WIRTSCHAFTSRECHT

WKO WIRTSCHAFTSKAMMERN ÖSTERREICHS

EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)
MUSTER

Die Experten der Wirtschaftskammern Österreichs haben für ihre Mitgliedsbetriebe nachstehendes Muster eines Datenverarbeitungsverzeichnisses nach Art 30 Abs. 2 EU-Datenschutz-Grundverordnung (DSGVO) für **Auftragsverarbeiter** 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 2 EU-Datenschutz-Grundverordnung (DSGVO) (Auftragsverarbeiter)

Inhalt

A. Stammblatt des Auftragsverarbeiters

1. **Name und Kontaktdaten des Auftragsverarbeiters/der Auftragsverarbeiter**

   - **Name und Anschrift:**
     …
     …
     …
     …

   - **Kontaktdaten:**
     T: **…**
     M: **…**
     E: **…**

   - *[falls vorhanden]*
     Name und Kontaktdaten des Datenschutzbeauftragten des Auftragsverarbeiters:

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

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

- **Name(n) und Anschrift(en):**
  …
  …
  …

- **Kontaktdaten:**
  T: **…**
  M: **…**
  E: **…**

- *[falls vorhanden]*
  Name und Kontaktdaten des Datenschutzbeauftragten des Auftragsverarbeiters:

- *[falls vorhanden]*
  Name und Kontaktdaten des Vertreters des (der) Verantwortlichen:[1]

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

- Übernahme von Transporten jeglicher Art für den Verantwortlichen
- …
- …

4. Übermittlung von personenbezogenen Daten in Drittländer, inkl. internationale Organisationen

- Ja ☐ Nein ☐

Wenn ja, Angabe des betreffenden Drittlandes bzw. der internationalen Organisation:

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 Binding Corporate Rules zur Anwendung kommen (genehmigte verbindliche konzerninterne Datenschutzvorschriften), die Übermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt):[2]

---

[1] Darunter sind Vertreter von nicht in der EU niedergelassenen Verantwortlichen zu verstehen.
[2] Siehe das Merkblatt der WKO „Internationalen Datenverkehr“.

TECHNISCH-ORGANISATORISCHE MASSNAHMEN[3]

VERTRAULICHKEIT

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;
- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis", Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten;
- **Pseudonymisierung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
- **Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

INTEGRITÄT[4]

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

VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;
- Rasche **Wiederherstellbarkeit**;
- **Löschungsfristen**: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.

VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen;
- **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Verantwortlichers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS), Vorabüberzeugungspflicht, Nachkontrollen.

---

[3] Entsprechend den Realitäten anpassen!

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