

VEREINBARUNG ÜBER DIE AUFTRAGSVERARBEITUNG

gemäß Artikel 28 der Verordnung (EU) 2016/679 (DSGVO)

Website as a Service (WaaS)

Fassung 1.1 | 02.09.2026 | ausschließlich im unternehmerischen Geschäftsverkehr (B2B)

zwischen

dem in der Leistungsvereinbarung als Auftraggeber genannten Kunden

– im Folgenden „Verantwortlicher“ oder „Kunde“ –

und

FDM Software GmbH

Adelheid-Popp-Gasse 8/2/57, 1220 Wien

FN 678054 p, Handelsgericht Wien, UID ATU83270238

– im Folgenden „Auftragsverarbeiter“ oder „FDM“ –

– gemeinsam die „Parteien“ –

Diese Auftragsverarbeitungsvereinbarung (AVV) ist Bestandteil der Leistungsvereinbarung zwischen dem Kunden und FDM und wird mit deren Abschluss wirksam; einer gesonderten Unterzeichnung bedarf es nicht.

1. Gegenstand, Dauer, Rangfolge

1.1 Diese Vereinbarung regelt die Verarbeitung personenbezogener Daten durch FDM im Auftrag des Kunden im Rahmen der Leistung „Website as a Service“ (WaaS) gemäß Leistungsvereinbarung.

1.2 Die Dauer entspricht der Laufzeit der Leistungsvereinbarung einschließlich der Export- und Löschrufen nach Ziffer 12.

1.3 Bei Widersprüchen zwischen dieser Vereinbarung und der Leistungsvereinbarung geht diese Vereinbarung in datenschutzrechtlichen Fragen vor. Die Haftungsregelungen der Leistungsvereinbarung gelten auch für Ansprüche aus dieser Vereinbarung, soweit Art. 82 DSGVO dem nicht entgegensteht.

2. Art, Zweck, Datenkategorien, betroffene Personen

2.1 Zweck der Verarbeitung: Bereitstellung und Nutzung der Leistung „Website as a Service“ (WaaS) zur Unterstützung des Kunden bei der Konzeption, Erstellung, dem Hosting, der Wartung, Aktualisierung und dem Support seiner Website bzw. Web-Anwendung einschließlich der hierfür erforderlichen Verarbeitung personenbezogener Daten.

2.2 Art der Verarbeitung: Erhebung durch Eingabe und über die Website (insbesondere Formulare), Speicherung, Strukturierung, Bereitstellung und Anzeige im Internet, Übermittlung an berechnigte Nutzer des Kunden, Export, Protokollierung, Sicherung und Löschung.

2.3 Kategorien betroffener Personen:

– Nutzer und Besucher der vom Kunden betriebenen Website bzw. Web-Anwendung;

- Personen, die über Kontakt-, Anfrage- oder Registrierungsformulare der Website personenbezogene Daten übermitteln;
- Beschäftigte und Beauftragte des Kunden, die die Website administrieren oder Inhalte pflegen.

2.4 Kategorien personenbezogener Daten:

- Identifikations- und Kontaktdaten: Vor- und Nachname, E-Mail-Adresse, Telefonnummer, Anschrift sowie weitere über Formulare der Website übermittelte Angaben;
- Inhaltsdaten: von Nutzern über die Website übermittelte oder auf der Website eingestellte Inhalte (z. B. Nachrichten, Uploads, Kommentare);
- Nutzer- und Zugangsdaten der Administratoren: E-Mail, Name, Rolle, Berechtigungen, Anmelde- und Zugriffszeitpunkte;
- Technische Daten: IP-Adresse, Geräte- und Browserinformationen, Zugriffs- und Verbindungsdaten sowie Cookies und ähnliche Kennungen;
- Protokolldaten: Audit- und Zugriffsereignisse mit handelnder Person, Rolle, Zeitpunkt und Ereignistyp, soweit für Nachvollziehbarkeit und Sicherheit erforderlich.

2.5 Besondere Kategorien personenbezogener Daten: Die Leistung ist nicht für die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO vorgesehen. Soweit der Kunde solche Daten dennoch verarbeitet, ist er für deren datenschutzrechtliche Zulässigkeit verantwortlich.

3. Verantwortlichkeit und Weisungen

3.1 Der Kunde ist allein Verantwortlicher für die Rechtmäßigkeit der Verarbeitung. Er bestimmt und dokumentiert die jeweils einschlägige Rechtsgrundlage nach Art. 6 und – soweit tatsächlich besondere Kategorien personenbezogener Daten verarbeitet werden – Art. 9 DSGVO, erfüllt die Informationspflichten nach Art. 13 und 14 DSGVO, prüft die Erforderlichkeit einer Datenschutz-Folgenabschätzung und wahrt die Betroffenenrechte.

3.2 FDM verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Kunden. Die Weisungen ergeben sich aus der Leistungsvereinbarung, dieser Vereinbarung und der Nutzung der Funktionen durch berechtigte Nutzer des Kunden (Konfiguration, Import, Freigaben, Löschungen, Exporte). Weitere Weisungen sind in Textform an office@fdm-software.at zu richten. FDM darf für weisungsbedingte Mehraufwände außerhalb des Funktionsumfangs ein angemessenes Entgelt verlangen.

3.3 FDM informiert den Kunden unverzüglich, wenn eine Weisung nach ihrer Auffassung gegen Datenschutzrecht verstößt, und darf die Ausführung bis zur Bestätigung aussetzen.

4. Pflichten von FDM

4.1 FDM stellt sicher, dass die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

4.2 FDM trifft die technischen und organisatorischen Maßnahmen nach Anlage 1 und überprüft sie regelmäßig. Maßnahmen dürfen weiterentwickelt werden, solange das Schutzniveau nicht unterschritten wird.

4.3 FDM unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und soweit dies möglich ist bei der Erfüllung seiner Pflichten zur Bearbeitung von Anträgen betroffener Personen nach Art. 12 bis 22 DSGVO. Die Unterstützung erfolgt vorrangig durch die im Rahmen der Leistung bereitgestellten Funktionen, insbesondere Export, Berichtigung und Löschung. Erhält FDM unmittelbar eine Betroffenenanfrage betreffend Kundendaten, informiert FDM den Kunden unverzüglich und beantwortet die Anfrage nicht selbst, sofern der Kunde FDM hierzu nicht ausdrücklich angewiesen hat.

4.4 FDM unterstützt den Kunden bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, Konsultation) unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen.

4.5 FDM informiert den Kunden unverzüglich, nachdem FDM eine Verletzung des Schutzes personenbezogener Kundendaten bekannt geworden ist, und stellt die nach Art. 33 Abs. 3 DSGVO erforderlichen Informationen zur Verfügung, soweit diese FDM vorliegen. Noch nicht verfügbare Informationen werden nachgereicht.

4.6 FDM stellt dem Kunden alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO erforderlich sind, und ermöglicht Überprüfungen nach Ziffer 9.

5. Pflichten des Kunden

5.1 Der Kunde übermittelt und erfasst nur Daten, die für die Zwecke nach Ziffer 2 erforderlich sind, und prüft die an FDM übermittelten Daten auf Datenminimierung und Richtigkeit. Datenfelder, die für die genutzten Funktionen nicht erforderlich sind, sollen nicht an FDM übermittelt werden.

5.2 Der Kunde vergibt Rollen und Berechtigungen (sofern anwendbar) nach dem Need-to-know-Prinzip, entfernt ausgeschiedene Nutzer unverzüglich, stellt sicher, dass über die Website veröffentlichte oder verarbeitete personenbezogene Daten nur berechtigten Personen zugänglich gemacht werden.

5.3 Der Kunde ist für die Rechtmäßigkeit der Übermittlung personenbezogener Daten an FDM verantwortlich und stellt sicher, dass seine Nutzer die für sie geltenden Rollen-, Berechtigungs-, Vertraulichkeits- und Datenminimierungsvorgaben einhalten.

5.4 Der Kunde stellt sicher, dass seine Nutzer personenbezogene Daten nur im Rahmen ihrer jeweiligen Berechtigungen und der geltenden Datenschutzvorgaben verarbeiten.

6. Subunternehmer (weitere Auftragsverarbeiter)

6.1 Der Kunde genehmigt allgemein den Einsatz der in Anlage 2 genannten Subunternehmer.

6.2 FDM informiert den Kunden über die beabsichtigte Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter und gibt ihm Gelegenheit, aus wichtigem datenschutzrechtlichem Grund zu widersprechen. Die Information erfolgt grundsätzlich vor deren Einsatz; in dringenden Fällen kann sie kurzfristig erfolgen. Kann einem berechtigten Widerspruch nicht durch eine für FDM zumutbare Alternative Rechnung getragen werden, ist FDM berechtigt, die betroffene Leistung oder die Leistungsvereinbarung zu kündigen.

6.3 FDM verpflichtet Subunternehmer vertraglich zu Datenschutzpflichten, die den Pflichten aus dieser Vereinbarung entsprechen, und bleibt gegenüber dem Kunden für deren Erfüllung verantwortlich.

6.4 Dienstleister, die keine personenbezogenen Kundendaten im Auftrag des Kunden verarbeiten, sind keine weiteren Auftragsverarbeiter im Sinne dieser Vereinbarung.

7. Vertraulichkeit

FDM behandelt alle Kundendaten vertraulich, auch über das Vertragsende hinaus, und gibt sie nur auf Weisung des Kunden, aufgrund gesetzlicher Verpflichtung oder an genehmigte Subunternehmer weiter. Bei gesetzlicher Verpflichtung informiert FDM den Kunden vor der Offenlegung, soweit rechtlich zulässig.

8. Verarbeitungsort und Drittlandtransfer

8.1 Die Verarbeitungsorte der von FDM eingesetzten weiteren Auftragsverarbeiter ergeben sich aus Anlage 2.

8.2 Eine Übermittlung personenbezogener Daten in Drittländer erfolgt nur unter den Voraussetzungen des Kapitels V DSGVO.

9. Kontrollrechte

9.1 FDM stellt dem Kunden die gemäß Art. 28 DSGVO erforderlichen Informationen zum Nachweis der Einhaltung dieser Vereinbarung zur Verfügung. Kontrollen erfolgen vorrangig anhand geeigneter Dokumentationen, Sicherheitsinformationen, Zertifizierungen, Prüfberichte oder angemessener Fragebögen.

Soweit dies zur Erfüllung der gesetzlichen Kontrollpflichten des Kunden erforderlich ist und diese Nachweise nicht ausreichen, ermöglicht FDM eine ergänzende Prüfung, vorrangig remote. Vor-Ort-Prüfungen sind nur zulässig, wenn eine gleich geeignete Dokumenten- oder Remote-Prüfung nicht ausreicht. Prüfungen sind außer bei dringendem Anlass mindestens vierzehn (14) Kalendertage vorher anzukündigen und so durchzuführen, dass Geschäftsbetrieb, Geschäftsgeheimnisse und Daten anderer Kunden geschützt bleiben.

Für Prüfungen, die über die übliche Bereitstellung von Nachweisen hinausgehen, kann FDM angemessenen Aufwand verrechnen, sofern kein von FDM zu vertretender wesentlicher Datenschutzverstoß festgestellt wird.

10. Verletzungen, Aufsichtsbehörden

Die Parteien unterstützen einander im gesetzlich erforderlichen Umfang bei Datenschutzverletzungen und aufsichtsbehördlichen Verfahren, soweit die jeweilige Verarbeitung betroffen ist.

11. Haftung

11.1 Für die Haftung der Parteien gelten Art. 82 DSGVO sowie ergänzend die Haftungsregelungen der Leistungsvereinbarung. Die Haftungsbeschränkungen der Leistungsvereinbarung gelten nicht, soweit sie gegenüber betroffenen Personen nach Art. 82 DSGVO unwirksam wären; im Innenverhältnis der Parteien bleiben sie anwendbar.

12. Beendigung, Rückgabe und Löschung

12.1 Nach einer Löschweisung werden personenbezogene Kundendaten entsprechend dem bei FDM eingesetzten Löschrückgabe- und Sicherungskonzept aus den Produktivsystemen entfernt. In Sicherungskopien enthaltene Daten werden im Rahmen der regulären Sicherungszyklen gelöscht oder überschrieben und bis dahin nicht erneut produktiv verarbeitet, sofern keine gesetzliche Verpflichtung hierzu besteht.

12.2 Ausgenommen sind Daten, die FDM aufgrund gesetzlicher Aufbewahrungspflichten speichern muss; diese werden gesperrt und ausschließlich für diesen Zweck aufbewahrt. Vertrags- und Abrechnungsdaten, die FDM als eigener Verantwortlicher verarbeitet, unterliegen den hierfür geltenden gesetzlichen Aufbewahrungsfristen und nicht der Löschweisung des Kunden im AVV.

12.3 Soweit Audit- und Protokolldaten personenbezogene Kundendaten enthalten, werden sie nur so lange gespeichert, wie dies für Sicherheits-, Nachweis- und Dokumentationszwecke erforderlich ist. Nach Wegfall dieser Zwecke werden personenbezogene Inhalte nach Maßgabe des jeweils geltenden Lösch- und Aufbewahrungskonzepts gelöscht oder anonymisiert. Nach Vertragsende gelten ergänzend die Ziffern 12.1 und 12.2.

13. Schlussbestimmungen

13.1 Änderungen bedürfen der Textform.

13.2 Es gilt österreichisches Recht unter Ausschluss der Verweisungsnormen des internationalen Privatrechts und des UN-Kaufrechts. Ausschließlicher Gerichtsstand ist Wien. Die sachliche Zuständigkeit richtet sich nach den gesetzlichen Vorschriften.

13.3 Die Anlagen 1 und 2 sind Bestandteil dieser Vereinbarung. Diese Vereinbarung wird mit Abschluss der Leistungsvereinbarung wirksam und bedarf keiner gesonderten Unterfertigung; eine solche, auch in elektronischer Form, ist zulässig.

Anlage 1 – Technische und organisatorische Maßnahmen

FDM trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO.

1. Zugriffsschutz

Der Zugriff auf personenbezogene Kundendaten ist auf autorisierte Personen beschränkt. FDM setzt geeignete Authentifizierungs- und Berechtigungsverfahren ein und beschränkt privilegierte Zugriffe nach dem Need-to-know-Prinzip.

2. Mandanten- und Berechtigungstrennung

Kundendaten werden durch geeignete technische Zugriffskontrollen logisch voneinander getrennt. Nutzer erhalten nur Zugriff auf die ihnen jeweils zugewiesenen Daten und Funktionen.

3. Übertragung und Speicherung

Personenbezogene Daten werden bei der Übertragung durch geeignete Verschlüsselungsverfahren geschützt. Für die Speicherung werden angemessene Sicherheitsmaßnahmen der eingesetzten Infrastruktur- und Hostinganbieter genutzt.

4. Protokollierung

Sicherheitsrelevante und wesentliche administrative Vorgänge werden in angemessenem Umfang protokolliert, soweit dies für Sicherheit, Nachvollziehbarkeit und Fehleranalyse erforderlich ist.

5. Verfügbarkeit und Wiederherstellung

FDM trifft angemessene Maßnahmen zur Sicherung der Verfügbarkeit und Wiederherstellbarkeit der Leistung und der darin verarbeiteten Daten.

6. Entwicklungs- und Betriebssicherheit

FDM setzt angemessene Verfahren für Entwicklung, Änderung und Betrieb der Leistung ein und überprüft sicherheitsrelevante Konfigurationen und Berechtigungen regelmäßig.

7. Organisatorische Maßnahmen

Personen mit Zugriff auf personenbezogene Kundendaten werden zur Vertraulichkeit verpflichtet. Zugriffsberechtigungen werden nach Erforderlichkeit vergeben und angepasst. Für Datenschutz- und Sicherheitsvorfälle bestehen geeignete interne Verfahren.

8. Weiterentwicklung der Maßnahmen

FDM darf einzelne technische und organisatorische Maßnahmen ändern oder durch gleichwertige Maßnahmen ersetzen, sofern dadurch das Schutzniveau insgesamt nicht wesentlich herabgesetzt wird.

Anlage 2: Genehmigte Subunternehmer

Der Kunde genehmigt die nachstehenden weiteren Auftragsverarbeiter. Änderungen folgen dem Verfahren nach Ziffer 6.2.

Subunternehmer	Leistung	Verarbeitete Daten	Verarbeitungsort
Supabase, Inc.	Datenbank, Authentifizierung, Dateiablage, Sicherungen	Kundendaten, Nutzerdaten, Audit-Protokolle	eu-west-1, Irland; etwaige Supportzugriffe nach Anbieter-DPA
Vercel Inc.	Hosting, Bereitstellung und Ausführung der Anwendung	Über die Anwendung übertragene Kunden- und Nutzerdaten sowie technische Verbindungs- und Protokolldaten	Verarbeitung nach Maßgabe des Vercel-DPA; Drittlandübermittlungen nur nach Kapitel V DSGVO
Resend Inc.	Versand transaktionaler E-Mails im Rahmen von Authentifizierung und Nutzerverwaltung	Name, E-Mail-Adresse sowie für den Versand erforderliche Authentifizierungs- und Einladungsinformationen	Verarbeitung nach Maßgabe des Resend-DPA; Drittlandübermittlungen nur nach Kapitel V DSGVO