

Vertrag zur Auftragsverarbeitung (AVV) – Mileon GmbH

Mileon GmbH · Rheinpromenade 9 · 40789 Monheim am Rhein · Stand: 29.10.2026

Dieser Vertrag erfüllt die Anforderungen aus Art. 28 Abs. 3 DSGVO für die Nutzung von Mileon.

Parteien

zwischen

dem Kunden (Unternehmen, das Mileon nutzt, wie im Vertrag über die Nutzung von Mileon bezeichnet) –
nachfolgend „**Verantwortlicher**“ –

und

Mileon GmbH, Rheinpromenade 9, 40789 Monheim am Rhein, vertreten durch den Geschäftsführer Leon-Mile
Subasic, E-Mail: info@mileon.cloud – nachfolgend „**Auftragsverarbeiter**“ –

Präambel

Der Auftragsverarbeiter stellt dem Verantwortlichen die Software Mileon für Personal- und Fuhrparkplanung als Online-Dienst bereit (Hauptvertrag: Nutzungsbedingungen bzw. AGB von Mileon). Dabei verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen. Dieser Vertrag regelt die Rechte und Pflichten der Parteien nach Art. 28 DSGVO. Er gilt ergänzend zum Hauptvertrag; bei Widersprüchen zum Datenschutz geht dieser Vertrag vor.

§ 1 Gegenstand, Dauer und Art der Verarbeitung

1. **Gegenstand:** Bereitstellung, Betrieb, Wartung, Sicherung und Support der Software Mileon für den Verantwortlichen. Jeder Kunde erhält eine eigene Instanz mit eigener Datenbank.
2. **Dauer:** Dieser Vertrag gilt, solange der Hauptvertrag besteht, und darüber hinaus, bis alle Daten nach § 9 gelöscht oder zurückgegeben sind.
3. **Art und Zweck:** Speichern, Ordnen, Anzeigen, Auswerten, Übermitteln an berechtigte Benutzer des Verantwortlichen, Sichern und Löschen. Zweck ist die Personaleinsatz- und Fuhrparkplanung des Verantwortlichen (Schichtplanung, Fahrer- und Fahrzeugverwaltung, Fristen, Schäden, Geräte, Tankkarten, Nachweise).

Betroffene Personen	Datenarten
Fahrer und sonstige Mitarbeiter des Verantwortlichen	Name, Personalnummer, Transporter-ID, Station, Telefon, E-Mail, Geburtsdatum; Beschäftigungsdaten (Eintritt, Vertragsende, Verlängerungen, Austritt, Wochenstunden); Schichten und Einsätze; Abwesenheiten (Urlaub, Krankheit ohne Diagnose); Führerschein- und Ausweisdaten (Nummer, Gültigkeit, Ausstellungsland, Arbeitsvisum); Unterweisungen und Sichtprüfungen; Fahrzeug-, Geräte- und Tankkartenzuordnung; Schäden und Unfälle einschließlich Fotos und Dokumenten dazu (z. B. Unfallbericht, Polizeimeldung, Gutachten)
Fahrer und Mitarbeiter (nur Rollen Administrator und HR-Manager)	Lohnart und -höhe, Steuerklasse, Steuer-ID, Sozialversicherungsnummer, Krankenkasse, IBAN, BIC
Benutzer von Mileon beim Verantwortlichen	Name, E-Mail, Rolle und Rechte, Anmeldezeitpunkte, Änderungsprotokoll

Betroffene Personen	Datenarten
Unfallgegner, Zeugen und sonstige Dritte	Name, Anschrift, Kennzeichen, Versicherungsdaten sowie Abbildungen, soweit sie in Unfallberichten, Polizeimeldungen oder Fotos zu einem Schaden enthalten sind

4. **Besondere Kategorien:** Krankmeldungen sind Gesundheitsdaten nach Art. 9 DSGVO. Mileon speichert dazu nur Zeitraum und Art „krank“, keine Diagnosen.
5. **Ort der Verarbeitung:** ausschließlich in Rechenzentren in der Europäischen Union. Eine Verarbeitung in einem Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und der Voraussetzungen der Art. 44 ff. DSGVO.

§ 2 Weisungen

1. Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen. Die Weisungen sind in diesem Vertrag, im Hauptvertrag und in der Nutzung der Funktionen von Mileon durch den Verantwortlichen festgelegt.
2. Einzelweisungen erteilt der Verantwortliche in Textform (z. B. E-Mail an info@mileon.cloud).
3. Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich. Er darf die Ausführung bis zur Bestätigung oder Änderung aussetzen.
4. Ist der Auftragsverarbeiter gesetzlich zu einer anderen Verarbeitung verpflichtet, teilt er dies dem Verantwortlichen vorher mit, soweit das Gesetz es nicht verbietet.

§ 3 Vertraulichkeit

Der Auftragsverarbeiter setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen. Zugriff auf Kundendaten erhalten sie nur, soweit es für Betrieb, Support oder Fehlerbehebung nötig ist.

§ 4 Technische und organisatorische Maßnahmen

1. Der Auftragsverarbeiter trifft die Maßnahmen nach Art. 32 DSGVO, die in **Anlage 1** beschrieben sind.
2. Er darf die Maßnahmen an den Stand der Technik anpassen, solange das Schutzniveau nicht sinkt. Wesentliche Änderungen dokumentiert er.

§ 5 Unterauftragsverarbeiter

1. Der Verantwortliche genehmigt die in **Anlage 2** genannten Unterauftragsverarbeiter.
2. Der Verantwortliche erteilt eine allgemeine Genehmigung für weitere Unterauftragsverarbeiter. Der Auftragsverarbeiter kündigt jede Änderung mindestens 30 Tage vorher in Textform an. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Kommt keine Einigung zustande, kann er den Hauptvertrag zum Wirksamwerden der Änderung kündigen.
3. Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten wie in diesem Vertrag.
4. Keine Unterauftragsverarbeitung sind Nebenleistungen wie Telekommunikation, Post oder Zahlungsabwicklung, soweit dabei keine Daten des Verantwortlichen aus Mileon verarbeitet werden.

§ 6 Rechte der betroffenen Personen

Der Auftragsverarbeiter unterstützt den Verantwortlichen mit den Funktionen von Mileon (Anzeigen, Ändern, Exportieren, Löschen) bei Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragbarkeit. Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter.

§ 7 Unterstützung und Meldung von Verletzungen

1. Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO.
2. Er unterstützt den Verantwortlichen bei Meldungen an die Aufsichtsbehörde, bei Benachrichtigungen betroffener Personen, bei Datenschutz-Folgenabschätzungen und bei vorherigen Konsultationen (Art. 32 bis 36 DSGVO).

§ 8 Nachweise und Kontrollen

1. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Pflichten aus Art. 28 DSGVO nötig sind.
2. Der Verantwortliche oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer darf Kontrollen durchführen. Vor-Ort-Kontrollen sind mit mindestens 14 Tagen Vorlauf anzumelden, finden während der Geschäftszeiten statt und dürfen den Betrieb nicht unangemessen stören. Aktuelle Prüfberichte oder Zertifikate können eine Kontrolle ersetzen.

§ 9 Löschung und Rückgabe

1. Nach Ende des Hauptvertrags kann der Verantwortliche seine Daten bis zu 30 Tage lang über die Exportfunktionen von Mileon herunterladen.
2. Danach löscht der Auftragsverarbeiter die Instanz mit allen Daten, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht. Sicherungskopien werden spätestens 30 Tage nach der Löschung der Instanz gelöscht.
3. Die Löschung bestätigt der Auftragsverarbeiter auf Anfrage in Textform.

§ 10 Haftung und Schlussbestimmungen

1. Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregeln des Hauptvertrags.
2. Änderungen und Ergänzungen bedürfen der Textform. Der Vertrag kann elektronisch geschlossen werden (Art. 28 Abs. 9 DSGVO), z. B. durch Bestätigung bei der Registrierung.
3. Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam. An ihre Stelle tritt eine Regelung, die dem Zweck der DSGVO am nächsten kommt.
4. Es gilt deutsches Recht. Gerichtsstand ist, soweit zulässig, der Sitz des Auftragsverarbeiters.

Anlage 1 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Schutzziel	Maßnahmen bei Mileon
Zutrittskontrolle	Server im Rechenzentrum des Hosting-Anbieters (Anlage 2) mit dessen physischer Zutrittskontrolle; keine Kundendaten in eigenen Büroräumen gespeichert

Schutzziel	Maßnahmen bei Mileon
Zugangskontrolle	Anmeldung nur mit persönlichem Konto; Passwörter mit Argon2 gehasht, Mindestlänge 12 Zeichen; Server-Zugang nur per SSH für die Geschäftsführung; Verwaltungsoberfläche mit Zwei-Faktor-Anmeldung; Einmal-Links zum Hochladen von Schadenfotos sind zeitlich begrenzt, jederzeit sperrbar, nur für einen Schaden gültig und nur als Prüfwert gespeichert
Zugriffskontrolle	Rollen und Rechte je Station (Administrator, Head of Operations, Station Manager, HR-Manager, Disponent, Nur lesen); Lohn- und Bankdaten nur für Administrator und HR-Manager; Abmeldung aller Sitzungen bei Rollenänderung
Trennungskontrolle	Eigene Instanz und eigene Datenbank je Kunde; kein Zugriff zwischen Kunden
Pseudonymisierung und Verschlüsselung	Übertragung ausschließlich verschlüsselt per HTTPS (TLS); Steuer-ID, Sozialversicherungsnummer, IBAN und Lohnangaben zusätzlich verschlüsselt gespeichert; Fotos werden beim Hochladen ohne Standort- und Gerätedaten gespeichert
Weitergabekontrolle	Exporte nur durch berechtigte Benutzer; Schutz gegen Fremdaufrufe von Formularen (CSRF-Schutz); E-Mails nur an die Adressen, die der Verantwortliche angibt
Eingabekontrolle	Änderungsprotokoll mit Benutzer und Zeitpunkt für wesentliche Änderungen
Verfügbarkeit und Belastbarkeit	Tägliche Datensicherung je Kunde; zusätzliche Sicherung vor jedem Update; Überwachung des Betriebszustands der Instanzen
Wiederherstellbarkeit	Wiederherstellung einer Instanz aus der Sicherung; Updates mit vorheriger Sicherung
Regelmäßige Überprüfung	Automatische Tests vor jeder neuen Version; Überprüfung dieser Maßnahmen mindestens einmal jährlich

Anlage 2 – Genehmigte Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung
IONOS SE, Elgendorfer Str. 57, 56410 Montabaur	Hosting des Servers (Rechenzentrum)	Europäische Union
IONOS SE, Elgendorfer Str. 57, 56410 Montabaur	Versand von E-Mails (Einladungen, Bestätigungen, Erinnerungen)	Europäische Union

Die Zahlungsabwicklung über Stripe betrifft nur die Vertrags- und Rechnungsdaten des Verantwortlichen selbst, nicht die Daten in Mileon. Sie ist deshalb keine Unterauftragsverarbeitung nach diesem Vertrag.

Ort, Datum, Unterschrift Verantwortlicher

Monheim am Rhein, Datum, Unterschrift Mileon GmbH
(Leon-Mile Subasic, Geschäftsführer)