

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG (AVV) gem. Art. 28 DSGVO

zwischen

(1) Verantwortlicher (Auftraggeber):

[Unternehmen] :::

[Adresse] :::

[Vertreten durch] :::

[Kontakt Datenschutz/IT] :::

und

(2) Auftragsverarbeiter (Auftragnehmer):

AddProcess GmbH

Tuchmacher Straße 20, 14482 Potsdam

Vertreten durch: [Geschäftsführer]

E-Mail: datenschutz@addprocess.de / support@addprocess.de

(„Auftragsverarbeiter“)

Präambel

Der Verantwortliche beauftragt den Auftragsverarbeiter mit IT-Dienstleistungen (z.B. Support, Administration, Beratung, Betrieb/Monitoring) bei denen eine Verarbeitung personenbezogener Daten im Auftrag erfolgen kann. Diese AVV regelt die datenschutzrechtlichen Pflichten der Parteien.

1. Gegenstand, Dauer und Umfang

1.1 Gegenstand: Erbringung von IT-Dienstleistungen gemäß Hauptvertrag/Leistungsbeschreibung/SLA, insbesondere:

- IT-Support/Helpdesk, Ticketbearbeitung
- Administration von Systemen/Identitäten (z.B. AD/Entra/M365)
- Betrieb/Überwachung, Wartung, Patch-/Update-Unterstützung

- Backup-/Restore-Unterstützung (sofern vereinbart)
- Projektleistungen (Migration/Einrichtung) (sofern vereinbart)

1.2 Dauer: Diese AVV gilt für die Laufzeit des Hauptvertrages und endet automatisch mit dessen Beendigung, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

1.3 Ort der Verarbeitung: [EU/EWR], sowie soweit erforderlich die Standorte von Unterauftragsverarbeitern (siehe Anlage 3).

2. Art und Zweck der Verarbeitung

2.1 Art der Verarbeitung: Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen/Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Abgleich/Verknüpfung, Einschränken, Löschen/Vernichten.

2.2 Zwecke: Durchführung des IT-Betriebs, Support/Fehlerbehebung, Administration, Sicherheit, Dokumentation, Kommunikation mit Anwendern, Wiederherstellung im Störfall.

3. Kategorien betroffener Personen und personenbezogener Daten

3.1 Betroffene Personen (Beispiele):

- Beschäftigte des Verantwortlichen
- Kunden/Interessenten des Verantwortlichen
- Lieferanten/Dienstleister des Verantwortlichen
- Website-Nutzer (falls Web/Tracking-Services beauftragt)

3.2 Datenkategorien (Beispiele):

- Stammdaten (Name, Anschrift, Kontaktdaten)
- Account-/Benutzerdaten (Login, Rollen, Berechtigungen)
- Kommunikationsdaten (E-Mail, Chat, Tickets, Telefonie-Metadaten)
- Vertrags- und Abrechnungsdaten (soweit im Support erforderlich)
- Protokoll-/Logdaten (IP, Zeitstempel, Geräte-/Systeminfos)

3.3 Besondere Kategorien i.S.d. Art. 9 DSGVO:

werden nicht verarbeitet

[] können verarbeitet werden (nur nach dokumentierter Weisung; zusätzliche Schutzmaßnahmen Anlage 2)

4. Weisungsrecht des Verantwortlichen

4.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen (Art. 28 Abs. 3 lit. a DSGVO), außer bei rechtlicher Verpflichtung.

4.2 Weisungen erfolgen in Textform (z.B. E-Mail, Ticket). Mündliche Weisungen sind unverzüglich zu bestätigen.

4.3 Erkennt der Auftragsverarbeiter eine Weisung als rechtswidrig, informiert er den Verantwortlichen unverzüglich.

5. Pflichten des Auftragsverarbeiters

5.1 Vertraulichkeit: Der Auftragsverarbeiter verpflichtet alle zur Verarbeitung befugten Personen auf Vertraulichkeit.

5.2 Sicherheit/TOM: Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO (siehe Anlage 2).

5.3 Unterstützung: Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Maßgabe von Art. 28 Abs. 3 lit. f DSGVO bei:

- Betroffenenrechten (Art. 12–22 DSGVO)
- Meldung von Verletzungen (Art. 33/34 DSGVO)
- Datenschutz-Folgenabschätzung (Art. 35 DSGVO) soweit relevant

5.4 Verzeichnis/Compliance: Der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

5.5 Rückgabe/Löschung: Nach Vertragsende löscht oder gibt der Auftragsverarbeiter personenbezogene Daten nach Weisung zurück, soweit keine gesetzliche Aufbewahrungspflicht besteht (Ziff. 11).

6. Unterauftragsverarbeiter (Subprocessor)

6.1 Der Auftragsverarbeiter darf Unterauftragsverarbeiter einsetzen, sofern:

- (a) der Verantwortliche vorab allgemein oder im Einzelfall genehmigt hat und
- (b) ein Vertrag nach Art. 28 DSGVO mit dem Unterauftragsverarbeiter besteht.

6.2 Allgemeine Genehmigung:

Der Verantwortliche erteilt eine allgemeine Genehmigung für die in Anlage 3 gelisteten Unterauftragsverarbeiter. Der Auftragsverarbeiter informiert über beabsichtigte Änderungen (Hinzufügung/Wechsel) in Textform mit einer Frist von 14 Tagen; der Verantwortliche kann aus wichtigem Grund widersprechen.

6.3 Der Auftragsverarbeiter bleibt für die Leistung der Unterauftragsverarbeiter verantwortlich.

7. Drittlandübermittlungen

7.1 Datenübermittlungen in Drittländer erfolgen nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss, SCC, zusätzliche Maßnahmen).

7.2 Details zu Drittländern/Schutzmechanismen sind in Anlage 3 zu dokumentieren.

8. Meldung von Datenschutzverletzungen

8.1 Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens binnen 48 Stunden nach Bekanntwerden, mit:

- Art der Verletzung, Kategorien/Umfang
- voraussichtliche Folgen
- ergriffene/empfohlene Maßnahmen
- Kontaktstelle

8.2 Der Auftragsverarbeiter unterstützt bei Meldung an Aufsichtsbehörden/Betroffene.

9. Betroffenenanfragen

9.1 Erhält der Auftragsverarbeiter eine Anfrage eines Betroffenen, leitet er sie unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht eigenständig, außer nach Weisung.

10. Kontroll- und Auditrechte

10.1 Der Verantwortliche ist berechtigt, die Einhaltung dieser AVV nach angemessener Ankündigung während üblicher Geschäftszeiten zu prüfen (Audit), unter Wahrung von Betriebs- und Geschäftsgeheimnissen.

10.2 Alternativ kann der Auftragsverarbeiter geeignete Nachweise bereitstellen (z.B. TOM-Dokumentation, relevante Zertifikate, PenTest-Reports soweit vorhanden).

10.3 Audits dürfen den Geschäftsbetrieb des Auftragsverarbeiters nicht unangemessen beeinträchtigen.

11. Rückgabe/Löschung nach Beendigung

11.1 Nach Beendigung des Hauptvertrags wird der Auftragsverarbeiter – nach Wahl/Weisung des Verantwortlichen – personenbezogene Daten zurückgeben oder löschen.

11.2 Backups: Löschung aus Backups erfolgt im Rahmen der regulären Backup-Rotation, sofern nicht anders angewiesen und technisch verhältnismäßig.

11.3 Herausgabeformate/Übergabewege werden abgestimmt (z.B. verschlüsselt, gesicherter Transfer).

12. Haftung

12.1 Es gelten die Haftungsregelungen des Hauptvertrages/AGB, soweit datenschutzrechtlich zulässig.

12.2 Unberührt bleiben gesetzliche Haftungsregelungen nach Art. 82 DSGVO.

13. Schlussbestimmungen

13.1 Änderungen/Ergänzungen dieser AVV bedürfen Textform.

13.2 Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

13.3 Es gilt deutsches Recht. Gerichtsstand – soweit zulässig – Potsdam.

ANLAGE 1: Leistungsgegenstand / Systeme / Servicezugänge

- Betroffene Systeme/Services: [M365/Entra/Exchange/SharePoint], [Server], [VPN/Firewall], [Ticketsystem], [Telefonie/VoIP], [Web/WordPress], [BI/Power BI], weitere gesondert benennen

- Zugriffsarten: Remote-Tool, VPN, Admin-Portale

- Ansprechpartner: Dipl.-Ing. Frank Groß

ANLAGE 2: Technische und organisatorische Maßnahmen (TOM) – Kurzstandard

A) Zutrittskontrolle:

- Zugriff auf Serverräume nur für Berechtigte; Schlüsselliste; Besucherdokumentation

B) Zugangskontrolle:

- MFA wo möglich; starke Passwörter; Rollen-/Rechtekonzept; regelmäßige Review

C) Zugriffskontrolle:

- Least-Privilege; getrennte Admin-Konten; Protokollierung administrativer Zugriffe

D) Weitergabekontrolle:

- Verschlüsselter Transport (TLS/VPN); sichere Freigaben; Freigabeprozesse

E) Eingabekontrolle:

- Logging von Änderungen; Ticket-/Change-Dokumentation

F) Auftragskontrolle:

- Weisungsmanagement; AVV/Vertraulichkeit; Subprocessor-Verträge

G) Verfügbarkeitskontrolle:

- Backup/Restore-Prozesse (soweit vereinbart); Monitoring; Patch-Management-Prozesse

H) Trennungsgebot:

- Mandantentrennung; getrennte Kundenumgebungen; separate Credentials

I) Incident-Management:

- Meldeprozess; Reaktionsplan; 48h-Info an Verantwortlichen

ANLAGE 3: Unterauftragsverarbeiter (Subprocessor) / Drittanbieterhosting

- [Drittanbieter 1] – Hosting/Cloud – [Land] – Schutzmechanismus [EU/EWR / SCC / Angemessenheitsbeschluss]

- [Drittanbieter 2] – Ticketing/Monitoring – [Land] – Schutzmechanismus