# EU-Datenschutz-Grundverordnung (DSGVO): Muster-Verarbeitungsverzeichnis für Verantwortliche

## Datenverarbeitungsverzeichnis mit Word-Download und Anwendungsbeispiel

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.

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

### Inhalt



### Stammdatenblatt

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

1. Name(n) und Anschrift(en):
2. E-Mail-Adresse(n) (und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.):
3. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.) des Datenschutzbeauftragten[1]:
4. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.) des Vertreters des (der) Verantwortlichen:[2]

### Datenverarbeitungen/Datenverarbeitungszwecke

1. Zwecke und Beschreibung der Datenverarbeitung[3]:
    a.
    b.
    c.
    d.
    e.
    f.

g.

h.

i.

usw.

2. Wurde eine Datenschutz-Folgenabschätzung durchgeführt?[4]
    a. Ja / Nein
        i. Wenn Ja, wann?
        ii. Wenn Nein, aus welchem Grund nicht?[5]

## Detailangaben zu .....

*(Einfügung der konkreten Datenverarbeitung aus dem B-Blatt, z.B. des Datenverarbeitungszweckes „Rechnungswesen"; das C-Blatt kann dann für jede der im B-Blatt angegebenen Datenverarbeitungszwecke verwendet werden, ohne dass die allgemeinen Angaben aus dem A- und B-Blatt wiederholt werden müssen)*

1. Kategorien der betroffenen Personen
   Lfd.Nr. *Beschreibung der Kategorien betroffener Personen (z.B. Kunden, Mitarbeiter, Lieferanten usw.)*
    a. *z.B. Kunden*
    b. *z.B. Mitarbeiter*
    c. *z.B. Lieferanten*
    d. usw.

2. Rechtsgrundlagen[6]
3. Verträge , Zustimmungserklärungen oder sonstige Unterlagen (z.B. Erledigung der Informationspflichten[7]) sind abgelegt:[8] (freiwillig)
4. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen[9]
    a. Kategorien der verarbeiteten Daten und ankreuzen, ob sie an Empfänger[10] übermittelt werden

| Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes | Lfd. Nr. | Datenkategorien | Besondere Datenkategorien iSd Art 9 DSGVO[11], strafrechtlich relevant iSd Art 10 DSGVO[12] | Empfänger | Empfänger | Empfänger | Empfänger | Empfänger | Empfänger | Empfänger | Empfänger | Empfänger | Empfänger |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 *(oder Angabe der Personenkategorie aus Punkt 1 des C-Blattes, z.B. „Kunden")* | 1 | | | | | | | | | | | | |
| | 2 | | | | | | | | | | | | |
| | 3 | | | | | | | | | | | | |
| | 4 | | | | | | | | | | | | |
| 2 | 5 | | | | | | | | | | | | |
| | 6 | | | | | | | | | | | | |
| | 7 | | | | | | | | | | | | |
| | 8 | | | | | | | | | | | | |
| | 9 | | | | | | | | | | | | |
| | 10 | | | | | | | | | | | | |

b. Löschungs- und Aufbewahrungsfristen (wenn möglich)

| Daten aus 4.a. (Lfd. Nr.) | Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen |
|---|---|
| | |
| | |
| | |

5. Kategorien von Empfängern[13], an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern[14]
   a. Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation wie z.B. UNO, OSZE)

| Empfänger-Kategorien bzw. Empfänger in Drittstaaten oder Internationalen Organisationen (aus 4.a) | Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU) | Internationale Organisation (Angabe der intern. Organisation) |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

   b. 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 (vor allem wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, keine Standardvertragsklauseln der Europäischen Kommission oder der nationalen Datenschutzbehörde verwendet werden oder genehmigte Zertifizierungsmechanismen in Anspruch genommen werden, keine Corporate binding rules zur Anwendung kommen (genehmigte

verbindliche konzerninterne Datenschutzvorschriften), die Ubermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt):

## Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

1. Vertraulichkeit:[15]
2. Integrität:[16]
3. Verfügbarkeit und Belastbarkeit:
4. Pseudonymisierung und Verschlüsselung:
5. Evaluierungsmaßnahmen:

---

[1] Sofern ein Datenschutzbeauftragter verpflichtend oder auf freiwilliger Basis bestellt wurde.

> **Hinweis:** Wenn keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht, der Verantwortliche aber freiwillig einen bestellen möchte, müssen trotzdem alle den Datenschutzbeauftragten betreffenden Bestimmungen der DSGVO eingehalten werden; möchte man das nicht, darf die bestellte Person nicht „*Datenschutzbeauftragter*" genannt werden, sondern sollte eine andere Bezeichnung gewählt werden (z.B. „*Datenschutzkoordinator*"). Dieser kann, muss aber nicht ins Verarbeitungsverzeichnis aufgenommen werden. Siehe dazu das WKO-Merkblatt „Datenschutzbeauftragter".

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

[3] Zum Begriff „Verarbeitung" siehe das Merkblatt „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 das Merkblatt „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] Eine Datenschutz-Folgenabschätzung ist nicht durchzuführen, wenn durch die Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte der Betroffenen besteht oder die Datenverarbeitungsart in der sogenannten „white list" der Datenschutzbehörde gelistet ist; Näheres dazu siehe auch das Merkblatt „Datenschutz-Folgenabschätzung" und „Prüfschema Internationaler Datenverkehr".

[6] Die Rechtsgrundlagen (z.B. rechtliche Verpflichtung, Einwilligung, Vertragserfüllung, lebenswichtige Interessen des Betroffenen, kein überwiegendes berechtigtes Interesse des Betroffenen) sind nach der DSGVO zwar nicht verpflichtend ins Verarbeitungsverzeichnis aufzunehmen. Allerdings unterliegt der verantwortliche Verarbeiter einer sogenannten Rechenschaftspflicht. Diese besagt eine Nachweispflicht bzgl. der Einhaltung der Pflichten nach der DSGVO. Dazu gehört unter anderem auch der Nachweis, dass die Datenverarbeitung nach den in der DSGVO normierten Rechtmäßigkeitsgrundlagen erfolgt. Siehe das Merkblatt „Grundsätze und Rechtmäßigkeit der Verarbeitung".

[7] Siehe zu den Informationspflichten das Merkblatt „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] 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 allerdings eine abstrakte Frist anzugeben (z.B. „nach Ablauf des Vertrages").

[10] In der Rubrik „Empfänger" sind nur die „Empfängerkategorien" (z.B. „Gerichte", „Banken" oder „Sozialversicherungsträger") einzutragen. Dazu gehören auch Auftragsverarbeiter. 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).

[11] Daten nach Art 9 DSGVO sind besondere Datenkategorien („sensible Daten): 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.

[12] Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln unter behördlicher Aufsicht.

[13] Es sind vor allem Übermittlungsempfänger („Dritte") als auch Auftragsverarbeiter hier zu dokumentieren. 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). Bei Empfängern in Drittstaaten (speziell in den USA wegen dem „Privacy Shield"-System) empfiehlt sich eine namentliche Nennung des Empfängers.

[14] Siehe dazu das Merkblatt „Internationaler Datenverkehr".

[15] Verhinderung von (unbeabsichtigter) Offenlegung oder unbefugten Zugang zu personenbezogenen Daten.

[16] Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.

Stand: 18.03.2021