

Auftragsverarbeitungsvertrag

gemäß Art. 28 DSGVO · Vorlage für KMU · DE

Rechtlich geprüft von einem zertifizierten Datenschutzbeauftragten (CIPP/E) · Bereitgestellt von ETHYX · Version 1.1 · Juli 2026

» **HINWEIS** Verwenden Sie diesen Auftragsverarbeitungsvertrag (AVV) immer dann, wenn Sie ein anderes Unternehmen mit der Verarbeitung personenbezogener Daten in Ihrem Auftrag beauftragen – z. B. einen CRM-, E-Mail-, Hosting- oder Lohnabrechnungsdienst (Art. 28 DSGVO verlangt dies). Große Anbieter (Google, Microsoft, AWS) stellen meist ihren eigenen AVV bereit; nutzen Sie dann deren Vertrag und überspringen Sie diese Vorlage. Verwenden Sie diese Vorlage, wenn SIE der Verantwortliche sind und einen kleineren Auftragsverarbeiter ohne eigenen AVV beauftragen, oder wenn Sie selbst ALS Auftragsverarbeiter einen anbieten müssen. Ersetzen Sie jeden [orangefarbenen Platzhalter], füllen Sie die drei Anlagen aus, löschen Sie alle Hinweis-Kästen und lassen Sie beide Parteien unterzeichnen. Lassen Sie die finale Fassung von einem qualifizierten Datenschutzbeauftragten prüfen.

Vertragsparteien

Dieser Auftragsverarbeitungsvertrag (der „Vertrag“) wird geschlossen zwischen:

[NAME DES VERANTWORTLICHEN], [Anschrift] (der „Verantwortliche“)

und

[NAME DES AUFTRAGSVERARBEITERS], [Anschrift] (der „Auftragsverarbeiter“)

(jeweils eine „Partei“, zusammen die „Parteien“).

» **HINWEIS** Der Verantwortliche entscheidet über Zweck und Mittel der Verarbeitung; der Auftragsverarbeiter handelt ausschließlich auf Weisung. Wenn Sie eine Leistung einkaufen, sind Sie in der Regel der Verantwortliche.

Präambel

Die Parteien haben einen Hauptvertrag über die Erbringung von **[Hauptleistung beschreiben, z. B. CRM-Software / Lohnabrechnung]** (der „Hauptvertrag“) geschlossen, in dessen Rahmen der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Dieser Vertrag regelt die datenschutzrechtlichen Pflichten nach Art. 28 DSGVO. Bei Widersprüchen in Datenschutzfragen geht dieser Vertrag dem Hauptvertrag vor.

§ 1 Gegenstand, Art, Zweck und Dauer

(1) Gegenstand, Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen sind in Anlage 1 festgelegt.

(2) Dieser Vertrag läuft für die Dauer des Hauptvertrags und endet automatisch mit dessen Beendigung, vorbehaltlich der Lösch- und Rückgabepflichten nach § 9.

§ 2 Weisungsrecht

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, einschließlich dieses Vertrags und des Hauptvertrags, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaats zur Verarbeitung verpflichtet; in diesem Fall teilt er dies dem Verantwortlichen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet (Art. 28 Abs. 3 lit. a).

(2) Weisungen erfolgen schriftlich oder in dokumentierter elektronischer Form. Mündliche Weisungen sind unverzüglich in dokumentierter Form zu bestätigen.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen das Datenschutzrecht verstößt. Er darf die betroffene Verarbeitung bis zur Bestätigung aussetzen.

§ 3 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich insbesondere:

- a) sicherzustellen, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b);
- b) die in Anlage 2 festgelegten technischen und organisatorischen Maßnahmen umzusetzen und aufrechtzuerhalten (Art. 32, Art. 28 Abs. 3 lit. c);
- c) die Bedingungen für die Inanspruchnahme von Unterauftragsverarbeitern nach § 4 einzuhalten (Art. 28 Abs. 3 lit. d);
- d) den Verantwortlichen nach Möglichkeit mit geeigneten Maßnahmen bei der Erfüllung von Betroffenenanfragen nach Kapitel III DSGVO zu unterstützen (Art. 28 Abs. 3 lit. e, siehe § 5);
- e) den Verantwortlichen bei der Einhaltung der Pflichten nach Art. 32–36 DSGVO (Sicherheit, Meldung von Datenpannen, Datenschutz-Folgenabschätzung und vorherige Konsultation) unter Berücksichtigung der ihm vorliegenden Informationen zu unterstützen (Art. 28 Abs. 3 lit. f);
- f) nach Wahl des Verantwortlichen alle personenbezogenen Daten nach Abschluss der Leistung zu löschen oder zurückzugeben und vorhandene Kopien zu löschen, sofern keine gesetzliche Aufbewahrungspflicht besteht (Art. 28 Abs. 3 lit. g, siehe § 9);
- g) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung von Art. 28 zur Verfügung zu stellen und Überprüfungen sowie Inspektionen zu ermöglichen und dazu beizutragen (Art. 28 Abs. 3 lit. h, siehe § 7);
- h) einen Ansprechpartner für Datenschutzfragen zu benennen: **[Name / E-Mail]**.
- i) (optional) ein eigenes Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO für die im Auftrag des Verantwortlichen durchgeführten Verarbeitungen führen und dem Verantwortlichen auf Anfrage den relevanten Auszug zur Verfügung stellen (entspricht den Musterklauseln 2021/915 der EU-Kommission).

§ 4 Unterauftragsverarbeiter

- (1) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter („Unterauftragsverarbeiter“) in Anspruch ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen. Die bei Vertragsschluss genehmigten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt.
- (2) Bei allgemeiner Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung mit einer Frist von mindestens **[14]** Tagen und gibt ihm Gelegenheit, aus berechtigten Datenschutzgründen zu widersprechen (Art. 28 Abs. 2).
- (3) Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf wie in diesem Vertrag und haftet gegenüber dem Verantwortlichen vollständig für dessen Leistung (Art. 28 Abs. 4).

§ 5 Unterstützung bei Betroffenenrechten

- (1) Der Auftragsverarbeiter unterstützt den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von Betroffenenanfragen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch – Art. 15–22 DSGVO).
- (2) Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet dieser die Anfrage unverzüglich an den Verantwortlichen weiter und antwortet nicht selbst, sofern er nicht dazu angewiesen wird.

§ 6 Verletzungen des Schutzes personenbezogener Daten

- (1) Der Auftragsverarbeiter benachrichtigt den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von **[24]** Stunden, nachdem ihm eine Verletzung des Schutzes der Daten des Verantwortlichen bekannt geworden ist, damit dieser seine 72-Stunden-Meldepflicht nach Art. 33 DSGVO erfüllen kann.
- (2) Die Benachrichtigung beschreibt soweit möglich die Art der Verletzung, die Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Maßnahmen.

§ 7 Überprüfungen und Inspektionen

- (1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle zum Nachweis der Einhaltung von Art. 28 DSGVO erforderlichen Informationen zur Verfügung.
- (2) Der Auftragsverarbeiter ermöglicht und unterstützt Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten Prüfer. Überprüfungen werden mit angemessener Frist (mindestens **[14]** Tage) angekündigt, finden während der Geschäftszeiten statt und stören den Betrieb nicht unangemessen. Anerkannte Zertifizierungen oder Prüfberichte (z. B. ISO 27001, SOC 2) können zur Reduzierung von Vor-Ort-Prüfungen vorgelegt werden.

§ 8 Übermittlung in Drittländer

- (1) Der Auftragsverarbeiter übermittelt personenbezogene Daten in ein Drittland (außerhalb EU/EWR) nur auf dokumentierte Weisung des Verantwortlichen und nur, wenn eine geeignete Garantie nach Kapitel V DSGVO vorliegt (z. B. Angemessenheitsbeschluss oder EU-Standardvertragsklauseln).
- (2) Bestehende Drittlandübermittlungen und ihre Garantien sind in Anlage 3 dokumentiert.

§ 9 Löschung und Rückgabe

- (1) Nach Beendigung des Hauptvertrags löscht oder gibt der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag verarbeiteten personenbezogenen Daten zurück und löscht vorhandene Kopien, sofern keine gesetzliche Aufbewahrungspflicht nach Unions- oder mitgliedstaatlichem Recht besteht.
- (2) Der Auftragsverarbeiter bestätigt die Löschung auf Verlangen in dokumentierter Form.

§ 10 Haftung und Laufzeit

- (1) Die Haftung richtet sich nach Art. 82 DSGVO und dem Hauptvertrag. Jede Partei haftet für Schäden aus einer gegen die DSGVO verstoßenden Verarbeitung gemäß Art. 82.
- (2) Dieser Vertrag kann zusammen mit dem Hauptvertrag gekündigt werden. Die Löscho- und Rückgabepflichten nach § 9 bestehen über die Beendigung hinaus fort.

§ 11 Schlussbestimmungen

- (1) Änderungen dieses Vertrags bedürfen der dokumentierten Form. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (2) Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
- (3) Dieser Vertrag unterliegt dem Recht **[der Bundesrepublik Deutschland]**, unbeschadet zwingender Vorschriften der DSGVO. Gerichtsstand ist **[Ort]**, soweit gesetzlich zulässig.

Unterschriften

Für den Verantwortlichen

Ort, Datum

Name, Funktion

Unterschrift

Für den Auftragsverarbeiter

Ort, Datum

Name, Funktion

Unterschrift

Anlage 1 – Beschreibung der Verarbeitung

» **HINWEIS** Füllen Sie diese Anlage präzise aus – sie legt genau fest, was der Auftragsverarbeiter darf. Vage Angaben schwächen den gesamten Vertrag. Halten Sie sie konsistent mit dem entsprechenden Eintrag in Ihrem VVT.

PUNKT	ANGABEN
Gegenstand der Verarbeitung	[z. B. Bereitstellung einer CRM-Software für das Kundenmanagement]
Art und Zweck	[z. B. Speicherung, Organisation und Abruf von Kundenkontaktdaten]
Dauer	[Laufzeit des Hauptvertrags]
Kategorien betroffener Personen	[z. B. Kunden, Interessenten, Mitarbeitende des Verantwortlichen]
Arten personenbezogener Daten	[z. B. Name, geschäftliche Kontaktdaten, Kommunikationshistorie]
Besondere Kategorien (Art. 9)	[keine / angeben, z. B. Gesundheitsdaten – falls zutreffend]
Häufigkeit der Verarbeitung	[laufend / periodisch]

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32)

Der Auftragsverarbeiter setzt die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (TOM) um und erhält sie aufrecht. Die Maßnahmen sind in der TOM-Dokumentation des Auftragsverarbeiters festgehalten, die Bestandteil dieser Anlage ist und mindestens folgende Bereiche abdeckt:

- Zutrittskontrolle
- Zugangs- und Zugriffskontrolle
- Netzwerk- und Serversicherheit
- Verschlüsselung (Übertragung und Ruhezustand)
- Pseudonymisierung
- Weitergabekontrolle
- Eingabekontrolle und Datensparsamkeit
- Verfügbarkeit und Belastbarkeit (Backup, Wiederherstellung)
- Trennungskontrolle
- Auftragskontrolle (Unterauftragsverarbeiter)
- Datenschutzmanagement und Reaktion auf Vorfälle
- Datenschutz durch Technikgestaltung und Voreinstellungen

» **HINWEIS** Fügen Sie hier die ausgefüllte ETHYX-TOM-Checkliste (Art. 32) bei oder verweisen Sie auf die Sicherheitsdokumentation des Auftragsverarbeiters (z. B. ISO-27001-Zertifikat, SOC-2-Bericht). Die Bereiche oben entsprechen den Abschnitten der TOM-Checkliste.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

UNTERAUFTRAGSVERARBEITER	LEISTUNG	STANDORT	DRITTLAND-GARANTIE
[z. B. Amazon Web Services]	[Hosting / Infrastruktur]	[EU-Region / USA]	[entfällt (EU) / SVK]

UNTERAUFTRAGSVERARBEITER	LEISTUNG	STANDORT	DRITTLAND-GARANTIE
[z. B. SendGrid]	[transaktionale E-Mails]	[USA]	[SVK]
[]	[]	[]	[]
[]	[]	[]	[]

» **HINWEIS** Führen Sie jeden Unterauftragsverarbeiter und die Garantie für jeden außerhalb der EU/EWR auf. Dies muss mit Ihrem VVT und dem Abschnitt „Drittlandübermittlungen“ Ihrer Datenschutzerklärung übereinstimmen.