie **auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt** sind.

Richtigkeit

Personenbezogene Daten müssen **sachlich richtig** und erforderlichenfalls auf dem neuesten Stand sein. Es müssen alle angemessenen Maßnahmen getroffen werden, damit unrichtige Daten unverzüglich gelöscht oder berichtigt werden.

Speicherbegrenzung

Die **Speicherfrist** für personenbezogene Daten muss auf das **unbedingt erforderliche Mindestmaß** beschränkt bleiben. Um dies zu erfüllen, ist es ratsam, als Verantwortlicher Fristen für die Löschung oder regelmäßige Überprüfung der Daten vorzusehen.

Integrität und Vertraulichkeit

Die Art und Weise, in der personenbezogene Daten verarbeitet werden, muss eine **angemessene Sicherheit der Daten** gewährleisten (einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, vor unbeabsichtigtem Verlust, vor unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung).

Online-Ratgeber und -Rechner

- ≫ Datenschutz-Grundverordnung (DSGVO)
- ≫ Informationsverpflichtungen nach der Datenschutz-Grundverordnung

Weiterführende Links

- ≫ EU-Datenschutz-Grundverordnung (DSGVO): Grundsätze und Rechtmäßigkeit der Verarbeitung (WKO)
- ≫ EU-Datenschutz-Grundverordnung DSGVO (WKO)
- ≫ Checkliste zur DSGVO (WKO)

Rechtsgrundlagen

- ≫ Datenschutz-Grundverordnung (DSGVO)
- ≫ Datenschutzgesetz (DSG)

Zum besseren Verständnis und zur leichteren Lesbarkeit gilt in diesem Text bei allen personenbezogenen Bezeichnungen die gewählte Form für beide Geschlechter.

Stand: 12.04.2019

Abgenommen durch:

- USP-Redaktion

Pflichten von Unternehmen – Datenschutz

Die Datenschutz-Grundverordnung (DSGVO) beinhaltet verschiedene Pflichten für datenverarbeitende Unternehmen. Die wichtigsten Pflichten werden nachfolgend in ihren Grundzügen dargestellt.

Datenverarbeitungsverzeichnis

Verantwortliche sowie Auftragsverarbeiter müssen ein Verzeichnis all ihrer Datenverarbeitungstätigkeiten führen **(Datenverarbeitungsverzeichnis)**. Das Datenverarbeitungsverzeichnis muss laufend aktualisiert werden. Der Umfang der Dokumentationspflicht ist für den Auftragsverarbeiter geringer als für den Verantwortlichen.

Ausführliche Informationen zum Thema "Verzeichnis von Verarbeitungstätigkeiten" finden sich auf USP.gv.at.

Privacy by Design/Privacy by Default

"Privacy by Design" bedeutet **"Datenschutz durch Technikgestaltung"**: Schon während der Planung von Datenverarbeitungsvorgängen sowie bei der Datenverarbeitung selbst müssen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um einen **angemessenen Schutz der Daten** sicherzustellen.

Beispiel: Pseudonymisierung, Verschlüsselung personenbezogener Daten

"Privacy by Default" bedeutet **"Datenschutz durch datenschutzfreundliche Voreinstellungen"**: Der

Verantwortliche muss sicherstellen, dass durch Voreinstellung grundsätzlich **nur solche Daten**, deren Verarbeitung für den jeweiligen Zweck auch **wirklich erforderlich** ist, verarbeitet werden. Diese Verpflichtung entspricht einem der wichtigsten Datenschutzgrundsätze der DSGVO, der "Datenminimierung".

Beispiel: Reicht das Alter oder das Geburtsjahr einer Person für den Zweck der Datenverarbeitung aus, darf nicht auch das genaue Geburtsdatum verarbeitet werden.

Informationspflichten

Der Verantwortliche ist verpflichtet, **betroffenen Personen, deren Daten er erhebt**, bestimmte **Informationen** zukommen zu lassen.

Beispiele: Namen und Kontaktdaten des Verantwortlichen, Zwecke der Datenverarbeitung, Speicherdauer

Erhebt der Verantwortliche die Daten bei der Person selbst, muss er die Informationen zum Zeitpunkt der Erhebung der Daten zur Verfügung stellen. Werden die Daten nicht bei der betroffenen Person erhoben, genügt grundsätzlich eine Informationserteilung binnen angemessener Frist, spätestens jedoch innerhalb eines Monats ab Erlangung der Daten.

In der **Praxis** werden die Informationen häufig über **Datenschutzbestimmungen** oder **Datenschutzerklärungen (Privacy Policies)** erteilt.

Welche Informationen im konkreten Fall erteilt werden müssen, lässt sich mittels des am Ende dieser Seite verlinkten Online-Ratgebers "Datenschutz-Grundverordnung" herausfinden.

Meldung von Datenschutzverletzungen

Kommt es zu einer **Verletzung des Schutzes personenbezogener Daten**, ist der Verantwortliche grundsätzlich verpflichtet, diese Verletzung sowohl der **Datenschutzbehörde** als auch (bei voraussichtlich hohem Risiko) der **betroffenen Person** zu **melden**.

Eine solche Datenschutzverletzung wird definiert als eine Verletzung der Sicherheit, die zur **Vernichtung**, zum **Verlust**, zur **Veränderung** oder zur **unbefugten Offenlegung** von beziehungsweise zum **unbefugten Zugang** zu personenbezogenen Daten führt.

Beispiele: Verlust eines Datenträgers, auf dem Kundendaten gespeichert sind; Hackerangriff

Wenn dem Auftragsverarbeiter eine Datenschutzverletzung bekannt wird, muss er diese dem Verantwortlichen unverzüglich melden.

Die Meldung der Datenschutzverletzung durch den Verantwortlichen an die **Datenschutzbehörde** muss **unverzüglich** und **möglichst binnen 72 Stunden** ab Kenntnis der Verletzung erfolgen.

Die Meldung der Verletzung an die **betroffene Person** muss **unverzüglich** und in klarer und einfacher Sprache erfolgen.

Ausführliche Muster für Meldungen an die Datenschutzbehörde bzw. betroffene Personensind am Ende dieser Seite abrufbar.

Datenschutzbeauftragter

In folgenden Fällen besteht eine **Verpflichtung** für Unternehmen, einen eigenen Datenschutzbeauftragten zu bestellen:

- Kerntätigkeit des Unternehmens ist:
    - Eine umfangreiche regelmäßige und systematische Überwachung von Personen (z.B. Berufsdetektive) **oder**
    - Eine umfangreiche Verarbeitung "sensibler Daten" (z.B. Krankenhäuser) oder von Daten über strafrechtliche Verurteilungen oder Straftaten

Liegt keiner dieser Fälle vor, können der Verantwortliche oder der Auftragsverarbeiter auch **freiwillig** einen Datenschutzbeauftragten benennen.

Aufgaben des Datenschutzbeauftragten sind u.a. die **Unterrichtung und Beratung** des Unternehmens und der Beschäftigten sowie die Überwachung der **Einhaltung** der Datenschutzvorschriften.

Datenschutz-Folgenabschätzung

HINWEIS Die **Datenschutzbehörde** hat eine **Verordnung** erlassen, in der jene Datenverarbeitungen angeführt sind, die von der Pflicht zur Datenschutz-Folgenabschätzung **ausgenommen** sind (sogenannte **"white list"** – siehe Link ganz unten).

Gehen Vorgänge der Datenverarbeitung **voraussichtlich** mit einem **hohen Risiko für die Rechte und Freiheiten natürlicher Personen** einher, muss der Verantwortliche noch **vor** der Verarbeitung eine sogenannte "Datenschutz-Folgenabschätzung" durchführen. Besteht voraussichtlich kein solches hohes Risiko, kann eine Datenschutz-Folgenabschätzung unterbleiben.

Beispiel für Pflicht zur Datenschutz-Folgenabschätzung: Umfangreiche Verarbeitung von Gesundheitsdaten oder von Daten über strafrechtliche Verurteilungen und Straftaten

Ergibt die Datenschutz-Folgenabschätzung, dass die Verarbeitung ein hohes Risiko zur Folge hätte, muss der Verantwortliche grundsätzlich noch **vor** der Verarbeitung die **Datenschutzbehörde konsultieren**.

Online-Ratgeber und -Rechner

- ≫ Datenschutz-Grundverordnung (DSGVO)
- ≫ Informationsverpflichtungen nach der Datenschutz-Grundverordnung

Weiterführende Links

- ≫ Meldung an die Datenschutzbehörde – Muster (WKO)
- ≫ Meldung an die Datenschutzbehörde – Ausgefülltes Beispiel (WKO)
- ≫ Benachrichtigung der betroffenen Person – Muster (WKO)
- ≫ Benachrichtigung der betroffenen Person – Ausgefülltes Beispiel (WKO)
- ≫ EU-Datenschutz-Grundverordnung DSGVO (WKO)
- ≫ Checkliste zur DSGVO (WKO)

Rechtsgrundlagen

- ≫ Datenschutz-Grundverordnung (DSGVO)
- ≫ Datenschutzgesetz (DSG)
- ≫ Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (BGBl. II Nr. 108/2018)

Zum besseren Verständnis und zur leichteren Lesbarkeit gilt in diesem Text bei allen personenbezogenen Bezeichnungen die gewählte Form für beide Geschlechter.

Stand: 12.04.2019

Abgenommen durch:

- USP-Redaktion

Verzeichnis von Verarbeitungstätigkeiten – Datenschutz

Die **Pflicht zur Erstattung von DVR-Meldungen** (Meldungen an das Datenverarbeitungsregister der Datenschutzbehörde) ist **entfallen**. Registrierungen im DVR wurden gegenstandslos.

Stattdessen müssen Verantwortliche sowie Auftragsverarbeiter ein Verzeichnis all ihrer Datenverarbeitungstätigkeiten führen **(Datenverarbeitungsverzeichnis)**. Das Verzeichnis muss schriftlich (einschließlich elektronisch) geführt werden. Es muss laufend aktualisiert werden. Der Umfang der Dokumentationspflicht ist für den Auftragsverarbeiter

geringer als für den Verantwortlichen.

Verantwortliche

Das Datenverarbeitungsverzeichnis eines Verantwortlichen betrifft sämtliche Verarbeitungstätigkeiten, die in seiner Zuständigkeit liegen. Das Verzeichnis muss Folgendes enthalten:

- **Namen und Kontaktdaten**
  - Des **Verantwortlichen**
  - Des etwaigen **Vertreters** des Verantwortlichen
  - Eines etwaigen **Datenschutzbeauftragten**
- **Zwecke** jeder einzelnen Datenverarbeitung
- Kategorien **betroffener Personen** (z.B. Kunden)
- Kategorien **verarbeiteter Daten** (z.B. Adressdaten)
- Kategorien von **Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt wurden oder noch offengelegt werden (z.B. Sozialversicherung oder Finanzamt), einschließlich Empfängerinnen/Empfänger in Drittstaaten (z.B. USA) oder internationalen Organisationen
- **Gegebenenfalls Übermittlungen** von personenbezogenen Daten **an einen Drittstaat oder an eine internationale Organisation**, einschließlich der Angabe des Drittstaates oder der internationalen Organisation
- **Nach Möglichkeit: Aufbewahrungsdauer** der verschiedenen Datenkategorien
- **Nach Möglichkeit:** Allgemeine Beschreibung der **Maßnahmen** zum Schutz personenbezogener Daten (z.B. Verschlüsselung der Daten)

Ausführliche Muster und ausgefüllte Beispiele von Datenverarbeitungsverzeichnissen sind am Ende dieser Seite abrufbar.

Auftragsverarbeiter

Das Datenverarbeitungsverzeichnis eines Auftragsverarbeiters betrifft sämtliche Verarbeitungstätigkeiten, die im Auftrag eines Verantwortlichen durchgeführt werden. Das Verzeichnis muss Folgendes enthalten:

- **Namen und Kontaktdaten**
  - Des **Auftragsverarbeiters**
  - Der **Verantwortlichen**, in deren Auftrag der Auftragsverarbeiter tätig ist
  - Des etwaigen **Vertreters** des Verantwortlichen oder des Auftragsverarbeiters
  - Eines etwaigen **Datenschutzbeauftragten**
- **Kategorien von Verarbeitungen**, die im Auftrag jedes Verantwortlichen durchgeführt werden
- **Gegebenenfalls Übermittlungen** von personenbezogenen Daten **an einen Drittstaat (z.B. USA) oder an eine internationale Organisation**, einschließlich der Angabe des Drittstaates oder der internationalen Organisation
- **Nach Möglichkeit:** Allgemeine Beschreibung der **Maßnahmen** zum Schutz personenbezogener Daten (z.B. Verschlüsselung der Daten)

Ausführliche Muster und ausgefüllte Beispiele von Datenverarbeitungsverzeichnissen sind am Ende dieser Seite abrufbar.

Zusammenarbeit mit der Aufsichtsbehörde

Verantwortliche und Auftragsverarbeiter sind verpflichtet, bei der Erfüllung ihrer Aufgaben mit der Aufsichtsbehörde (das ist die Datenschutzbehörde) zusammenzuarbeiten. Auf Anfrage müssen sie der Behörde die Datenverarbeitungsverzeichnisse vorlegen.

Online-Ratgeber und -Rechner

- ≫ Datenschutz-Grundverordnung (DSGVO)
- ≫ Informationsverpflichtungen nach der Datenschutz-Grundverordnung

Weiterführende Links

- ≫ Datenverarbeitungsverzeichnis für Verantwortliche – Muster (WKO)
- ≫ Datenverarbeitungsverzeichnis für Verantwortliche – Ausgefülltes Beispiel (WKO)
- ≫ Datenverarbeitungsverzeichnis für Auftragsverarbeiter – Muster (WKO)

- ≫ Datenverarbeitungsverzeichnis für Auftragsverarbeiter – Ausgefülltes Beispiel (WKO)
- ≫ EU-Datenschutz-Grundverordnung DSGVO (WKO)
- ≫ Checkliste zur DSGVO (WKO)

Rechtsgrundlagen

- ≫ Datenschutz-Grundverordnung (DSGVO)
- ≫ Datenschutzgesetz (DSG)

Zum besseren Verständnis und zur leichteren Lesbarkeit gilt in diesem Text bei allen personenbezogenen Bezeichnungen die gewählte Form für beide Geschlechter.

Stand: 12.04.2019

Abgenommen durch:

- USP-Redaktion

Einwilligung in die Datenverarbeitung – Datenschutz

Die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn sie sich auf eine der in der Datenschutz-Grundverordnung (DSGVO) genannten Rechtsgrundlagen stützt. Eine in der Praxis häufig vorkommende Rechtsgrundlage ist die **Einwilligung der betroffenen Person zu der Verarbeitung der sie betreffenden Daten**.

Beispiel: Zustimmung zum Erhalt eines Newsletters

Eine datenschutzrechtliche Einwilligung ist **unter folgenden Voraussetzungen zulässig**:

- **Freiwilligkeit**
  Die betroffene Person muss freiwillig, d.h. ohne Zwang und aufgrund freier Entscheidung, in die Verarbeitung ihrer Daten einwilligen. Ein Verstoß gegen dieses Prinzip liegt z.B. dann vor, wenn ein Vertragsabschluss von der Einwilligung zur Zusendung von Werbung abhängig gemacht wird (sogenanntes "Koppelungsverbot").
- **Form**
  Eine Einwilligung kann schriftlich, mündlich, elektronisch oder auch ≫ konkludent erfolgen. Bloßes Stillschweigen ohne zusätzliche Zeichen stellt keine gültige Einwilligung dar. Für die Verarbeitung "sensibler Daten" ist eine ausdrückliche Einwilligungserklärung erforderlich.
  Beispiel für eine elektronisch abgegebene Einwilligungserklärung: Anklicken eines Kästchens zu einer vorformulierten Einwilligungserklärung auf einer Website
  ACHTUNG: Die Einwilligung muss aktiv erfolgen. Ist ein Kästchen bereits vorangeklickt, liegt keine gültige Einwilligung vor!
- **Umfassende Information**
  Die betroffene Person (z.B. der Empfänger eines Newsletters) muss im Zuge der Abgabe der Einwilligungserklärung folgende Informationen erhalten:
  - Daten, die verarbeitet werden (z.B. Name, Geburtsdatum, Adresse)
  - Zweck der Datenverarbeitung (z.B. Übermittlung eines monatlichen Newsletters mit dem Inhalt XY per E-Mail); ACHTUNG: Wenn die Verarbeitung mehreren Zwecken dient, sollte für jeden dieser Verarbeitungszwecke eine eigene Einwilligung gegeben werden!
  - Etwaige dritte Datenempfänger
  - Recht der betroffenen Person, die Einwilligung jederzeit zu widerrufen
- **Verständlichkeit, leichte Zugänglichkeit, klare und einfache Sprache**
  Eine vorformulierte Einwilligungserklärung muss in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden.

TIPP Aus Beweisgründen wird empfohlen, entweder schriftliche oder auf andere Art nachweisbare Einwilligungserklärungen einzuholen.

Einwilligungserklärungen in AGB

Allgemeine Geschäftsbedingungen (AGB) enthalten üblicherweise viele verschiedene Bestimmungen, unter anderem

z.B. zu Lieferbedingungen, Gewährleistungsrechten von Kunden etc.

Es wird empfohlen, (vorformulierte) Einwilligungserklärungen **nicht** in Allgemeine Geschäftsbedingungen zu integrieren. Stattdessen sollten zusätzlich zu den AGB **separate Einwilligungen** der betroffenen Personen eingeholt werden. Der Grund dafür ist, dass eine in AGB enthaltene Einwilligungserklärung gegen das Prinzip der Freiwilligkeit verstoßen könnte (Koppelungsverbot).

Bestehende Einwilligungserklärungen

Wenn bestehende Einwilligungserklärungen (nach dem "alten", bis 24. Mai 2018 geltenden Datenschutzrecht) auch noch ab 25. Mai 2018 datenschutzkonform sind, d.h. der **neuen Rechtslage entsprechen**, sind sie **weiterhin gültig**.

Wenn dies jedoch **nicht** der Fall ist, müssen die bisher verwendeten Einwilligungserklärungen **angepasst** werden. D.h. es müssen **neue Zustimmungserklärungen** der betroffenen Personen eingeholt werden.

Beispiel: Wenn eine Person bei Abgabe der Einwilligungserklärung nicht über ihr jederzeitiges Widerrufsrecht informiert wurde, muss von ihr eine neue Zustimmung zur Datenverarbeitung eingeholt werden.

Online-Ratgeber und -Rechner

- ≫ Datenschutz-Grundverordnung (DSGVO)
- ≫ Informationsverpflichtungen nach der Datenschutz-Grundverordnung

Weiterführende Links

- ≫ EU-Datenschutz-Grundverordnung (DSGVO): Einwilligungserklärung (WKO)
- ≫ Einwilligung / Rechtmäßigkeit der Verarbeitung nach EU-Datenschutz-Grundverordnung – FAQ (WKO)
- ≫ EU-Datenschutz-Grundverordnung FAQ (WKO)
- ≫ Checkliste zur DSGVO (WKO)

Rechtsgrundlagen

- ≫ Datenschutz-Grundverordnung (DSGVO)
- ≫ Datenschutzgesetz (DSG)

Zum besseren Verständnis und zur leichteren Lesbarkeit gilt in diesem Text bei allen personenbezogenen Bezeichnungen die gewählte Form für beide Geschlechter.

Stand: 12.04.2019

Abgenommen durch:

- USP-Redaktion

Rechte von Betroffenen – Datenschutz

Rechte aufgrund von Informationspflichten von Unternehmen

Der Verantwortliche ist verpflichtet, **betroffenen Personen, deren Daten er erhebt**, bestimmte **Informationen** zukommen zu lassen (z.B. Namen und Kontaktdaten des Verantwortlichen, Zwecke der Datenverarbeitung, Speicherdauer etc.). Nähere Informationen zum Thema "Informationspflichten" finden sich auf USP.gv.at.

Darüber hinaus legt die Datenschutz-Grundverordnung (DSGVO) verschiedene Rechte betroffener Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten fest. Der Verantwortliche muss geeignete Maßnahmen treffen, um der betroffenen Person alle Informationen und alle Mitteilungen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Im Folgenden werden die Rechte von Betroffenen in ihren Grundzügen dargestellt.

Recht auf Auskunft

Jeder Betroffene kann vom Verantwortlichen Auskunft darüber verlangen, **ob**, und **wenn ja, welche** ihn betreffende **personenbezogene Daten** verarbeitet werden. Dies ist jederzeit und ohne Begründung möglich.

Der Verantwortliche muss im Zuge der Auskunftserteilung **Kopien der verarbeiteten Daten** zur Verfügung stellen (z.B. E-Mails, Auszüge aus Datenbanken etc.). **Informieren** muss er **unter anderem** über die Verarbeitungszwecke, die Kategorien der Daten, die verarbeitet werden, die Empfänger der Daten, sowie, wenn möglich, die geplante Speicherdauer.

Die Auskunft kann **formlos** beantragt werden. Sie ist **grundsätzlich kostenlos**, sofern die betroffene Person nicht mehr als eine Datenkopie verlangt.

Recht auf Löschung ("Recht auf Vergessenwerden")

Die betroffene Person hat das Recht, vom Verantwortlichen die **unverzügliche Löschung** der sie betreffenden Daten zu verlangen. Der Verantwortliche muss die Löschung unverzüglich durchführen, wenn **einer der folgenden Gründe** vorliegt:

- Die Daten sind nicht mehr erforderlich
- Die betroffene Person hat ihre Einwilligung widerrufen
- Die betroffene Person hat Widerspruch gegen die Verarbeitung eingelegt
- Die Daten wurden unrechtmäßig verarbeitet
- Die Löschung der Daten ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich

Ein unbegründetes Recht auf Löschung besteht daher nicht. Die Löschung wird durch einen **formlosen Antrag** verlangt. Sie ist **grundsätzlich kostenlos**.

Ausführliche Informationen zum Thema "≫ Recht auf Löschung bei Google, Bing, Yahoo etc." finden sich auf oesterreich.gv.at.

Recht auf Berichtigung

Die betroffene Person kann vom Verantwortlichen die **unverzügliche Berichtigung** und/oder die **Vervollständigung** der sie betreffenden Daten verlangen.

Beispiel: Falsche Wohnadresse

Die Berichtigung wird durch einen **formlosen Antrag** verlangt. Sie ist **grundsätzlich kostenlos**.

Weitere Rechte

Neben den genannten – in der Praxis wichtigsten – Rechten von Betroffenen sieht die DSGVO auch ein **Recht auf Einschränkung der Datenverarbeitung** vor. Die Einschränkung kann mit Begründung verlangt werden (z.B. Widerspruch der betroffenen Person gegen die Verarbeitung). Darüber hinaus kommt Betroffenen ein **Recht auf Datenübertragbarkeit** (Recht auf Erhalt und – sofern technisch machbar – Übermittlung der Daten an einen anderen Verantwortlichen) sowie ein **Widerspruchsrecht** (Recht auf Widerspruch gegen die Verarbeitung der Daten) zu.

Fristen für den Verantwortlichen

Antragsrechte

Macht eine betroffene Person von einem der genannten Antragsrechte Gebrauch (Recht auf Auskunft, Löschung, Berichtigung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch), muss der Verantwortliche **unverzüglich**, in jedem Fall aber **innerhalb eines Monats** nach Eingang der Anfrage antworten. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist.

Informationspflicht

Erhebt der Verantwortliche die Daten **bei der Person selbst**, muss er die Informationen zum **Zeitpunkt der Erhebung** der Daten zur Verfügung stellen. Werden die Daten **nicht bei der betroffenen Person** erhoben, genügt

grundsätzlich eine Informationserteilung binnen **angemessener Frist**, spätestens jedoch innerhalb eines Monats ab Erlangung der Daten.

Beschwerde bei der Datenschutzbehörde

Im Falle einer behaupteten Rechtsverletzung kann jede betroffene Person **innerhalb eines Jahres** ab Kenntnis von dem beschwerenden Ereignis eine Beschwerde bei der Datenschutzbehörde einbringen. Das Bundesverwaltungsgericht entscheidet über Beschwerden gegen Bescheide der Datenschutzbehörde. Auch im Falle der Verletzung der Entscheidungspflicht der Datenschutzbehörde (Säumnis) ist das Bundesverwaltungsgericht zuständig.

Online-Ratgeber und -Rechner

- ≫ Datenschutz-Grundverordnung (DSGVO)
- ≫ Informationsverpflichtungen nach der Datenschutz-Grundverordnung

Weiterführende Links

- ≫ EU-Datenschutz-Grundverordnung (DSGVO): Betroffenenrechte (WKO)
- ≫ Österreichische Datenschutzbehörde
- ≫ EU-Datenschutz-Grundverordnung DSGVO (WKO)
- ≫ Checkliste zur DSGVO (WKO)

Rechtsgrundlagen

- ≫ Datenschutz-Grundverordnung (DSGVO)
- ≫ Datenschutzgesetz (DSG)

Zum besseren Verständnis und zur leichteren Lesbarkeit gilt in diesem Text bei allen personenbezogenen Bezeichnungen die gewählte Form für beide Geschlechter.

Stand: 12.04.2019

Abgenommen durch:

- USP-Redaktion