WIRTSCHAFTSRECHT

WKO REICHS

EU-DATENSCHUTZ-GRUNDVERORDNUNG
MUSTER

Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 DSGVO

mit spezifischen Schwerpunkt für die Weitergabe von Aufträgen im Güterbeförderungsgewerbe

Die Experten der Wirtschaftskammern Österreichs haben für ihre Mitgliedsbetriebe nachstehendes Muster einer Vereinbarung über eine Auftragsverarbeitung nach Art 28 DSGVO erstellt.

Dieses Merkblatt 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!

HINWEISE
Dieser Mustervertrag ist auf eine Auftragsverarbeitung in Österreich, innerhalb des EWR oder in Staaten mit angemessenem Datenschutzniveau zugeschnitten. Für die Auftragsverarbeitung in Drittstaaten ist die Verwendung von Standardvertragsklauseln zu empfehlen (Bewilligungsfreiheit nach Art 46 Abs 2 lit c DSGVO).

Dieser Mustervertrag wurde mit größter Sorgfalt erstellt und kann laufend aktualisiert werden. Für die Richtigkeit, Vollständigkeit, Aktualität oder Qualität des bereitgestellten Musters sowie auch für weiterführende Links können wir jedoch keine Gewähr übernehmen. Haftungsansprüche gegen Personen, welche dieses Muster bereitgestellt haben, sind daher ausgeschlossen.

Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:	Der Auftragsverarbeiter:
[*NN*] [*Anschrift*]	**[*NN*]** [*Anschrift*]
(im Folgenden Verantwortlicher)	(im Folgenden Auftragsverarbeiter)

1. GEGENSTAND DER VEREINBARUNG

(1) Gegenstand dieser Vereinbarung ist die Durchführung folgender Aufgaben:
- Übernahme von Transporten jeglicher Art für den Verantwortlichen
- …
- …

Diese Vereinbarung ist als Ergänzung zu bereits bestehenden Verträgen und Vereinbarungen zu verstehen. *[eventuell anführen!]*

(2) Folgende Datenkategorien werden verarbeitet:
- Kontaktdaten (Firmenname, Ansprechpartner, Anrede, Geschlecht, Adresse, Telefon- und Faxnummern, E-Mail-Adresse
- …
- …

(3) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:
- Kundendaten
- …
- …

(4) Die Verarbeitung ist folgender Art:
Erheben, Erfassen Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten]

2. DAUER DER VEREINBARUNG

{bei einmaliger Durchführung} Dieser Vertrag beginnt am *[Datum einfügen]* und endet nach einmaliger Ausführung.
ODER

{bei befristeter Laufzeit} Die Vereinbarung ist befristet abgeschlossen und endet mit [*Fristende eintragen*]
ODER

{bei unbefristeter Laufzeit} Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von [*Kündigungsfrist eintragen, zB ein Monat*] zum [*Kündigungstermin eintragen, zB Kalendervierteljahr*] gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. PFLICHTEN DES AUFTRAGSVERARBEITERS

(1) Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen – zu verarbeiten, sofern er nicht hierzu rechtlich verpflichtet ist. In solch einem Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern eine solche Mitteilung nicht rechtlich verboten ist.
(2) Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht.
(3) Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (siehe Punkt 7 sowie Einzelheiten sind der Anlage ./11 zu entnehmen).
(4) Der Auftragsverarbeiter unterstützt angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen, damit der Verantwortliche seine Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person (zB Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Verantwortlichen alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragsverarbeiter gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Verantwortlichen der von ihm betriebenen Datenanwendung hält, hat der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiterzuleiten und dies dem Antragsteller mitzuteilen.
(5) Der Auftragsverarbeiter unterstützt unter Berücksichtigung der Art der Vereinbarung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (zB Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).
(6) Der Auftragsverarbeiter hat für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten.
(7) Dem Verantwortlichen wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen – die

vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen.

(8) Der Auftragsverarbeiter ist nach Beendigung dieser Vereinbarung verpflichtet – sofern nicht eine rechtliche Verpflichtung zur Speicherung besteht – alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Verantwortlichen zu übergeben / in dessen Auftrag zu vernichten.

(9) Der Auftragsverarbeiter teilt dem Verantwortlichen unverzüglich Störungen, Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung des Veranwortlichen durchführen.

4. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

{Ausschließliche Durchführung innerhalb der EU/des EWR} Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.
ODER

{Bei Durchführung, wenn auch nur teilweise, außerhalb der EU/des EWR wird empfohlen die Auftragsverarbeiter-Vereinbarung des Auftragsverarbeiters zu berücksichtigen bzw. dieser – u.U. mit individuellen Abänderungen zuzustimmen}

5. SUB-AUFTRAGSVERARBEITER

{Verbot der Hinzuziehung eines Sub-Auftragsverarbeiters} Der Auftragsverarbeiter ist nicht berechtigt, einen Sub-Auftragsverarbeiter heranzuziehen.
ODER

{Zulässigkeit der Hinzuziehung eines bestimmten Sub-Auftragsverarbeiters} Der Auftragsverarbeiter ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter hinzuziehen: [*Firmenname und Sitz ergänzen, Art der Tätigkeiten]*.
Beabsichtigte Änderungen des Sub-Auftragsverarbeiters sind dem Verantwortlicher so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls untersagen kann. Der Auftragsverarbeiter schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragsverarbeiter auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.
ODER

{Zulässigkeit der Hinzuziehung von Sub-Auftragsverarbeitern} Der Auftragsverarbeiter kann Sub-Auftragsverarbeiter für die unter Punkt 1.(1) genannten Tätigkeiten hinzuziehen.
Er hat den Verantwortlicher von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. Der Auftragsverarbeiter schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragsverarbeiter auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen

Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

[*Ort*], am [*Datum*]

Für den Verantwortlichen:

.....
[*Name samt Funktion*]

[*Ort*], am [*Datum*]

Für den Auftragsverarbeiter:

.....
[*Name samt Funktion*]

ANLAGE ./1 – TECHNISCH-ORGANISATORISCHE MASSNAHMEN[1]

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[2]

- **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.

---

[1] Entsprechend den Realitäten anpassen!

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