

AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

gemäß Art. 28 DSGVO

zwischen

Verantwortlicher / Auftraggeber

Unternehmen / Name: _____

Rechtsform: _____

Anschrift / Sitz: _____

Vertreten durch: _____

– nachfolgend „Verantwortlicher“ genannt –

und

Auftragsverarbeiter / Auftragnehmer

Unternehmen / Name: _____

Rechtsform: _____

Anschrift / Sitz: _____

Vertreten durch: _____

– nachfolgend „Auftragsverarbeiter“ genannt –

wird folgende Vereinbarung zur Auftragsverarbeitung geschlossen.

§ 1 Gegenstand der Vereinbarung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Zusammenhang mit folgendem Hauptvertrag beziehungsweise folgender Leistung:

Bezeichnung des Hauptvertrages / Dienstes:

Vertragsdatum:

Beschreibung der Leistung:

Diese Vereinbarung ergänzt den zugrunde liegenden Hauptvertrag um die datenschutzrechtlichen Regelungen zur Verarbeitung personenbezogener Daten im Auftrag.

§ 2 Dauer der Verarbeitung

Die Verarbeitung beginnt am:

und dauert:

- ☐ bis zur Beendigung des Hauptvertrages.
- ☐ bis zum _____.
- ☐ für folgenden Zeitraum:
- ☐ solange personenbezogene Daten aufgrund des Auftrags verarbeitet werden.

§ 3 Art der Verarbeitung

Die Verarbeitung umfasst insbesondere:

- ☐ Erheben
- ☐ Erfassen
- ☐ Organisieren
- ☐ Ordnen
- ☐ Speichern
- ☐ Anpassen
- ☐ Verändern
- ☐ Auslesen
- ☐ Abfragen
- ☐ Verwenden
- ☐ Übermitteln
- ☐ Bereitstellen

- ☐ Abgleichen
- ☐ Verknüpfen
- ☐ Einschränken
- ☐ Löschen
- ☐ Vernichten
- ☐ sonstige Verarbeitung:

§ 4 Zweck der Verarbeitung

Die Verarbeitung erfolgt ausschließlich zu folgenden Zwecken:

- ☐ Hosting
- ☐ IT-Betrieb
- ☐ Cloud-Speicherung
- ☐ Kundenverwaltung
- ☐ Newsletter-Versand
- ☐ Support
- ☐ Wartung
- ☐ Lohn- / Gehaltsabrechnung
- ☐ Buchhaltung
- ☐ Analyse
- ☐ Softwarebereitstellung
- ☐ Datensicherung
- ☐ sonstiger Zweck:

§ 5 Kategorien personenbezogener Daten

Verarbeitet werden insbesondere:

- ☐ Stammdaten

- ☐ Name
- ☐ Anschrift
- ☐ Kontaktdaten
- ☐ E-Mail-Adresse
- ☐ Telefonnummer
- ☐ Kundennummer
- ☐ Vertragsdaten
- ☐ Rechnungsdaten
- ☐ Zahlungsdaten
- ☐ Bankdaten
- ☐ Nutzungsdaten
- ☐ Protokolldaten
- ☐ IP-Adressen
- ☐ Zugangsdaten
- ☐ Kommunikationsdaten
- ☐ Beschäftigtendaten
- ☐ Bewerberdaten
- ☐ Standortdaten
- ☐ Bild- / Videodaten
- ☐ sonstige personenbezogene Daten:

§ 6 Besondere Kategorien personenbezogener Daten

Es werden:

- ☐ keine besonderen Kategorien personenbezogener Daten verarbeitet.
- ☐ folgende besonderen Kategorien personenbezogener Daten verarbeitet:
- ☐ Gesundheitsdaten

- ☐ biometrische Daten
- ☐ genetische Daten
- ☐ Daten zur religiösen oder weltanschaulichen Überzeugung
- ☐ Daten zur Gewerkschaftszugehörigkeit
- ☐ Daten zur sexuellen Orientierung / zum Sexualleben
- ☐ Daten zur politischen Meinung
- ☐ Daten zur rassischen oder ethnischen Herkunft
- ☐ sonstige besondere Daten:

Zusätzliche Schutzmaßnahmen:

§ 7 Kategorien betroffener Personen

Betroffene Personen sind:

- ☐ Kunden
- ☐ Interessenten
- ☐ Newsletter-Empfänger
- ☐ Websitebesucher
- ☐ Mitarbeiter
- ☐ Bewerber
- ☐ Lieferanten
- ☐ Ansprechpartner bei Geschäftspartnern
- ☐ Nutzer / Mitglieder
- ☐ Patienten / Mandanten / Klienten
- ☐ sonstige Personen:

§ 8 Weisungsgebundenheit

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, soweit nicht eine gesetzliche Verpflichtung zu einer anderen Verarbeitung besteht.

Weisungen können insbesondere betreffen:

- Art und Umfang der Verarbeitung,
- Zweck der Verarbeitung,
- Speicherdauer,
- Löschung,
- Übermittlung,
- technische Verarbeitungsvorgänge.

Art. 28 Abs. 3 DSGVO sieht ausdrücklich vor, dass die Verarbeitung grundsätzlich nur auf dokumentierte Weisung des Verantwortlichen erfolgen darf.

§ 9 Weisungsberechtigte Personen

Weisungsberechtigt auf Seiten des Verantwortlichen sind:

Name: _____

Funktion: _____

E-Mail: _____

Weitere weisungsberechtigte Personen:

§ 10 Weisungsempfänger

Weisungen werden auf Seiten des Auftragsverarbeiters entgegengenommen durch:

Name / Funktion: _____

E-Mail: _____

Alternativer Kontakt:

§ 11 Form der Weisungen

Weisungen erfolgen:

☐ per E-Mail

- ☐ schriftlich
- ☐ über Ticketsystem
- ☐ über Kundenportal
- ☐ telefonisch mit anschließender Dokumentation
- ☐ in anderer dokumentierter Form:

§ 12 Unzulässige Weisungen

Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen Datenschutzrecht verstößt, informiert er den Verantwortlichen unverzüglich.

Die Durchführung der betreffenden Weisung wird:

- ☐ bis zur Klärung ausgesetzt, soweit rechtlich zulässig.
- ☐ nach folgender Regelung behandelt:

§ 13 Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass Personen, die zur Verarbeitung personenbezogener Daten befugt sind:

- zur Vertraulichkeit verpflichtet wurden oder
- einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Zugriff erhalten nur Personen, die diesen für die Durchführung des Auftrags benötigen.

§ 14 Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten.

Die Maßnahmen werden in

Anlage 1 – Technische und organisatorische Maßnahmen (TOMs)

dokumentiert.

Sie umfassen insbesondere, soweit für die konkrete Verarbeitung angemessen:

- ☐ Zutrittskontrolle
- ☐ Zugangskontrolle

- ☐ Zugriffskontrolle
- ☐ Verschlüsselung
- ☐ Pseudonymisierung
- ☐ Datensicherung
- ☐ Wiederherstellungsverfahren
- ☐ Protokollierung
- ☐ Berechtigungsmanagement
- ☐ Malware-Schutz
- ☐ Update- / Patchmanagement
- ☐ Backup-Konzept
- ☐ Löschkonzept
- ☐ Verfügbarkeitsmaßnahmen
- ☐ regelmäßige Überprüfung der Schutzmaßnahmen
- ☐ sonstige Maßnahme:

§ 15 Anpassung der TOMs

Technische und organisatorische Maßnahmen dürfen im Rahmen des technischen Fortschritts weiterentwickelt werden.

Dabei darf das vereinbarte Schutzniveau nicht unangemessen unterschritten werden.

Wesentliche Änderungen werden:

- ☐ dem Verantwortlichen mitgeteilt.
- ☐ auf Anfrage dokumentiert.
- ☐ nach folgender Regelung mitgeteilt:

§ 16 Unterstützung bei Betroffenenrechten

Der Auftragsverarbeiter unterstützt den Verantwortlichen im erforderlichen Umfang bei der Erfüllung von Betroffenenrechten.

Dies betrifft insbesondere Anträge auf:

- ☐ Auskunft
- ☐ Berichtigung
- ☐ Löschung
- ☐ Einschränkung der Verarbeitung
- ☐ Datenübertragbarkeit
- ☐ Widerspruch
- ☐ sonstige Betroffenenrechte

Geht ein entsprechender Antrag unmittelbar beim Auftragsverarbeiter ein, wird dieser grundsätzlich unverzüglich an den Verantwortlichen weitergeleitet.

§ 17 Datenschutzverletzungen

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn ihm eine Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit dem Auftrag bekannt wird.

Die Meldung soll – soweit verfügbar – insbesondere enthalten:

- Art des Vorfalls,
- betroffene Daten,
- betroffene Personengruppen,
- voraussichtliche Folgen,
- bereits ergriffene Maßnahmen,
- Ansprechpartner.

Meldeweg:

§ 18 Unterstützung bei Melde- und Informationspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen der ihm zur Verfügung stehenden Informationen bei der Erfüllung gesetzlicher Pflichten im Zusammenhang mit Datenschutzverletzungen.

Die Verantwortung für die Entscheidung über eine Meldung an eine Aufsichtsbehörde beziehungsweise Information betroffener Personen verbleibt beim Verantwortlichen, soweit gesetzlich nichts anderes bestimmt ist.

§ 19 Datenschutz-Folgenabschätzung

Soweit die Voraussetzungen vorliegen, unterstützt der Auftragsverarbeiter den Verantwortlichen im angemessenen Umfang bei:

- ☐ Datenschutz-Folgenabschätzungen
- ☐ vorherigen Konsultationen der Aufsichtsbehörde
- ☐ Risikobewertungen
- ☐ Dokumentation technischer Maßnahmen
- ☐ sonstigen Maßnahmen:

§ 20 Unterauftragsverarbeiter

Der Auftragsverarbeiter darf weitere Auftragsverarbeiter einsetzen:

- ☐ nur nach vorheriger gesonderter Genehmigung.
- ☐ aufgrund einer allgemeinen schriftlichen Genehmigung.

Art. 28 Abs. 2 DSGVO sieht vor, dass weitere Auftragsverarbeiter nur mit vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung des Verantwortlichen eingesetzt werden dürfen. Bei allgemeiner Genehmigung ist über geplante Änderungen zu informieren, damit der Verantwortliche widersprechen kann.

§ 21 Bereits genehmigte Unterauftragsverarbeiter

Folgende Unterauftragsverarbeiter sind genehmigt:

Unternehmen	Leistung	Standort / Land

§ 22 Änderungen bei Unterauftragsverarbeitern

Bei allgemeiner Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen über:

- Aufnahme neuer Unterauftragsverarbeiter,
- Ersetzung bestehender Unterauftragsverarbeiter.

Informationsfrist:

_____ **Tage vor der Änderung**

Der Verantwortliche kann aus nachvollziehbaren datenschutzrechtlichen Gründen innerhalb von

_____ **Tagen**

widersprechen.

Verfahren bei Widerspruch:

§ 23 Pflichten der Unterauftragsverarbeiter

Der Auftragsverarbeiter stellt sicher, dass Unterauftragsverarbeiter Datenschutzpflichten übernehmen, die den für die konkrete Unterauftragsverarbeitung erforderlichen Pflichten dieses Vertrages entsprechen.

Erfüllt ein weiterer Auftragsverarbeiter seine Datenschutzpflichten nicht, bleibt der ursprüngliche Auftragsverarbeiter nach Art. 28 DSGVO gegenüber dem Verantwortlichen grundsätzlich für die Erfüllung der Pflichten des weiteren Auftragsverarbeiters verantwortlich.

§ 24 Verarbeitung innerhalb der EU / des EWR

Die Verarbeitung erfolgt:

- ☐ ausschließlich innerhalb der Europäischen Union / des Europäischen Wirtschaftsraums.
- ☐ teilweise außerhalb der EU / des EWR.

Verarbeitungsstandorte:

§ 25 Drittlandübermittlungen

Eine Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation erfolgt:

- ☐ nicht.

☐ nur nach dokumentierter Weisung des Verantwortlichen und bei Vorliegen der gesetzlichen Voraussetzungen.

Betroffene Länder:

Übermittlungsmechanismus:

- ☐ Angemessenheitsbeschluss
- ☐ Standardvertragsklauseln
- ☐ andere geeignete Garantien
- ☐ sonstige Rechtsgrundlage:

Erforderliche zusätzliche Schutzmaßnahmen:

§ 26 Kontroll- und Nachweispflichten

Der Auftragsverarbeiter stellt dem Verantwortlichen die Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Pflichten aus dieser Vereinbarung angemessen nachzuweisen.

Nachweise können insbesondere erfolgen durch:

- ☐ Zertifizierungen
- ☐ Auditberichte
- ☐ Sicherheitsberichte
- ☐ TOM-Dokumentation
- ☐ Fragebögen
- ☐ unabhängige Prüfberichte
- ☐ sonstige Nachweise:

§ 27 Audits und Kontrollen

Der Verantwortliche darf die Einhaltung der vereinbarten Datenschutzpflichten im angemessenen Umfang kontrollieren beziehungsweise durch einen zur Vertraulichkeit verpflichteten Dritten kontrollieren lassen.

Kontrollen erfolgen grundsätzlich:

- mit angemessener Vorankündigung,
- während üblicher Geschäftszeiten,
- unter angemessener Rücksichtnahme auf Betriebs- und Geschäftsgeheimnisse.

Vorankündigungsfrist:

_____ **Werktage**

Ausnahmen bei dringendem Anlass:

§ 28 Kosten von Kontrollen

- ☐ Normale Nachweise sind mit der Vergütung des Hauptvertrages abgegolten.
- ☐ Außergewöhnlich aufwendige Vor-Ort-Audits können nach vorheriger Abstimmung berechnet werden.
- ☐ folgende Regelung:

Zwingende gesetzliche Kontrollrechte bleiben unberührt.

§ 29 Löschung und Rückgabe nach Vertragsende

Nach Beendigung der Verarbeitung werden personenbezogene Daten nach Wahl des Verantwortlichen:

- ☐ zurückgegeben und anschließend gelöscht.
- ☐ gelöscht.
- ☐ nach folgender Weisung behandelt:

Ausgenommen sind Daten, deren weitere Speicherung gesetzlich vorgeschrieben ist.

§ 30 Löschbestätigung

Nach Abschluss der Löschung:

- ☐ stellt der Auftragsverarbeiter auf Anfrage eine Bestätigung aus.
- ☐ wird automatisch eine Löschbestätigung erstellt.
- ☐ gilt folgende Regelung:

§ 31 Sicherungskopien / Backups

Personenbezogene Daten können nach einer Löschung technisch noch in Sicherungskopien enthalten sein.

Backup-Aufbewahrungsdauer:

_____ **Tage / Wochen / Monate**

Sicherungskopien werden:

- ☐ nicht mehr produktiv verwendet.
- ☐ nach Ablauf des Backup-Zyklus überschrieben.
- ☐ nach folgender Regelung gelöscht:

§ 32 Herausgabe von Daten

Auf Anweisung des Verantwortlichen stellt der Auftragsverarbeiter Daten in folgendem Format bereit:

- ☐ CSV
- ☐ XML
- ☐ JSON
- ☐ Datenbankexport
- ☐ PDF
- ☐ Originalformat
- ☐ anderes Format:

§ 33 Verantwortlichkeit

Der Verantwortliche bleibt für die Rechtmäßigkeit der Verarbeitung, insbesondere für:

- Rechtsgrundlagen,
- Informationspflichten,
- Betroffenenrechte,

- Zweckfestlegung

verantwortlich, soweit die DSGVO diese Verantwortung ihm zuweist.

Der Auftragsverarbeiter ist für die Einhaltung der unmittelbar für ihn geltenden Datenschutzpflichten verantwortlich.

§ 34 Eigenständige Verarbeitung

Der Auftragsverarbeiter darf die im Auftrag verarbeiteten personenbezogenen Daten nicht für eigene, mit dem Auftrag unvereinbare Zwecke verwenden.

Soweit der Auftragsverarbeiter Zwecke und Mittel einer Verarbeitung selbst bestimmt, kann er insoweit datenschutzrechtlich als Verantwortlicher einzuordnen sein. Art. 28 Abs. 10 DSGVO enthält hierfür ausdrücklich eine entsprechende Regelung.

§ 35 Datenschutzbeauftragter / Datenschutzkontakt

Verantwortlicher

Datenschutzbeauftragter / Ansprechpartner:

E-Mail:

Auftragsverarbeiter

Datenschutzbeauftragter / Ansprechpartner:

E-Mail:

§ 36 Behördenanfragen

Erhält der Auftragsverarbeiter eine behördliche Anfrage zu im Auftrag verarbeiteten personenbezogenen Daten, informiert er den Verantwortlichen, soweit dies rechtlich zulässig ist.

Zwingende gesetzliche Offenlegungspflichten bleiben unberührt.

§ 37 Verzeichnis von Verarbeitungstätigkeiten

Der Auftragsverarbeiter erfüllt die für ihn geltenden gesetzlichen Dokumentationspflichten.

Soweit erforderlich, stellt der Verantwortliche dem Auftragsverarbeiter die notwendigen Informationen über die Auftragsverarbeitung zur Verfügung.

§ 38 Änderungen der Verarbeitung

Wesentliche Änderungen an:

- Zweck,
- Datenarten,
- Personengruppen,
- Verarbeitungssystemen,
- Standorten

werden dokumentiert und, soweit erforderlich, vor Umsetzung abgestimmt.

Änderungsverfahren:

§ 39 Rangfolge

Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag haben hinsichtlich der datenschutzrechtlichen Auftragsverarbeitung die Regelungen dieses AVV Vorrang, soweit zwingendes Recht nichts anderes bestimmt.

§ 40 Haftung

Die Haftung richtet sich nach den gesetzlichen Vorschriften und ergänzend nach wirksamen Regelungen des Hauptvertrages.

Zwingende datenschutzrechtliche Haftungsvorschriften bleiben unberührt.

§ 41 Vertragsdauer

Diese Vereinbarung gilt:

- ☐ für die Laufzeit des Hauptvertrages.
- ☐ bis zur vollständigen Beendigung der Verarbeitung personenbezogener Daten.
- ☐ bis zum:

§ 42 Anlagen

Bestandteil dieser Vereinbarung sind:

- ☐ Anlage 1 – Technische und organisatorische Maßnahmen
- ☐ Anlage 2 – Unterauftragsverarbeiter
- ☐ Anlage 3 – Verarbeitungstätigkeiten / Leistungsbeschreibung
- ☐ Anlage 4 – Drittlandübermittlungen
- ☐ Anlage 5 – Weisungsberechtigte Ansprechpartner
- ☐ Sonstige:

ANLAGE 1 – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

1. Zutrittskontrolle

Maßnahmen zum Schutz physischer Verarbeitungsorte:

- ☐ Schließsystem
- ☐ Zugangskarten
- ☐ Besuchermanagement
- ☐ Alarmanlage
- ☐ Rechenzentrum mit kontrolliertem Zutritt
- ☐ sonstige Maßnahme:

2. Zugangskontrolle

- ☐ individuelle Benutzerkonten
- ☐ sichere Passwortrichtlinie
- ☐ Mehrfaktor-Authentifizierung
- ☐ automatische Sperrung
- ☐ zentrale Benutzerverwaltung
- ☐ sonstige Maßnahme:

3. Zugriffskontrolle

- ☐ Rollen- und Berechtigungskonzept
- ☐ Need-to-know-Prinzip
- ☐ regelmäßige Berechtigungsprüfung
- ☐ Protokollierung administrativer Zugriffe
- ☐ sonstige Maßnahme:

4. Verschlüsselung

- ☐ Transportverschlüsselung
- ☐ Verschlüsselung gespeicherter Daten
- ☐ verschlüsselte Backups
- ☐ Verschlüsselung mobiler Geräte
- ☐ andere Maßnahmen:

5. Datensicherung und Verfügbarkeit

- ☐ regelmäßige Backups
- ☐ räumlich getrennte Sicherung
- ☐ Wiederherstellungstests
- ☐ Notfallplan
- ☐ redundante Systeme
- ☐ unterbrechungsfreie Stromversorgung
- ☐ sonstige Maßnahme:

6. Integrität und Protokollierung

- ☐ Logging

- ☐ Änderungsprotokolle
- ☐ Malware-Schutz
- ☐ Patchmanagement
- ☐ Monitoring
- ☐ sonstige Maßnahme:

7. Löschung und Datenträger

- ☐ Löschkonzept
- ☐ sichere Datenträgervernichtung
- ☐ geregelte Wiederverwendung
- ☐ automatisierte Löschfristen
- ☐ sonstige Maßnahme:

8. Organisation

- ☐ Datenschutzrichtlinien
- ☐ Mitarbeiterschulungen
- ☐ Vertraulichkeitsverpflichtungen
- ☐ Incident-Response-Prozess
- ☐ regelmäßige Sicherheitsüberprüfung
- ☐ Dienstleistermanagement
- ☐ sonstige Maßnahme:

ANLAGE 2 – UNTERAUFTRAGSVERARBEITER

Unternehmen	Anschrift	Leistung	Verarbeitungsor
n	t	g	t

ANLAGE 3 – BESCHREIBUNG DER VERARBEITUNG

Gegenstand:

Dauer:

Art der Verarbeitung:

Zweck:

Datenkategorien:

Betroffene Personen:

Hinweis

Diese Vorlage ist ein allgemeines Muster und ersetzt keine individuelle rechtliche oder datenschutzrechtliche Beratung.

Vor Verwendung sollte insbesondere geprüft werden, ob tatsächlich eine Auftragsverarbeitung vorliegt. Nicht jede Weitergabe personenbezogener Daten an einen Dienstleister ist automatisch eine Auftragsverarbeitung.

Auch technische und organisatorische Maßnahmen können nicht sinnvoll als identische Standardliste für jeden Anbieter verwendet werden. Sie müssen zum konkreten Risiko, zur Datenart und zum eingesetzten Verarbeitungssystem passen.

Unterschriften

Ort: _____

Datum: _____

Verantwortlicher

Name / Funktion: _____

Unterschrift: _____

Auftragsverarbeiter

Name / Funktion: _____

Unterschrift: _____