

*Ausfüllhilfe*

*zum*

Datenverarbeitungsverzeichnis

# nach Art 30 Abs 1 Datenschutz- Grundverordnung (DSGVO)

Zu jeder Überschrift des Musters enthält diese Ausfüllhilfe eine kurze Erläuterung, die zur besseren Unterscheidung in Kursiv gedruckt ist.

# Deckblatt

Das Deckblatt dient als Übersicht/Inhaltsverzeichnis und hat keine selbstständige rechtliche Bedeutung.

Zu beachten ist, dass alle Geschäftsprozesse, bei denen personenbezogene Daten verarbeitet werden, vollständig erfasst und gegebenenfalls aktualisiert werden.

Der Detaillierungsgrad, in dem die Geschäftsprozesse gegliedert werden, ist gesetzlich nicht vorgegeben. Bei der im Muster gewählten Darstellung wird der Informationsgehalt auf das tatsächlich notwendige Ausmaß (zzgl. einiger „praktischer“ Informationen) beschränkt.

Aus Transparenzgründen sollten alle Versionen des Verzeichnisses mit Datum und Unterschrift dokumentiert werden.

# Allgemeine Informationen

Die verpflichtenden (Mindest-)Angaben eines Verarbeitungsverzeichnisses ergeben sich für Verantwortliche aus Art 30 Abs 1 DSGVO.

Jede „Organisation“ (dh auch jedes Unternehmen, gleich welcher Rechtsform) muss ein gesondertes Verarbeitungsverzeichnis erstellen, wenn die Verarbeitung von personenbezogenen Daten natürlicher Personen nicht nur gelegentlich stattfindet. Das wird bei nahezu allen Unternehmen, die wirtschaftlich tätig sind, der Fall sein, sodass davon auszugehen ist, dass alle Unternehmen verpflichtet sind, diese datenschutzrechtliche Dokumentation zu erstellen.

Verantwortlicher iSd DSGVO ist dann die Organisation, dh das Unternehmen, zB die GmbH, die OG, die KG oder auch das Einzelunternehmen, welches über Zweck und Mittel der Verarbeitung der Daten entscheidet, dh personenbezogene Daten von natürlichen Personen zur Erfüllung der unternehmerischen Aufgaben verarbeitet.

Letztlich bleibt es dem Verantwortlichen vorbehalten, weitere, über dieses Mindestmaß hinausgehende Informationen in das Verzeichnis mitaufzunehmen.

Ein detailliertes Verzeichnis hat den praktischen Vorteil, dass es dem Verantwortlichen einen guten Überblick über die Verarbeitungsvorgänge in seinem Unternehmen bieten kann. Ein Nachteil bei einem detaillierten Verzeichnis kann der mit der Erstellung und der laufenden Aktualisierung verbundene hohe Arbeitsaufwand sein. Darüber hinaus besteht die „Gefahr“, dass das Verzeichnis, z.B. wenn dieses der Behörde vorgelegt werden muss, diese leichter auf „Unstimmigkeiten“ oder Fehler aufmerksam werden kann, als wenn sich das Verzeichnis auf das Mindestmaß beschränkt.

Das vorliegende Muster ist weitestgehend auf das gesetzlich notwendige Ausmaß beschränkt, wobei sich teils auch darüber hinausgehende Informationen (z.B. indem nicht nur die Kategorien der personenbezogenen Daten, sondern tatsächlich sämtliche Daten angegeben werden) wiederfinden.

Der Verantwortliche hat auch die Möglichkeit, parallel zu diesem „knappen“ Verzeichnis und detaillierteres für rein interne Zwecke zu führen, sofern dies gewünscht ist.

Grundsätzlich können in detailliertere Verzeichnisse z.B. noch nachfolgende, weitergehende Informationen mitaufgenommen werden:

Angabe der einzelnen (Fach-)Abteilungen (ggf mit einem Ansprechpartner) bei den einzelnen Datenverarbeitungen; allgemeine Informationen zur Datenschutz-Folgenabschätzung (wurde eine solche durchgeführt, wenn ja, warum); Angaben zu den Rechtsgrundlagen der einzelnen Datenverarbeitungen; Angaben zur Herkunft der einzelnen Daten, etc.

Hier können praktische alle „nützlichen“ und relevanten Informationen mitaufgenommen werden.

# Stammdaten

Nachfolgende Angaben sind zunächst in ein „Stammdatenblatt“ einzufügen:

## Verantwortlicher

Der „Verantwortliche“ iSd DSGVO ist im Verzeichnis zu nennen. Die Unternehmensbezeichnung muss der Firma (sofern im Firmenbuch eingetragen) oder der konkreten Geschäftsbezeichnung (mit Angabe der Namen der natürlichen Person bei einem nicht eingetragenen Einzelunternehmen) entsprechen, um Verwechslungen zu verhindern.

Es sind Name und die Kontaktdaten des Verantwortlichen (bzw. der „gemeinsam“ Verantwortlichen) anzugeben.

Nach § 9 VStG haften alle Geschäftsführer für die Einhaltung der Verwaltungsgesetze, dh auch des DSG. Um zu vermeiden, dass im Fall einer Rechtsverletzung alle Geschäftsführer bestraft werden, sollte die Geschäftseinteilung vorsehen, dass nur einer von mehreren Geschäftsführern für Belange des Datenschutzes zuständig ist.

Die Haftung des Geschäftsführers besteht unabhängig von der Bestellung eines Datenschutzbeauftragten.

## Datenschutzbeauftragter

Ob eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht, ergibt sich aus Art 37 DSGVO (siehe Allgemeiner Teil).

# 

# Verarbeitungsprozesse

In weiterer Folge sollte eine Gliederung nach den einzelnen Verarbeitungsprozessen im Unternehmen erfolgen, wobei bei jedem Verarbeitungsprozess zumindest nachfolgende Angaben enthalten sein sollen:

## Verfahren

#### Bezeichnung:

Der Verarbeitungsprozess soll eine Kurzbezeichnung erhalten, die sich aus der Tätigkeit an sich ergibt.

## Zweckbestimmung

Die Zweckbestimmung des Verarbeitungsprozesses ist möglichst vollständig und präzise anzugeben.

## Details zur Datenverarbeitung

### Betroffene Personen

Die betroffenen Personen sind in typische Kategorien zu gliedern. Das dient einer genaueren Zuordnung der Datenkategorien (siehe unten). Betroffene Personen, die besonders schutzwürdig sind, wie Kinder, Kranke, Personen mit besonderen Bedürfnissen, sind hervorzuheben, damit die technisch-organisatorischen Maßnahmen darauf Rücksicht nehmen können.

Der Anwendungsbereich der DSGVO bezieht sich nur auf natürliche Personen, wobei zB auch Ansprechpartner bei juristischen Personen (die zB in der Korrespondenz oder in E-Mail-Adressen identifiziert werden) dazu zählen.

### Datenverwendung & Weitergabe

Weitergabe bedeutet die Übermittlung oder Bereitstellung von Daten über eine betroffene Person an jemanden, der vom Verantwortlichen und vom Betroffenen verschieden ist. Der Adressat einer Nachricht (Brief, E-Mail etc) ist daher Betroffener und nicht Empfänger einer Weitergabe, ebenso wie Dienstleister, die für den Verantwortlichen tätig sind, zB der Internetprovider, eine Steuerberatung oder Rechtsanwaltskanzlei und auch eine Behörde (zB bei der notwendigen Weitergabe von Meldedaten durch Beherbergungsbetriebe).

#### Verwendung intern

Die Weitergabe von Daten an andere Abteilungen des Unternehmens ist zu dokumentieren. Die Abteilung, die für den Prozess hauptverantwortlich ist, ist daher nicht mehr anzuführen.

Der Rechtsgrund muss Art 6 DSGVO entsprechen. Einwilligung darf nur angeführt werden, wenn diese den Vorgaben des Art 7 DSGVO entspricht (siehe Allgemeiner Teil). Der Rechtsgrund einer positiven Interessensabwägung (beim berechtigten Interesse) darf nur angegeben werden, wenn transparent gemacht wird, welche Interessen gegeneinander abgewogen werden.

#### Weitergabe extern

Die Weitergabe an Dritte (außerhalb des Unternehmens) mit Sitz in der EU wird hier eingetragen.

#### Weitergabe Drittstaaten

Hier werden Übermittlungen an Dritte mit Sitz in Staaten außerhalb der EU angeführt, und zwar unabhängig davon, ob der Staat ein angemessenes Schutzniveau gewährleistet oder nicht. Das Schutzniveau im Drittland wirkt sich nur auf die Voraussetzungen für die Zulässigkeit der Übermittlung aus. Bei der Weitergabe von personenbezogene Daten an Empfänger in sog. unsichere Drittländer sind besondere Vorkehrungen iSd Art 44 ff. DSGVO notwendig, damit diese Weitergabe zulässig ist, oder es müssen Ausnahmen des Art 49 DSGVO erfüllt sein.

### Auftragsverarbeiter

Es können ein oder mehrere Auftragsverarbeiter angeführt werden, die für den Verantwortlichen Teile von Verarbeitungstätigkeiten ausführen (zB Speicherung von Daten bei Cloud-Anbietern, die Übermittlung von Daten durch Internet- oder E-Mailprovider oder der Versand von Newslettern durch einen Anbieter eines Newsletter-Tools).

## Datenkategorien

### Gliederung

Die Datenkategorien werden getrennt nach den Kategorien von Betroffenen dargestellt, um mögliche Unterschiede leichter zu erkennen.

Nicht jede technische Informationseinheit (Datenfeld) muss als Datenkategorie gesondert angeführt werden. Es sollen aber nur solche Daten zu einer Kategorie zusammengefasst werden, die bezüglich Weitergabe und der Rechtsgrundlage der Verarbeitung gleich zu behandeln sind. Unter Kontaktdaten werden zB Telefonnummern, E- Mail-Adressen, Skype-Nummern etc zusammengefasst.

### Löschfristen

Für die Löschfristen können keine allgemein gültigen Werte angegeben werden. Gesetzliche Aufbewahrungspflichten sind jedenfalls die Untergrenze für die Speicherdauer, ohne triftige Begründung einer längeren Speicherung aber auch die Obergrenze.

Die gesetzlichen Aufbewahrungsfristen sind im Muster als Löschfrist vorausgefüllt, eine Verlängerung ist aber – bei entsprechender Begründung denkbar. Weitere gesetzliche Verjährungs- und Präklusionsfristen und eine FAQ-Liste zum Löschen hat die WKO folgenden Dokumenten zusammengefasst:

#### [https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und- aufbewahrungsfristen.html](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html)

* + - [https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo- aufbewahrungsfristen-loeschung-faq.html](https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-aufbewahrungsfristen-loeschung-faq.html)

Für alle Daten, die mit Vertragsbeziehungen im Zusammenhang stehen, kann die Verjährungsfrist für Schadenersatzansprüche von 3 Jahren (§ 1489 ABGB) als Untergrenze gelten. Im Hinblick auf das Risiko verborgener Mängel bzw einer späten Erkennbarkeit eines Schadens, wird eine Verlängerung um 1 bis 2 Jahre vertretbar sein.

Diese Frist beginnt mit dem Ende der Vertragserfüllung, dh z.B. mit Ende der gebuchten Reise oder Ende der Fitnesscenter-Mitgliedschaft, zu laufen.

Mit Einwilligung des Betroffenen können auch längere Löschfristen vorgesehen werden.

# Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

In einem „letzten“ Teil sollte sodann noch eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen erfolgen:

Gemäß Art 30 Abs 1 lit g DSGVO hat der Verantwortliche nach Möglichkeit eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art 32 Abs 1 DSGVO in das Verzeichnis der Verarbeitungstätigkeiten aufzunehmen. Dabei hat der Verantwortliche grundsätzlich je nach Einzelfall und entsprechend den mit den Datenverarbeitungen verbundenen Risiken selbst zu entscheiden, welche zumutbaren, technischen und organisatorischen Maßnahmen er ergreift. Nach Art 32 Abs 1 lit a bis d DSGVO müssen diese Maßnahmen miteinschließen:

* die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
* die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
* die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
* ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Im vorliegenden Muster wurden hinsichtlich der technischen und organisatorischen Maßnahmen die Kategorien Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit, Pseudonymisierung und Verschlüsselung sowie Evaluierungsmaßnahmen festgelegt. Das Verzeichnis sollte jedenfalls eine auf den Einzelfall bezogene, allgemeine Beschreibung der konkret ergriffenen Maßnahmen enthalten.

# 