EU-Datenschutz-Grundverordnung (DSGVO): Mustervertrag für die Auftragsverarbeitung

Vereinbarung über eine Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:

[NN]
[Anschrift]

(im Folgenden Auftraggeber)

Der Auftragsverarbeiter:

[NN]
[Anschrift]

(im Folgenden Auftragnehmer)

1. Gegenstand der Vereinbarung

(1) Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben: [*möglichst detaillierte Beschreibung der Aufgaben des Auftragnehmers, einschließlich Art und Zweck der vorgesehenen Verarbeitung].*

{Falls es einen weitergehenden Rahmenvertrag, Werkvertrag, Leistungsvereinbarung, udgl gibt} Diese Vereinbarung ist als Ergänzung zu [*Vertrag, etc samt Datum ergänzen*] zu verstehen.

(2) Folgende Datenkategorien werden verarbeitet: [*Datenkategorien aufzählen, zB Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bonitätsdaten, Bestelldaten, Entgeltdaten, usw*].

(3) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung: [*Betroffenenkategorien ergänzen, zB Kunden, Interessenten, Lieferanten, Ansprechpartner, Beschäftigte, usw.*

2. Dauer der Vereinbarung

{Einmalige Durchführung} Die Vereinbarung endet mit einmaliger Durchführung der Arbeiten.

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

{Unbefristete 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 Kalenderviertaljahr*] gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine

Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(2) Der Auftragnehmer 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 Auftragnehmer aufrecht.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage ./1 zu entnehmen).

(4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenverarbeitung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (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 Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch von ihm beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten[1]. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.

(9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. Ort der Durchführung der Datenverarbeitung [2]

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

{Bei Durchführung, wenn auch nur teilweise, außerhalb der EU/des EWR} Datenverarbeitungstätigkeiten werden zumindest zum Teil auch außerhalb der EU bzw des EWR durchgeführt, und zwar in [*Staaten aufzählen*]. Das angemessene Datenschutzniveau ergibt sich aus[3]

- einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO.
- einer Ausnahme für den bestimmten Fall nach Art 49 Abs 1 DSGVO.
- verbindlichen internen Datenschutzvorschriften nach Art 47 iVm Art 46 Abs 2 lit b DSGVO.
- Standarddatenschutzklauseln nach Art 46 Abs 2 lit c und d DSGVO.
- genehmigten Verhaltensregeln nach Art 46 Abs 2 lit e iVm Art 40 DSGVO.
- einen genehmigten Zertifizierungsmechanismus nach Art 46 Abs 2 lit f iVm Art 42 DSGVO.
- von der Datenschutzbehörde bewilligte Vertragsklauseln nach Art 46 Abs 3 lit a DSGVO.
- einer Ausnahme für den Einzelfall nach Art 49 Abs 1 Unterabsatz 2 DSGVO.

5. Sub-Auftragsverarbeiter [4]

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

{Zulässigkeit der Hinzuziehung eines bestimmten Sub-Auftragsverarbeiters} Der Auftragnehmer ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter hinzuziehen: [*Firmenname und Sitz ergänzen, Art der Tätigkeiten]*.
Beabsichtigte Änderungen des Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls untersagen kann. Der Auftragnehmer 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 Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

{Zulässigkeit der Hinzuziehung von Sub-Auftragsverarbeitern} Der Auftragnehmer kann Sub-Auftragsverarbeiter [*Tätigkeiten*] hinzuziehen.
Er hat den Auftraggeber von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. Der Auftragnehmer 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 Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

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

Für den Auftraggeber:

.....

[*Name samt Funktion*]

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

Für den Auftragnehmer:

.....

[*Name samt Funktion*]

Anlage ./1 – Technisch-organisatorische Maßnahmen [5]

A. Vertraulichkeit

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:

☐ Schlüssel	☐ Magnet- oder Chipkarten
☐ Elektrische Türöffner	☐ Portier
☐ Sicherheitspersonal	☐ Alarmanlagen
☐ Videoanlage	☐ Einbruchshemmende Fenster und/oder Sicherheitstüren
☐ Anmeldung beim Empfang mit Personenkontrolle	☐ Begleitung von Besuchern im Unternehmensgebäude
☐ Tragen von Firmen-/Besucherausweisen	☐ Sonstiges:

Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch:

☐ Kennwörter (einschließlich entsprechender Policy)	☐ Verschlüsselung von Datenträgern
☐ Automatische Sperrmechanismen	☐ Sonstiges:
☐ Zwei-Faktor-Authentifizierung	

Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

☐ Standard-Berechtigungsprofile auf „need to know-Basis“	☐ Standardprozess für Berechtigungsvergabe
☐ Protokollierung von Zugriffen	☐ Sichere Aufbewahrung von Speichermedien
☐ Periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten	☐ Datenschutzgerechte Wiederverwendung von Datenträgern
☐ Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger	☐ Clear-Desk/Clear-Screen Policy
☐ Sonstiges:	

Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.

☐ Ja	☐ Nein

Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

☐ Ja	☐ Nein

B. Datenintegrität [6]

Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

☐ Verschlüsselung von Datenträgern	☐ Verschlüsselung von Dateien
☐ Virtual Private Networks (VPN)	☐ Elektronische Signatur
☐ Sonstiges:	

Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:

☐ Protokollierung	☐ Dokumentenmanagement
☐ Sonstiges:	

C. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

☐ 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
☐ Sonstiges:	

Rasche **Wiederherstellbarkeit:**

☐ Ja	☐ Nein

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen:

☐ Ja	☐ Nein

Incident-Response-Management:

☐ Ja	☐ Nein

Datenschutzfreundliche Voreinstellungen:

☐ Ja	☐ Nein

Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers durch:

☐ Eindeutige Vertragsgestaltung	☐ Formalisiertes Auftragsmanagement
☐ Strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS)	☐ Vorabüberzeugungspflicht
☐ Nachkontrollen	☐ Sonstiges:

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.

Wir behalten uns ausdrücklich vor, das Muster ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen und übernehmen daher keine Gewähr und Haftung für die dauerhafte Verfügbarkeit der des Musters.

---

[1] Nichtzutreffendes bitte streichen.

[2] Nichtzutreffendes bitte streichen.

[3] Nichtzutreffendes bitte streichen. Siehe im Allgemeinen Merkblatt Internationaler Datenverkehr nach der EU-DSGVO.

[4] Nichtzutreffendes bitte streichen.

[5] Entsprechend den bestehenden technisch-organisatorischen Maßnahmen anpassen.

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

(Stand: 5.4.2022 inhaltlich unverändert)

Stand: 05.04.2022