Auftragsverarbeitungsvertrag

gemäß Art. 28 DSGVO

Version 2.0 – Stand: März 2026

1. Vertragsgegenstand

Dieser Auftragsverarbeitungsvertrag (AVV) regelt gemäß Art. 28 DSGVO die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Kunden (Auftraggeber) im Rahmen der Bereitstellung, des Betriebs, der Wartung und der Weiterentwicklung digitaler Softwarelösungen.

Der AVV gilt für sämtliche Leistungen im Zusammenhang mit dem Hosting, dem technischen Betrieb sowie der laufenden Betreuung der eingesetzten Web-Applikationen, die auf einem dedizierten Virtual Private Server (VPS) des Auftragsverarbeiters betrieben werden.

2. Vertragsparteien

Auftraggeber (Verantwortlicher im Sinne der DSGVO)

Der jeweilige Kunde, der die Software des Auftragsverarbeiters nutzt. Die konkreten Kontaktdaten des Auftraggebers ergeben sich aus dem zugrundeliegenden Hauptvertrag.

Auftragsverarbeiter

Name	Daniel Reichhart
Marke / Handelsname	Digitaler Mitarbeiter
Adresse	Parzhofstraße 14, 4040 Linz, Österreich
E-Mail	office@digitalma.at
Website	www.digitalma.at
USt-ID	Kleinunternehmer gemäß § 6 Abs. 1 Z 27 UStG

3. Gegenstand und Dauer der Verarbeitung

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich für die Dauer der aktiven Nutzung der Software durch den Auftraggeber auf Basis des Hauptvertrags.

Nach Beendigung des Hauptvertrags werden personenbezogene Daten ausschließlich insoweit weiterverarbeitet, als dies zur Erfüllung gesetzlicher Aufbewahrungspflichten (insbesondere nach österreichischer Bundesabgabenordnung, BAO, oder UGB) zwingend erforderlich ist. Nach Ablauf dieser Fristen erfolgt die unwiderrufliche Löschung bzw. Vernichtung.

4. Art und Zweck der Verarbeitung

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich zu folgenden Zwecken:

- Technische Bereitstellung und Betrieb der Softwarelösungen
- Hosting und sichere Speicherung der Daten auf dem VPS
- Laufende Wartung, Support und Fehlerbehebung
- Durchführung automatisierter und manueller Datensicherungen
- Sicherstellung der IT-Sicherheit und Systemverfügbarkeit
- Weiterentwicklung der Softwarefunktionalität auf Weisung des Auftraggebers

Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters, insbesondere für Werbung, Marktforschung oder Profilbildung, findet ausdrücklich nicht statt.

5. Art der personenbezogenen Daten

Je nach genutzter Software können insbesondere folgende Datenkategorien verarbeitet werden:

- Stammdaten: Name, Anschrift, Geburtsdatum
- Kontaktdaten: E-Mail-Adresse, Telefonnummer
- Kunden- und Auftragsdaten
- Fahrzeug- und Vertragsdaten (bei Kfz-Anwendungen)
- Dokumente, Berichte, Fotos und sonstige Uploadinhalte
- Nutzungs- und Protokolldaten (Logs)
- Rechnungs- und Angebotsdaten

Besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO (z. B. Gesundheitsdaten, biometrische Daten, religiöse oder politische Überzeugungen) werden durch den Auftragsverarbeiter nicht gezielt verarbeitet. Sollte der Auftraggeber solche Daten selbst in die Software eingeben, trägt er hierfür die alleinige datenschutzrechtliche Verantwortung.

6. Kategorien betroffener Personen

- Kunden und Interessenten des Auftraggebers
- Mitarbeiterinnen und Mitarbeiter des Auftraggebers
- Geschäftspartner und Lieferanten des Auftraggebers
- Sonstige natürliche Personen, deren Daten der Auftraggeber in der Software verwaltet

7. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich gegenüber dem Auftraggeber:

- Personenbezogene Daten ausschließlich auf dokumentierte, schriftliche oder elektronische Weisung des Auftraggebers zu verarbeiten; widerspricht eine Weisung nach Einschätzung des Auftragsverarbeiters geltendem Datenschutzrecht, wird der Auftraggeber unverzüglich informiert
- Alle mit der Verarbeitung befassten Personen zur Vertraulichkeit zu verpflichten und dies zu dokumentieren

- Alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO umzusetzen und regelmäßig zu überprüfen
- Den Auftraggeber bei der Wahrnehmung von Betroffenenrechten (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) zu unterstützen und erforderliche Informationen unverzüglich, spätestens innerhalb von 72 Stunden, bereitzustellen
- Datenschutzverletzungen (Art. 33 DSGVO) unverzüglich, spätestens binnen 24 Stunden nach Kenntnisnahme, an den Auftraggeber zu melden und alle für die Meldung an die zuständige Aufsichtsbehörde erforderlichen Informationen zur Verfügung zu stellen
- Den Auftraggeber bei der Durchführung von Datenschutz-Folgenabschätzungen (DSFA, Art. 35 DSGVO) zu unterstützen, sofern erforderlich
- Personenbezogene Daten nicht ohne ausdrückliche schriftliche Genehmigung des Auftraggebers an Dritte weiterzugeben
- Einen Verzeichnis der Verarbeitungstätigkeiten (Art. 30 Abs. 2 DSGVO) zu führen und auf Anfrage vorzulegen

8. Technische und organisatorische Maßnahmen (TOM, Art. 32 DSGVO)

Der Auftragsverarbeiter setzt insbesondere folgende Schutzmaßnahmen um:

Zutrittskontrolle

- Server physisch in gesicherten Rechenzentren (ISO 27001-zertifiziert) des Hosting-Dienstleisters untergebracht
- Kein physischer Zugang durch den Auftragsverarbeiter selbst – ausschließlich gesicherter Remote-Zugriff

Zugangskontrolle

- SSH-Zugriff ausschließlich mit kryptografischen Schlüsseln (kein Passwort-Login)
- Individuelle, starke Passwörter pro Anwendung und Datenbank
- Rollentrennung: Jede Applikation nutzt einen eigenen, rechtlich beschränkten Datenbankbenutzer

Zugriffskontrolle

- Rollenbasiertes Berechtigungssystem innerhalb jeder Applikation
- Passwörter in der Datenbank grundsätzlich mit bcrypt gehasht und gesalzen
- Sessions über serverseitige, signierte Cookies (HttpOnly, Secure, SameSite)

Übertragungssicherheit

- Alle Verbindungen ausschließlich über HTTPS/TLS (Let's Encrypt, automatische Zertifikatserneuerung)
- Erzwungene Weiterleitung von HTTP auf HTTPS via Nginx
- Kommunikation zwischen Applikation und Datenbank ausschließlich lokal (localhost, kein externer DB-Port)

Eingabekontrolle und Protokollierung

- Applikationsseitige Validierung und Bereinigung aller Nutzereingaben (Input Validation, XSS- und SQL-Injection-Schutz)
- PM2-Prozessmanager protokolliert Applikationsaktivitäten
- Nginx-Zugriffslogs für alle HTTP-Anfragen

Verfügbarkeit und Wiederherstellbarkeit

- Automatisches tägliches Datenbank-Backup (02:00 Uhr) mit 30-Tage-Aufbewahrung auf gesondertem Speichermedium (OneDrive)
- Wöchentlicher Vollserver-Snapshot durch den Hosting-Dienstleister
- Kontinuierliches Availability-Monitoring aller Applikationen (UptimeRobot, 5-Minuten-Intervall) mit sofortiger E-Mail-Benachrichtigung bei Ausfall
- Datenbankwiederherstellung aus Backup innerhalb weniger Stunden möglich

Trennungsgebot

- Logische und technische Trennung der Kundendaten: Jede Applikation verfügt über eine eigene, isolierte PostgreSQL-Datenbank mit eigenem Datenbankbenutzer
- Keine Mandantenvermischung auf Datenbankebene

9. Einsatz von Subunternehmern (Unterauftragsverarbeitern)

Zur Erbringung der vertragsgegenständlichen Leistungen werden folgende Subunternehmer eingesetzt:

Unternehmen	Sitz	Zweck	Grundlage
Hostinger International Ltd.	EU (Zypern / Deutschland)	VPS-Hosting (Rechenzen-trum Deutschland)	Vertrag mit Datenverarbei-tungsklauseln; DSGVO-konform (EU)
Microsoft Corporation (OneDrive)	USA / EU-Datencenter	Verschlüsselte Backup-Ablage	EU-US Data Privacy Framework; Microsoft DPA

Der Auftragsverarbeiter verpflichtet alle eingesetzten Subunternehmer vertraglich zur Einhaltung der Datenschutzanforderungen der DSGVO und des österreichischen Datenschutzgesetzes (DSG). Bei Änderungen des Subunternehmereinsatzes wird der Auftraggeber vorab schriftlich informiert und erhält die Möglichkeit, Einwände zu erheben.

Alle Produktionsdaten werden ausschließlich auf dem VPS-Server in Deutschland (EU) gespeichert und verarbeitet. Eine Übermittlung von Produktionsdaten in Drittländer außerhalb der EU/des EWR findet nicht statt. Backups werden verschlüsselt übertragen und auf Microsofts EU-Rechenzentren gespeichert.

10. Kontrollrechte des Auftraggebers

Der Auftraggeber ist berechtigt, die Einhaltung der datenschutzrechtlichen Verpflichtungen jederzeit zu überprüfen. Kontrollen bedürfen einer angemessenen Vorankündigung von mindestens 5 Werktagen und dürfen den laufenden Betrieb des Auftragsverarbeiters nicht unverhältnismäßig beeinträchtigen.

Der Auftragsverarbeiter stellt auf begründete schriftliche Anfrage alle erforderlichen Informationen und Nachweise zur Verfügung, insbesondere Auskünfte über die eingesetzten technischen und organisatorischen Maßnahmen.

Physische On-Site-Inspektionen am Serverstandort des Hosting-Dienstleisters liegen außerhalb der Möglichkeiten des Auftragsverarbeiters. In diesem Fall kann der Auftraggeber die einschlägigen Zertifizierungen und Prüfberichte des Hosting-Dienstleisters (z. B. ISO 27001) anfordern.

11. Löschung und Rückgabe von Daten

Nach Beendigung des Hauptvertrags werden alle personenbezogenen Daten des Auftraggebers auf dessen ausdrückliche schriftliche Weisung entweder:

- in einem gängigen, maschinenlesbaren Format (z. B. SQL-Export, CSV) an den Auftraggeber übergeben und anschließend beim Auftragsverarbeiter unwiderruflich gelöscht, oder
- ohne gesonderte Weisung spätestens 30 Tage nach Vertragsende unwiderruflich gelöscht,

sofern keine gesetzlichen Aufbewahrungspflichten einer Löschung entgegenstehen (z. B. Rechnungslegungspflichten gemäß UGB, BAO). In diesem Fall werden nur die zwingend aufzubewahrenden Daten für die Dauer der gesetzlichen Frist gespeichert und danach gelöscht.

Automatisierte Backups werden entsprechend der technischen Speicherzyklen (derzeit 30 Tage) automatisch überschrieben und gelöscht.

12. Haftung

Jede Vertragspartei haftet gegenüber Betroffenen und Aufsichtsbehörden nach den Bestimmungen der DSGVO sowie des österreichischen Datenschutzgesetzes (DSG 2018 idgF) entsprechend ihrer jeweiligen Verantwortung.

Der Auftraggeber bleibt als Verantwortlicher im Sinne von Art. 4 Z 7 DSGVO für die Rechtmäßigkeit der Erhebung und Verarbeitung personenbezogener Daten allein verantwortlich. Der Auftragsverarbeiter haftet ausschließlich für Schäden, die durch eine nachweislich ihm zurechenbare Verletzung seiner vertraglichen oder gesetzlichen Datenschutzpflichten entstanden sind.

Die Haftung des Auftragsverarbeiters für leicht fahrlässig verursachte Sachschäden ist auf das Dreifache des vereinbarten jährlichen Entgelts begrenzt, sofern dem Auftragnehmer kein grobes Verschulden oder Vorsatz zur Last fällt.

13. Vertragsabschluss und Geltung

Dieser AVV wird integrierender Bestandteil des Hauptvertrags zwischen Auftraggeber und Auftragsverarbeiter. Mit Abschluss des Nutzungsvertrages oder spätestens mit Beginn der Nutzung der Software gilt dieser AVV als ausdrücklich vereinbart.

Änderungen dieses AVV bedürfen der Schriftform (E-Mail genügt). Mündliche Nebenabreden haben keine Wirksamkeit.

14. Anwendbares Recht und Gerichtsstand

Es gilt ausschließlich österreichisches Recht, insbesondere die Datenschutz-Grundverordnung (DSGVO – VO (EU) 2016/679), das österreichische Datenschutzgesetz (DSG 2018 idgF) sowie ergänzend das ABGB und UGB, unter Ausschluss des internationalen Privatrechts (IPRG/Rom I-VO).

Zuständige Datenschutzbehörde ist die österreichische Datenschutzbehörde (DSB), Barichgasse 40–42, 1030 Wien, dsb.gv.at.

Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AVV ist das sachlich zuständige Gericht in Linz, Österreich, soweit gesetzlich zulässig.

Sollten einzelne Bestimmungen dieses AVV ganz oder teilweise unwirksam sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die unwirksame Bestimmung ist durch eine rechtlich wirksame zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung möglichst nahekommt.

15. Unterzeichnung

Dieser AVV gilt mit Unterzeichnung des Hauptvertrags bzw. mit Beginn der Nutzung als vereinbart. Zur Dokumentation können beide Parteien diesen AVV gesondert unterzeichnen:

Auftraggeber	**Auftragsverarbeiter**
Ort, Datum, Unterschrift	Ort, Datum, Unterschrift – Daniel Reichhart