WIRTSCHAFTSRECHT

WKO WIRTSCHAFTSKAMMERN ÖSTERREICHS

# EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO): MUSTER – DATENVERARBEITUNGSVERZEICHNIS FÜR VERANTWORTLICHE

MUSTER ZUM DOWNLOAD

## Muster eines Datenverarbeitungsverzeichnisses nach Art. 30 Abs. 1 EU-Datenschutz-Grundverordnung (DSGVO) (Verantwortliche)

Die Experten der Wirtschaftskammern Österreichs haben für ihre Mitgliedsbetriebe nachstehendes Muster eines Datenverarbeitungsverzeichnisses nach Art 30 Abs. 1 EU-Datenschutz-Grundverordnung (DSGVO) für **Verantwortliche** erstellt.

Als Ausfüllhilfe ist ein bereits ausgefülltes fiktives Beispiel unter Anwendungsbeispiel für Verantwortliche“ (PDF-Version) im Download-Bereich verfügbar.

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

Stand: Juni 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 im Internet unter http://wko.at/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 1 EU-Datenschutz-Grundverordnung (DSGVO)
# (Verantwortlicher)

MUSTER

## Inhalt

# A. Stammdatenblatt

**Name und Kontaktdaten des (der) für die Verarbeitung (gemeinsam) Verantwortlichen**

**a. Name(n) und Anschrift(en):……..**

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

**c. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.) des Datenschutzbeauftragten[1]: ……..**

**d. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.) des Vertreters des (der) Verantwortlichen:[2] ……..**

MUSTER

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

[2] Darunter sind Vertreter von nicht in der EU niedergelassenen Verantwortlichen zu verstehen.

# B. Datenverarbeitungen/Datenverarbeitungszwecke

**1. Zwecke und Beschreibung der Datenverarbeitung[3]:**

1. ……..
2. ……..
3. ……..
4. ……..
5. ……..
6. ……..
7. ……..
8. ……..
9. ……..

**usw.**

**2. Wurde eine Datenschutz-Folgenabschätzung durchgeführt?[4]**

**Ja** ☐ **Wann?** ……..
**Nein** ☐ **Warum nicht?** [5] ……..

MUSTER

[3] Zum Begriff „Verarbeitung“ siehe Wichtige Begriffsbestimmungen; sollten Daten auch an „Dritte“ oder an Auftragsverarbeiter übermittelt werden, sind auch die Zwecke dieser Datenübermittlungen im Verarbeitungsverzeichnis zu dokumentieren.
[4] Zur Datenschutz-Folgenabschätzung siehe Datenschutz-Folgenabschätzung. Im Verarbeitungsverzeichnis sind zwar Angaben zur Datenschutz-Folgenabschätzung nicht zwingend vorgesehen. Aus Gründen der Rechenschaftspflicht empfehlen sich aber grundsätzliche Angaben darüber auch ins Verarbeitungsverzeichnis aufzunehmen.
[5] Zu den Gründen, warum keine Datenschutz-Folgenabschätzung durchzuführen ist, siehe auch Datenschutz-Folgenabschätzung und Prüfschema Internationaler Datenverkehr. Es empfiehlt sich etwa, die Ergebnisse des WKO Online-Ratgebers Datenschutz-Folgenabschätzung hier zu dokumentieren.

# C. Detailangaben zu …..

| 1. Kategorien der betroffenen Personen | |
|---|---|
| **Lfd. Nr.** | **Beschreibung der Kategorien betroffener Personen** *(z.B. Kunden, Mitarbeiter, Lieferanten usw.)* |
| 1 | …… |
| 2 | …… |
| 3 | …… |
| 4 | …… |

| 2. Rechtmäßigkeitsgrundlagen[6] | |
|---|---|
| **Lfd. Nr.** | **Beschreibung der Rechtmäßigkeitsgrundlagen, auf die sich Datenverarbeitung stützt** |
| 1 | Art. 6 Abs. 1 lit. a DSGVO (Einwilligung des Betroffenen) |
| 2 | Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung) |
| 3 | Art. 6 Abs. 1 lit. c DSGVO (gesetzliche Verpflichtungen nach *z.B. BAO, UGB, Arbeitsrecht*) |
| 4 | Art. 6 Abs. 1 lit. f DSGVO (berechtigte Interessen des Verantwortlichen oder eines Dritten) |

**3. Verträge, Zustimmungserklärungen oder sonstige Unterlagen (z.B. Erledigung der Informationspflichten[7]) sind abgelegt:[8] (freiwillig)**

**……..**

| 4. Datenübermittlungen (Kategorien der Empfänger[9], Zweck und Rechtmäßigkeitsgrundlagen) | | | |
|---|---|---|---|
| **Lfd. Nr.** | **Beschreibung der Empfängerkategorien** | **Zweck** | **Rechtmäßigkeitsgrundlagen** |
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |

| 5. Löschungs- und Aufbewahrungsfristen (wenn möglich)[10] | |
|---|---|
| **Lfd. Nr.** | **Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen** *( zB Vertragslaufzeit, sieben Jahre für BAO, usw.)* |

[6] Die Rechtmäßigkeitsgrundlagen sind nach der DSGVO zwar nicht verpflichtend in das Verarbeitungsverzeichnis aufzunehmen, allerdings aufgrund der Rechenschaftspflicht zu empfehlen. Siehe dazu: Grundsätze und Rechtmäßigkeit der Verarbeitung.

[7] Siehe zu den Informationspflichten: Informationspflichten.

[8] Die Angabe, wo die Unterlagen innerhalb der Organisation abgelegt wurden, ist nicht verpflichtend im Verarbeitungsverzeichnis zu dokumentieren, erleichtert aber vor allem in größeren, arbeitsteilig organisierten Einrichtungen das Auffinden der entscheidenden Unterlagen (dient also lediglich der innerbetrieblichen Arbeitserleichterung).

[9] Bei der Umschreibung der Empfängerkategorien ist darauf zu achten, dass eine Überprüfung der Rechtmäßigkeit ermöglicht wird (so wird z.B. die bloße Angabe von „Konzern" als Empfänger nicht ausreichen, weil daraus nicht eruierbar sein wird, ob die Daten rechtmäßig an die Muttergesellschaft und/oder an Schwestergesellschaften übertragen werden).

[10] Nach der DSGVO sind die Löschfristen bzw. Aufbewahrungsfristen nach Möglichkeit ins Verarbeitungsverzeichnis aufzunehmen. Beispielsweise kann bei unbefristeten Verträgen keine konkrete Löschfrist angegeben werden, da der konkrete Vertragsablauf unbestimmt ist. Es empfiehlt sich hier eine abstrakte Frist anzugeben (z.B. „nach Ablauf des Vertrages"). Siehe dazu auch: Speicher-, Verjährungs- und Aufbewahrungsfristen.

MUSTER

| | |
|---|---|
| 1 | …… |
| 2 | …… |
| 3 | …… |
| | |

## 6. Kategorien der verarbeiteten Daten, Empfängerkategorien, Rechtmäßigkeitsgrundlagen und Löschungs- bzw. Aufbewahrungsfristen

**Verarbeitung besonders geschützter Daten[11]**

| | | |
|---|---|---|
| Werden sensible Daten (Art 9 Abs 1 DSGVO)[12] verarbeitet? | Ja ☐ | Nein ☐ |
| Werden strafrechtlich relevante Daten (Art 10 DSGVO) verarbeitet?[13] | Ja ☐ | Nein ☐ |

| Kategorien der betroffenen Personen[14] | Lfd. Nr. | Datenkategorien | Rechtmäßigkeits-grundlagen[15] | Löschungs- und Aufbewahrungsfristen[16] | Datenübermittlungen[17] |
|---|---|---|---|---|---|
| | 1 | | | | |
| | 2 | | | | |
| | 3 | | | | |
| | 4 | | | | |
| | 5 | | | | |
| | 6 | | | | |
| | 7 | | | | |
| | 8 | | | | |
| | 9 | | | | |
| | 10 | | | | |

| 7. Empfänger in Drittländern[18] | | |
|---|---|---|
| **Empfängerkategorien bzw. Empfänger in Drittstaaten oder Internationalen Organisationen (aus 4)** | **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[19]** |

[11] Diese Angabe empfiehlt sich im Hinblick auf eine raschere Erfassung der Risikoneigung der Datenverarbeitung.
[12] „Sensible Daten" nach Art 9 DSGVO sind besondere Datenkategorien: rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und biometrische Daten zur Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung.
[13] Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln unter behördlicher Aufsicht.
[14] Laut Punkt 1. des C-Blattes.
[15] Laut Punkt 2. des C-Blattes.
[16] Laut Punkt 5. des C-Blattes.
[17] Laut Punkt 4. des C-Blattes.
[18] Damit sind Empfänger gemeint, die ihren Sitz außerhalb der EU haben. Siehe dazu: Internationaler Datenverkehr.
[19] Vor allem wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, keine Standardvertragsklauseln der Europäischen Kommission oder der nationalen Datenschutzbehörde verwendet

MUSTER

| | | |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

MUSTER

werden oder genehmigte Zertifizierungsmechanismen in Anspruch genommen werden, keine Corporate binding rules zur Anwendung kommen (genehmigte verbindliche konzerninterne Datenschutzvorschriften), die Übermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt). Siehe: Internationaler Datenverkehr.

# D. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen[20]

**a. Vertraulichkeit[21]:**

**b. Integrität[22]:**

**c. Verfügbarkeit und Belastbarkeit:**

**d. Pseudonymisierung und Verschlüsselung:**

**e. Evaluierungsmaßnahmen:**

MUSTER

[20] Eine Liste mit konkreten Maßnahmen findet sich als Anhang zum Mustervertrag für die Auftragsverarbeitung.
[21] Verhinderung von (unbeabsichtigter) Offenlegung oder unbefugten Zugang zu personenbezogenen Daten.
[22] Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.