AUFTRAGSVERARBEITUNGSVERTRAG

gemäss Art. 28 DSGVO / Art. 9 nDSG

Data Processing Agreement (DPA) | Standard-Version | Zehnder Governance

Dieses Template ist ein rechtlich vollständiger Auftragsverarbeitungsvertrag (AVV) gemäss Art. 28 DSGVO und Art. 9 nDSG. Er regelt die Verarbeitung von Personendaten durch einen Dienstleister (Auftragsverarbeiter) im Auftrag eines Unternehmens (Verantwortlicher).

Ausfüllhinweis: Alle [PLATZHALTER] in eckigen Klammern sind durch die tatsächlichen Angaben zu ersetzen. Grau-kursive Hinweise (wie dieser) dienen der Orientierung und sind im finalen Dokument zu löschen.

VERTRAGSPARTEIEN

Dieser Auftragsverarbeitungsvertrag wird abgeschlossen zwischen:

DER VERANTWORTLICHE (Controller)
Firmenname: [FIRMENNAME VERANTWORTLICHER]
Rechtsform: [z.B. GmbH / AG / Einzelunternehmen]
Adresse: [STRASSE, PLZ ORT, LAND]
UID/Handelsregisternummer: [UID-NUMMER]
Vertreten durch: [NAME, FUNKTION]
E-Mail Datenschutz: [DATENSCHUTZ@UNTERNEHMEN.COM]
(nachfolgend "Verantwortlicher" oder "Auftraggeber")

— UND —

DER AUFTRAGSVERARBEITER (Processor)
Firmenname: [FIRMENNAME AUFTRAGSVERARBEITER]
Rechtsform: [z.B. GmbH / AG]
Adresse: [STRASSE, PLZ ORT, LAND]
UID/Handelsregisternummer: [UID-NUMMER]
Vertreten durch: [NAME, FUNKTION]
E-Mail Datenschutz: [DATENSCHUTZ@DIENSTLEISTER.COM]
(nachfolgend "Auftragsverarbeiter" oder "Auftragnehmer")

Verantwortlicher und Auftragsverarbeiter werden nachfolgend gemeinsam als "die Parteien" bezeichnet.

PRÄAMBEL

Die Parteien haben einen [BEZEICHNUNG DES HAUPTVERTRAGS, z.B. Dienstleistungsvertrag / SaaS-Vertrag / IT-Servicevertrag] vom [DATUM] abgeschlossen (nachfolgend "Hauptvertrag"). Im Rahmen der Erfüllung dieses Hauptvertrags verarbeitet der Auftragsverarbeiter im Auftrag des Verantwortlichen Personendaten.

Dieser AVV konkretisiert die datenschutzrechtlichen Pflichten der Parteien gemäss:

- Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO)
- Art. 9 des revidierten Bundesgesetzes über den Datenschutz (nDSG, in Kraft seit 1. September 2023)
- Weiteren anwendbaren Datenschutzgesetzen gemäss Anhang 1

Im Falle von Widersprüchen zwischen diesem AVV und dem Hauptvertrag hat dieser AVV in datenschutzrechtlichen Fragen Vorrang.

Art. 1 — Gegenstand und Dauer der Verarbeitung

1.1 Gegenstand

Der Auftragsverarbeiter verarbeitet Personendaten ausschliesslich im Auftrag und nach dokumentierter Weisung des Verantwortlichen. Gegenstand, Art und Zweck der Verarbeitung, die Art der Personendaten sowie die Kategorien betroffener Personen sind in Anhang 1 (Verarbeitungsbeschreibung) festgelegt.

1.2 Dauer

Dieser AVV gilt für die Dauer des Hauptvertrags. Nach Beendigung des Hauptvertrags gelten die Regelungen zu Rückgabe und Löschung (Art. 10) fort, bis die Rückgabe oder Löschung abgeschlossen ist.

Art. 2 — Weisungsgebundenheit

Der Auftragsverarbeiter verarbeitet Personendaten ausschliesslich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach dem Unionsrecht oder dem Recht des Mitgliedstaates, dem er unterliegt, zur Verarbeitung verpflichtet. In diesem Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht aus wichtigen Gründen des öffentlichen Interesses verbietet.

Weisungen des Verantwortlichen sind schriftlich zu erteilen (E-Mail ist ausreichend). Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, eine Weisung verstosse gegen geltendes Datenschutzrecht.

Weisungsberechtigte Person beim Verantwortlichen: [NAME / FUNKTION / E-MAIL]

Weisungsempfangende Person beim Auftragsverarbeiter: [NAME / FUNKTION / E-MAIL]

Art. 3 — Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der Personendaten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

Der Auftragsverarbeiter darf Personendaten nur denjenigen Mitarbeitenden zugänglich machen, die diese für die Erfüllung des Hauptvertrags benötigen (Need-to-know-Prinzip).

Art. 4 — Technische und organisatorische Massnahmen (TOMs)

Der Auftragsverarbeiter trifft alle erforderlichen technischen und organisatorischen Massnahmen gemäss Art. 32 DSGVO / Art. 8 nDSG, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die zum Zeitpunkt des Vertragsabschlusses geltenden TOMs sind in Anhang 2 (TOMs) dokumentiert.

Der Auftragsverarbeiter ist berechtigt, die TOMs zu aktualisieren, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind dem Verantwortlichen vorab schriftlich mitzuteilen.

Massnahmen umfassen insbesondere:

- Pseudonymisierung und Verschlüsselung von Personendaten (at rest und in transit)
- Massnahmen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit
- Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit
- Zugangskontrolle und Berechtigungsmanagement (Least Privilege)
- Protokollierung von Zugriffen auf Personendaten

Art. 5 — Unterauftragsverarbeiter (Sub-Processors)

5.1 Genehmigung

Der Auftragsverarbeiter darf Unterauftragsverarbeiter nur mit vorheriger schriftlicher Genehmigung des Verantwortlichen einsetzen.

Option A (Einzelgenehmigung): Jeder Unterauftragsverarbeiter bedarf einer expliziten Vorab-Genehmigung des Verantwortlichen.

Option B (Generelle Genehmigung mit Widerspruchsrecht): Der Verantwortliche erteilt hiermit eine generelle Genehmigung für die in Anhang 3 aufgeführten Unterauftragsverarbeiter. Änderungen (Hinzufügen oder Ersetzen) sind dem Verantwortlichen mindestens [30] Tage im Voraus schriftlich mitzuteilen. Der Verantwortliche kann gegen die Änderung innerhalb von [14] Tagen schriftlich Widerspruch einlegen.

Ausfüllhinweis: Eine der beiden Optionen auswählen und die andere streichen.

5.2 Pflichten bei Unterauftragsverhältnissen

Der Auftragsverarbeiter legt Unterauftragsverarbeitern dieselben Datenschutzpflichten auf, die ihm selbst gemäss diesem AVV obliegen. Er haftet gegenüber dem Verantwortlichen für die Einhaltung dieser Pflichten durch den Unterauftragsverarbeiter.

Bei Drittlandtransfers an Unterauftragsverarbeiter stellt der Auftragsverarbeiter sicher, dass geeignete Garantien im Sinne von Art. 46 DSGVO (z.B. EU-Standardvertragsklauseln) vorhanden sind.

Art. 6 — Unterstützungspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung seiner datenschutzrechtlichen Pflichten, insbesondere:

- Beantwortung von Anfragen betroffener Personen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) — Reaktion innerhalb von [5] Arbeitstagen
- Durchführung von Datenschutz-Folgeabschätzungen (DPIA/DSFA)
- Vorherige Konsultation der Aufsichtsbehörde gemäss Art. 36 DSGVO
- Bereitstellung aller für die Einhaltung der Rechenschaftspflicht erforderlichen Informationen

Die Unterstützungsleistungen gemäss diesem Artikel können, sofern sie über den vereinbarten Leistungsumfang hinausgehen, nach dem vereinbarten Stundensatz oder gemäss separater Vereinbarung vergütet werden.

Art. 7 — Meldung von Datenschutzverletzungen

Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes von Personendaten (Datenpanne) unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Bekanntwerden. Diese Frist gilt auch dann, wenn noch nicht alle Informationen vorliegen.

Die Meldung hat folgende Mindestangaben zu enthalten:

- Beschreibung der Art der Verletzung (soweit möglich)
- Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze
- Wahrscheinliche Folgen der Verletzung
- Ergriffene oder vorgeschlagene Massnahmen zur Behebung

Meldungen sind zu richten an: [E-MAIL-ADRESSE DATENSCHUTZ VERANTWORTLICHER]

Die Meldepflicht des Auftragsverarbeiters befreit den Verantwortlichen nicht von seiner eigenen gesetzlichen Pflicht, Datenschutzverletzungen innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde zu melden (Art. 33 DSGVO / Art. 24 nDSG).

Art. 8 — Audit- und Kontrollrechte

Der Verantwortliche ist berechtigt, die Einhaltung dieses AVV durch den Auftragsverarbeiter zu überprüfen. Audits können durchgeführt werden durch:

- Selbstauskunft des Auftragsverarbeiters (Fragebögen, Zertifikatsnachweise)
- Inspektion beim Auftragsverarbeiter — mit [10] Arbeitstagen Voranmeldung, maximal 1x pro Jahr
- Beauftragung eines unabhängigen, zur Vertraulichkeit verpflichteten Dritten

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zur Verfügung und kooperiert bei Audits. Audit-Kosten trägt grundsätzlich der Verantwortliche; bei festgestellten wesentlichen Verstössen trägt der Auftragsverarbeiter die Kosten.

Anerkannte Zertifizierungen (z.B. ISO 27001, SOC 2) oder Testate können als Nachweis dienen und Audits ersetzen oder reduzieren.

Art. 9 — Internationale Datentransfers

Eine Übermittlung von Personendaten in Drittländer (ausserhalb EU/EWR/Schweiz) durch den Auftragsverarbeiter oder seine Unterauftragsverarbeiter ist nur zulässig, wenn:

- der Verantwortliche vorab schriftlich zugestimmt hat, und
- ein Angemessenheitsbeschluss der EU-Kommission oder der EU-Standardvertragsklauseln (SCCs, Beschluss 2021/914/EU) oder eine andere geeignete Garantie gemäss Art. 46 DSGVO vorliegt, und
- für Transfers aus der Schweiz zusätzlich die Anforderungen des nDSG und der EDÖB-Anerkennungsliste erfüllt sind.

Derzeit autorisierte Drittland-Transfers: [LAND / EMPFÄNGER / TRANSFERMECHANISMUS] — siehe Anhang 3.

Ausfüllhinweis: Falls keine Drittlandtransfers stattfinden, diesen Absatz entsprechend anpassen oder streichen.

Art. 10 — Rückgabe und Löschung nach Vertragsende

Nach Beendigung des Hauptvertrags hat der Auftragsverarbeiter sämtliche Personendaten nach Wahl des Verantwortlichen:

- vollständig zurückzugeben (in einem gängigen, maschinenlesbaren Format), oder
- vollständig und nachweislich zu löschen,

sofern keine gesetzliche Pflicht zur weiteren Aufbewahrung besteht.

Die Rückgabe oder Löschung hat innerhalb von [30] Tagen nach Vertragsbeendigung zu erfolgen. Der Auftragsverarbeiter bestätigt die Löschung schriftlich.

Gesetzliche Aufbewahrungspflichten des Auftragsverarbeiters bleiben unberührt. In diesem Fall verarbeitet der Auftragsverarbeiter die betreffenden Daten bis zum Ablauf der Frist auf das unbedingt notwendige Mass beschränkt.

Art. 11 — Haftung

Jede Partei haftet für Schäden, die durch eine Verletzung dieses AVV oder des anwendbaren Datenschutzrechts entstehen, nach Massgabe der gesetzlichen Bestimmungen (insb. Art. 82 DSGVO).

Im Aussenverhältnis gegenüber betroffenen Personen haften der Verantwortliche und der Auftragsverarbeiter gesamtschuldnerisch. Im Innenverhältnis trägt jede Partei den Schadensanteil, der ihrem Verschulden entspricht.

Die Haftung des Auftragsverarbeiters für Schäden aus diesem AVV ist — soweit gesetzlich zulässig — auf [BETRAG / z.B. CHF 500'000 oder den Jahreswert des Hauptvertrags] begrenzt.

Ausfüllhinweis: Haftungsbeschränkung ist verhandelbar. Für regulierte Bereiche (Gesundheit, Finanz) keine oder höhere Limite vereinbaren.

Art. 12 — Schlussbestimmungen

12.1 Anwendbares Recht und Gerichtsstand

Dieser AVV untersteht dem Recht [der Europäischen Union und des Staates / der Schweiz] [LAND/KANTON EINFÜGEN]. Gerichtsstand ist [ORT].

Ausfüllhinweis: Bei CH-Unternehmen typischerweise Schweizer Recht; bei EU-Unternehmen Recht des jeweiligen Mitgliedstaats. Beide können nebeneinander gelten.

12.2 Schriftform

Änderungen und Ergänzungen dieses AVV bedürfen der Schriftform. Elektronische Kommunikation (E-Mail mit qualifizierter elektronischer Signatur oder im gegenseitigen Einvernehmen) gilt als schriftlich.

12.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses AVV unwirksam oder undurchführbar sein, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck der ursprünglichen Regelung möglichst nahekommt.

12.4 Verhältnis zu anderen Vereinbarungen

Dieser AVV ersetzt alle vorherigen Vereinbarungen der Parteien zum Thema Datenverarbeitung. Im Übrigen bleibt der Hauptvertrag unberührt.

UNTERSCHRIFTEN

Durch Unterzeichnung bestätigen die Parteien, den vorliegenden AVV gelesen, verstanden und akzeptiert zu haben.

FÜR DEN VERANTWORTLICHEN:		FÜR DEN AUFTRAGSVERARBEITER:
_____ *Ort, Datum*		_____ *Ort, Datum*
_____ *Unterschrift, Name, Funktion*		_____ *Unterschrift, Name, Funktion*

ANHANG 1 — Verarbeitungsbeschreibung (Art. 28 Abs. 3 DSGVO)

Ausfüllhinweis: Dieser Anhang ist für jede Verarbeitung spezifisch auszufüllen. Er ist das Herzstück des AVV.

Verarbeitungsbeschreibung	
Gegenstand der Verarbeitung	[z.B. Betrieb einer SaaS-HR-Plattform, Hosting von Kundendaten, E-Mail-Marketing-Dienstleistungen]
Zweck der Verarbeitung	[z.B. Verwaltung von Mitarbeiterdaten, Versand von Marketing-E-Mails, Cloud-Hosting]
Art der Verarbeitung	[z.B. Speicherung, Übermittlung, Analyse, Pseudonymisierung]
Kategorien betroffener Personen	[z.B. Mitarbeitende des Verantwortlichen / Kunden des Verantwortlichen / Bewerber]
Kategorien von Personendaten	[z.B. Stammdaten (Name, Adresse), Kontaktdaten (E-Mail, Telefon), HR-Daten (Lohn, Abwesenheiten), Zahlungsdaten]
Besondere Kategorien (Art. 9 DSGVO)	[Falls zutreffend: z.B. Gesundheitsdaten, biometrische Daten — andernfalls: 'Nicht zutreffend']
Standorte der Verarbeitung	[z.B. Rechenzentrum Frankfurt (EU), Backup Zürich (CH)]
Löschfristen	[z.B. Löschung 30 Tage nach Vertragsende / gemäss gesetzlicher Aufbewahrungspflicht]

ANHANG 2 — Technische und Organisatorische Massnahmen (TOMs)

Ausfüllhinweis: Der Auftragsverarbeiter füllt diesen Anhang aus. Die Angaben sollten spezifisch und nachprüfbar sein — nicht nur allgemeine Aussagen.

Massnahme	Status	Konkrete Umsetzung
Zutrittskontrolle		
Physische Zugangskontrolle zu Rechenzentren	[ ] Umgesetzt	*[z.B. Schlüsselkarten, Biometrie, Videoüberwachung]*
Zugangskontrolle (logisch)		
Multi-Faktor-Authentifizierung (MFA)	[ ] Umgesetzt	*[z.B. TOTP-App, Hardware-Token, SMS — für alle Admin-Zugänge]*
Rollen- und Berechtigungskonzept (Least Privilege)	[ ] Umgesetzt	*[z.B. RBAC-System, quartalsweise Review der Berechtigungen]*
Verschlüsselung & Übertragungssicherheit		
Verschlüsselung at rest	[ ] Umgesetzt	*[z.B. AES-256 für alle gespeicherten Personendaten]*
Verschlüsselung in transit (TLS)	[ ] Umgesetzt	*[z.B. TLS 1.2 oder höher für alle Datenübertragungen]*
Verfügbarkeit & Wiederherstellung		
Backup & Restore (regelmässig getestet)	[ ] Umgesetzt	*[z.B. tägliche Backups, monatlicher Restore-Test, RPO/RTO]*
Logging & Monitoring	[ ] Umgesetzt	*[z.B. SIEM-System, Anomalieerkennung, 90 Tage Logaufbewahrung]*

ANHANG 3 — Unterauftragsverarbeiter

Ausfüllhinweis: Alle eingesetzten Unterauftragsverarbeiter auflisten. Typische Beispiele: AWS (Hosting), Sendgrid (E-Mail), Stripe (Zahlung).

Unterauftragsverarbeiter	Sitz / Land	Transfermechanismus	Zweck
[z.B. Amazon Web Services]	*[z.B. USA / EU-West]*	*[z.B. EU SCCs / Angemessenheit]*	*[z.B. Cloud-Hosting, Datenspeicherung]*
[Unterauftragsverarbeiter 2]	[ ]	[ ]	[ ]

RECHTLICHER HINWEIS: Dieses Template wurde von Zehnder Governance sorgfältig erstellt und basiert auf dem Stand der DSGVO, nDSG und UK GDPR (März 2026). Es ersetzt keine individuelle Rechtsberatung. Für regulierte Sektoren (Gesundheit, Finanzdienstleistungen, kritische Infrastruktur) oder komplexe Verarbeitungen empfiehlt sich eine individuelle rechtliche Prüfung. Zehnder Governance übernimmt keine Haftung für die vollständige Rechtmässigkeit des ausgefüllten Dokuments.