

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO
Version 2.0 – Stand: März 2026

Mit der Nutzung dieser Software erklären Sie sich mit diesem Auftragsverarbeitungsvertrag einverstanden. Eine gesonderte Unterzeichnung ist nicht erforderlich.

1. Vertragsgegenstand

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

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

Steuerlicher Status: 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 Unternehmensgesetzbuch – UGB) zwingend erforderlich ist. Nach Ablauf dieser Fristen erfolgt die unwiderrufliche Löschung der Daten.

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-Server
- 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 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
- Ein Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO zu führen und auf Anfrage vorzulegen

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

Zutrittskontrolle

- Server physisch in gesicherten Rechenzentren des Hosting-Dienstleisters untergebracht
- Kein physischer Zugang durch den Auftragsverarbeiter – ausschließlich gesicherter Remote-Zugriff

Zugangskontrolle

- SSH-Zugriff ausschließlich mit kryptografischen Schlüsseln (kein Passwortlogin)
- 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 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
- Datenbankzugriff ausschließlich lokal (kein externer Datenbankport erreichbar)

Eingabekontrolle und Protokollierung

- Applikationsseitige Validierung und Bereinigung aller Nutzereingaben (XSS- und SQL-Injection-Schutz)
- Prozessmanager protokolliert Applikationsaktivitäten
- Webserver-Zugriffslogs für alle HTTP-Anfragen

Verfügbarkeit und Wiederherstellbarkeit

- Automatisches tägliches Datenbank-Backup (02:00 Uhr) mit 30-tägiger Aufbewahrung auf gesondertem Speichermedium
- Wöchentlicher Vollserver-Snapshot durch den Hosting-Dienstleister
- Kontinuierliches Monitoring aller Applikationen im 5-Minuten-Takt mit sofortiger E-Mail-Alarmierung bei Ausfall
- Datenbankwiederherstellung aus Backup innerhalb weniger Stunden möglich

Trennungsgebot

- Jede Applikation verfügt über eine eigene, isolierte PostgreSQL-Datenbank mit eigenem Datenbankbenutzer
- Keine Vermischung von Kundendaten zwischen verschiedenen Mandanten

9. Einsatz von Subunternehmern (Unterauftragsverarbeitern)

Zur Erbringung der vertragsgegenständlichen Leistungen werden folgende Subunternehmer eingesetzt:

Hostinger International Ltd.

Zweck: VPS-Hosting

Serverstandort: Deutschland (EU)

Rechtsgrundlage: Vertrag mit DSGVO-konformen Datenschutzklauseln

Microsoft Corporation (OneDrive)

Zweck: Verschlüsselte Backup-Ablage

Serverstandort: EU-Rechenzentren

Rechtsgrundlage: EU-US Data Privacy Framework, Microsoft DPA

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 EU-Rechenzentren gespeichert.

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

10. Kontrollrechte des Auftraggebers

Der Auftraggeber ist berechtigt, die Einhaltung der datenschutzrechtlichen Verpflichtungen jederzeit zu überprüfen. Schriftliche Anfragen sind an office@digitalma.at zu richten. Der Auftragsverarbeiter stellt auf begründete Anfrage alle erforderlichen Informationen und Nachweise zur Verfügung.

Kontrollen bedürfen einer angemessenen Vorankündigung von mindestens 5 Werktagen und dürfen den laufenden Betrieb nicht unverhältnismäßig beeinträchtigen. Physische On-Site-Inspektionen am Serverstandort des Hosting-Dienstleisters liegen außerhalb der Möglichkeiten des Auftragsverarbeiters; in diesem Fall können die einschlägigen Zertifizierungen des Hosting-Dienstleisters angefordert werden.

11. Löschung und Rückgabe von Daten

Nach Beendigung des Vertragsverhältnisses werden alle personenbezogenen Daten des Auftraggebers:

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

sofern keine gesetzlichen Aufbewahrungspflichten (z. B. gemäß UGB, BAO) entgegenstehen. 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.

13. Vertragsschluss durch Nutzung

Dieser AVV wird mit Beginn der Nutzung der Software automatisch Bestandteil des Vertragsverhältnisses zwischen Auftraggeber und Auftragsverarbeiter. Eine gesonderte

Unterzeichnung ist nicht erforderlich. Durch die aktive Nutzung der Software erklärt der Auftraggeber sein ausdrückliches Einverständnis mit diesem AVV.

Änderungen dieses AVV werden dem Auftraggeber mindestens 14 Tage vor Inkrafttreten per E-Mail oder Benachrichtigung innerhalb der Software mitgeteilt. Wird der Nutzung nach Bekanntgabe der Änderungen nicht schriftlich widersprochen, gilt dies als Zustimmung.

14. Anwendbares Recht und Gerichtsstand

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

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

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

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.