WIRTSCHAFTSRECHT

WKO WIRTSCHAFTSKAMMERN ÖSTERREICHS

EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

BEISPIEL

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

(HINWEIS: es wird darauf hingewiesen, dass es sich hier um ein fiktives Beispiel handelt. Bei der praktischen Umsetzung ist auf die konkreten Anwendungsfälle im Unternehmen abzustellen)

Stand: April 2019

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) 51450-1615,
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 beide Geschlechter!

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

Inhalt

A. Stammblatt 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 zB Tel.Nr.):
ines.musterfrau@abcd.at

c. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Datenschutzbeauftragten des Auftragsverarbeiters[1]:
Hans Musterfrau, selbe Anschrift wie Auftragsverarbeiter; hans.musterfrau@abcd.at

[1] Sofern ein Datenschutzbeauftragter verpflichtend oder auf freiwilliger Basis bestellt wurde. 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: 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 (zB „*Datenschutzkoordinator*“). Dieser kann, muss aber nicht ins Verarbeitungsverzeichnis aufgenommen werden. Siehe dazu das WKO-Merkblatt „Datenschutzbeauftragter“.

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)

a. Name(n) und Anschrift(en):
Max Mustermann GmbH, Neuer Weg 1, ZZZZ Musterdorf

b. E-Mail-Adresse(n) (und allenfalls weitere Kontaktdaten wie zB Tel.Nr.):
max@mustermann.at

c. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Datenschutzbeauftragten[2]:
Franz Fachmann e.U., Datenstraße 1, YYYY Datenstadt

d. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Vertreters des (der) Verantwortlichen[3]:
KEINER

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 (zB Materialwirtschaft, Finanzbuchhaltung)
- **Security-Services:**
  Firewall, Anti-Virus-Services

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

a. Ja ☐ Nein ☐X

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

[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.

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 Binding Corporate Rules zur Anwendung kommen (genehmigte verbindliche konzerninterne Datenschutzvorschriften), die Übermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt)[4]:

[4] Siehe das Merkblatt der WKO „Internationalen Datenverkehr“.

C. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

a. Vertraulichkeit:

i. Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, zB: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;

ii. Zugangskontrolle: Schutz vor unbefugter Systembenutzung, zB: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

iii. Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, zB: Protokollierung von Zugriffen

b. Integrität:

i. Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, zB: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

ii. Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, zB: Protokollierung, Dokumentenmanagement;

c. Verfügbarkeit und Belastbarkeit:

i. Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, zB: 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 (zB Risikoanalyse, Datenschutz-Folgenabschätzung), einschließlich regelmäßiger Mitarbeiter-Schulungen;