

EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

BEISPIEL EINES DATENVERARBEITUNGSVERZEICHNIS NACH ART. 30 ABS. 2 EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO) (AUFTRAGSVERARBEITER)

Die Experten der Wirtschaftskammern Österreichs haben für ihre Mitgliedsbetriebe nachstehendes Beispiel eines Datenverarbeitungsverzeichnisses nach Art. 30 Abs. 2 EU-Datenschutz-Grundverordnung (DSGVO) für Auftragsverarbeiter nach dem Vorbild des im Download-Bereich verfügbaren Muster, erstellt.

Es handelt sich um ein fiktives Beispiel. Bei der praktischen Umsetzung ist auf die konkreten Anwendungsfälle im Unternehmen abzustellen.

Das hinterlegte Wasserzeichen „Beispiel“ kann einfach aus dem Word-Dokument entfernt werden.

Stand: Mai 2024

Dies ist ein Produkt der Zusammenarbeit aller Wirtschaftskammern.

Bei Fragen wenden Sie sich bitte an die Wirtschaftskammer Ihres Bundeslandes:

Burgenland, Tel. Nr.: 05 90907, Kärnten, Tel. Nr.: 05 90904, Niederösterreich Tel. Nr.: (02742) 851-0,
Oberösterreich, Tel. Nr.: 05 90909, Salzburg, Tel. Nr.: (0662) 8888-0, Steiermark, Tel. Nr.: (0316) 601-0,
Tirol, Tel. Nr.: 05 90905-1111, Vorarlberg, Tel. Nr.: (05522) 305-0, Wien, Tel. Nr.: (01) 51450-1010.

Hinweis! Diese Information finden Sie auch auf wko.at bei den Serviceangeboten Ihrer Wirtschaftskammer zum [Datenschutz](#). Alle Angaben erfolgen trotz sorgfältigster Bearbeitung ohne Gewähr.

Eine Haftung der Wirtschaftskammern Österreichs ist ausgeschlossen.

Bei allen personenbezogenen Bezeichnungen gilt die gewählte Form für alle Geschlechter!

Datenverarbeitungsverzeichnis nach Art 30 Abs 2 EU-Datenschutz-
Grundverordnung (DSGVO)
(Auftragsverarbeiter)

Inhalt

- A. Stamblatt des Auftragsverarbeiters
- B. Stamblatt des/der Verantwortlichen und Angaben zur Auftragsdatenverarbeitung
- C. Allgemeine Beschreibung der organisatorisch-technischen Maßnahmen

BEISPIEL

A. Stamblatt des Auftragsverarbeiters

1. Name und Kontaktdaten des Auftragsverarbeiters/der Auftragsverarbeiter

a. Name und Anschrift:

Ines Musterfrau e.U., Expertenstraße 1, XXXX Musterstadt

b. E-Mail-Adresse (und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.):

ines.musterfrau@abcd.at

c. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.) des Datenschutzbeauftragten des Auftragsverarbeiters¹:

Hans Musterfrau, selbe Anschrift wie Auftragsverarbeiter; hans.musterfrau@abcd.at

B. Stamblatt zum Verantwortlichen, in dessen Namen Daten verarbeitet werden, und Angaben zur Auftragsdatenverarbeitung

2. Name und Kontaktdaten des (der) für die Verarbeitung (gemeinsam) Verantwortlichen (=Auftraggeber)

a. Name(n) und Anschrift(en):

Max Mustermann GmbH, Neuer Weg 1, ZZZZ Musterdorf

b. E-Mail-Adresse(n) (und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.):

max@mustermann.at

c. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.) des Datenschutzbeauftragten²:

Franz Fachmann e.U., Datenstraße 1, YYYY Datenstadt

d. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.) des Vertreters des (der) Verantwortlichen³:

KEINER

¹ Ob die Angabe des Datenschutzbeauftragten des Verantwortlichen im Verarbeitungsverzeichnis des Auftragsverarbeiters (unter Pkt. B) verpflichtend ist, kann aufgrund der Formulierung der Bestimmung des Art. 30 Abs. 2 lit. a DSGVO derzeit noch nicht abschließend geklärt werden; die Anführung kann aber bei der Zusammenarbeit mit dem Verantwortlichen im Einzelfall Erleichterungen bringen.

HINWEIS: Sofern ein Datenschutzbeauftragter verpflichtend oder auf freiwilliger Basis bestellt wurde. Siehe dazu: [Datenschutzbeauftragter](#). Ein Datenschutzkoordinator kann, muss aber nicht ins Verarbeitungsverzeichnis aufgenommen werden.

² Ob auch die Daten eines beim Verantwortlichen bestellten Datenschutzbeauftragten im Verarbeitungsverzeichnis des Auftragsverarbeiters zu dokumentieren sind, ist aus dem Verordnungstext nicht eindeutig ablesbar. Es erscheint jedoch aus pragmatischen Gründen durchaus sinnvoll zu sein, diese Daten (sofern vorhanden) ins Verzeichnis aufzunehmen, erleichtert es doch die datenschutzrechtliche Zusammenarbeit zwischen Verantwortlichen und Auftragsverarbeiter.

³ Darunter sind Vertreter von nicht in der EU niedergelassenen Verantwortlichen zu verstehen.

3. Kategorien von Verarbeitungen, die im Auftrag des konkreten Verantwortlichen durchgeführt werden

(Angabe der angebotenen Leistung, die im Zusammenhang mit der Verarbeitung personenbezogener Daten steht)

- **Cloud-Computing:**
Storage, Application-Services (z.B. Materialwirtschaft, Finanzbuchhaltung)
- **Security-Services:**
Firewall, Anti-Virus-Services

4. Empfänger in Drittländern ⁴		
Empfängerkategorien bzw. Empfänger in Drittstaaten oder Internationalen Organisationen	Angabe des Drittstaats	Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Abs 1 Unterabsatz 1 DSGVO erfolgt ⁵

⁴ Damit sind Empfänger gemeint, die ihren Sitz außerhalb der EU bzw. des EWR haben. Siehe dazu: [Internationaler Datenverkehr](#).

⁵ Gemäß den Art. 45 bis 49 DSGVO. Siehe dazu: [Internationaler Datenverkehr](#).

C. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen⁶

a. Vertraulichkeit:

- i. Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;
- ii. Zugangskontrolle: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- iii. Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Protokollierung von Zugriffen

b. Integrität:

- i. Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- ii. Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

c. Verfügbarkeit und Belastbarkeit:

- i. Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie, Virenschutz, Firewall;

d. Pseudonymisierung und Verschlüsselung:

- i. Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
- ii. Verschlüsselung: sofern für die jeweilige Datenverarbeitung möglich, werden folgende Verschlüsselungstechnologien eingesetzt:

e. Evaluierungsmaßnahmen:

- i. Datenschutz-Management (z.B. Risikoanalyse, Datenschutz-Folgenabschätzung), einschließlich regelmäßiger Mitarbeiter-Schulungen;

⁶ Eine ausführlichere Liste mit konkreten Maßnahmen findet sich als Anhang zum [Mustervertrag für die Auftragsverarbeitung](#).