

Vertrag zur Auftragsverarbeitung (AVV)

Anlage 2 zu den AGB für DALNO · gemäß Art. 28 DSGVO · Version 2.1 · abrufbar unter dalno.app/avv.html

Vertragsschluss. Diese AVV ist Anlage 2 zu den AGB für DALNO. Sie wird mit Annahme des Angebots Bestandteil des Vertrags, ohne gesonderte Unterschrift. Art. 28 Abs. 9 DSGVO lässt dafür die elektronische Form zu. Die AVV ist unter dalno.app/avv.html abrufbar und kann dort als PDF gespeichert werden; auf Wunsch sendet der Auftragsverarbeiter sie per E-Mail.

Präambel

Zwischen den Parteien besteht ein Vertrag über die Nutzung von DALNO nach den AGB („Hauptvertrag“). DALNO ermöglicht das Melden von Verkäufen und Beständen durch Verkaufsstellen und das Bestellen durch Geschäftskunden des Verantwortlichen. Dabei verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen. Diese AVV regelt die Pflichten der Parteien nach Art. 28 DSGVO.

§ 1 Gegenstand und Dauer

(1) Gegenstand ist die Bereitstellung von DALNO als Online-Dienst zur Erfassung und Auswertung von Verkäufen, Beständen und Bestellungen. Die Verarbeitung umfasst Speicherung, Auswertung und Bereitstellung der Daten, die der Verantwortliche und seine Nutzer eingeben.

(2) Die Verarbeitung dauert so lange wie der Hauptvertrag. § 11 bleibt unberührt.

§ 2 Art und Zweck der Verarbeitung

(1) Art der Verarbeitung:

- Erfassung von Daten über die Apps (Melden, Bestellen) und die Büro-Oberfläche
- Speicherung in einer Datenbank auf Servern in Deutschland
- Anzeige, Auswertung und Zusammenfassung für Berichte
- Exporte (Excel, CSV, PDF) zur Weiterverarbeitung beim Verantwortlichen
- Versand von Push-Benachrichtigungen an Endgeräte der Nutzer
- Protokollierung sicherheitsrelevanter Vorgänge (Audit-Log)
- Datensicherungen

(2) Die Verarbeitung dient ausschließlich der Bereitstellung von DALNO nach dem Hauptvertrag. Eine Nutzung zu eigenen Zwecken des Auftragsverarbeiters ist ausgeschlossen.

§ 3 Art der personenbezogenen Daten

- Stammdaten der Nutzer: Vorname, Nachname, Benutzername, ggf. E-Mail-Adresse oder Telefonnummer, soweit der Verantwortliche sie hinterlegt
- Zugangsdaten: Passwort als Hash (bcrypt), TOTP-Geheimnis verschlüsselt
- Rolle und Zuordnung zu Verkaufsstellen bzw. Geschäftskunden
- Stammdaten der Geschäftskunden des Verantwortlichen: Firmenname, Anschrift, Ansprechpartner, Lieferdaten
- Aktivitätsdaten: Meldungen, Bestellungen, Mengen, Preise und Zeitstempel
- Audit-Daten: Anmeldeversuche, sicherheitsrelevante Aktionen, Änderungen an Bestellungen

- Push-Daten: gerätebezogene Tokens für Benachrichtigungen

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO werden nicht verarbeitet.

§ 4 Kategorien betroffener Personen

- Mitarbeiter des Verantwortlichen, insbesondere an Verkaufsstellen, im Innendienst und als Administratoren
- Ansprechpartner und Nutzer der Geschäftskunden des Verantwortlichen, die über die Bestell-App bestellen

§ 5 Pflichten des Auftragsverarbeiters

(1) **Weisungen.** Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen. Der Hauptvertrag und diese AVV gelten als Weisung. Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich.

(2) **Vertraulichkeit.** Der Auftragsverarbeiter verpflichtet alle Personen, die mit der Verarbeitung befasst sind, auf Vertraulichkeit.

(3) **Sicherheit.** Der Auftragsverarbeiter trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Sie stehen in Anhang 1, werden regelmäßig überprüft und dem Stand der Technik angepasst.

(4) **Unterstützung.** Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des Möglichen bei Anfragen betroffener Personen (Art. 15 bis 22 DSGVO), bei der Sicherheit der Verarbeitung (Art. 32), bei Meldungen von Datenschutzverletzungen (Art. 33, 34), bei Datenschutz-Folgenabschätzungen (Art. 35) und bei der Konsultation der Aufsichtsbehörde (Art. 36).

(5) **Ansprechpartner Datenschutz.** Ein Datenschutzbeauftragter ist beim Auftragsverarbeiter derzeit gesetzlich nicht vorgeschrieben. Ansprechpartner für alle Fragen des Datenschutzes ist Rainer Huber, Geschäftsführer, erreichbar unter info@dalno.app. Wird ein Datenschutzbeauftragter benannt, teilt der Auftragsverarbeiter dessen Kontaktdaten mit.

§ 6 Pflichten des Verantwortlichen

(1) Der Verantwortliche stellt sicher, dass die Verarbeitung eine Rechtsgrundlage nach Art. 6 DSGVO hat, und informiert die betroffenen Personen nach Art. 13, 14 DSGVO.

(2) Der Verantwortliche benennt eine weisungsberechtigte Person. Weisungen erteilt er in Textform; mündliche Weisungen bestätigt er unverzüglich in Textform.

(3) Stellt der Verantwortliche Fehler oder Unregelmäßigkeiten im Hinblick auf den Datenschutz fest, informiert er den Auftragsverarbeiter unverzüglich.

§ 7 Unterauftragsverarbeiter

(1) Der Verantwortliche genehmigt mit Vertragsschluss die folgenden Unterauftragsverarbeiter:

Unterauftragsverarbeiter	Sitz	Gegenstand
IONOS SE	Deutschland (Montabaur; Rechenzentren in Deutschland)	Hosting der Server, Speicherung der Datenbank und der Datensicherungen

(2) Über beabsichtigte Änderungen informiert der Auftragsverarbeiter mindestens 30 Tage vorher in Textform. Der Verantwortliche kann innerhalb von 14 Tagen nach der Information aus berechtigten Gründen in Textform widersprechen. Bei einem Widerspruch kann jede Partei den Hauptvertrag zum Ende des laufenden Vertragsjahres kündigen.

(3) Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten, die ihn selbst treffen.

§ 8 Rechte der betroffenen Personen

Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter. Er unterstützt den Verantwortlichen insbesondere durch:

- Bereitstellung der gespeicherten Daten in einem strukturierten, gängigen und maschinenlesbaren Format
- Löschung oder Berichtigung einzelner Datensätze auf Weisung
- Einschränkung der Verarbeitung einzelner Datensätze auf Weisung

Eigenmächtige Auskünfte an betroffene Personen oder Dritte erteilt der Auftragsverarbeiter nicht.

§ 9 Meldung von Datenschutzverletzungen

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, über jede Verletzung des Schutzes personenbezogener Daten. Die Meldung enthält mindestens:

- Art der Verletzung mit Kategorien und ungefährender Zahl der betroffenen Personen und Datensätze
- Name und Kontaktdaten einer Anlaufstelle
- wahrscheinliche Folgen der Verletzung
- ergriffene oder vorgeschlagene Maßnahmen

Er unterstützt den Verantwortlichen bei der Meldung an die Aufsichtsbehörde (Art. 33 DSGVO) und gegebenenfalls bei der Benachrichtigung betroffener Personen (Art. 34 DSGVO).

§ 10 Kontrollen

(1) Der Auftragsverarbeiter weist die Einhaltung dieser AVV auf Anforderung nach, etwa durch das aktuelle Verzeichnis der Maßnahmen (Anhang 1), vorhandene Zertifikate oder Prüfberichte oder schriftliche Auskünfte zu Einzelfragen.

(2) Der Verantwortliche darf sich nach Ankündigung von in der Regel mindestens 14 Tagen während der üblichen Geschäftszeiten vor Ort überzeugen. Kontrollen beschränken sich auf das Erforderliche und stören den Betrieb nicht unverhältnismäßig. Ihre Kosten trägt der Verantwortliche.

§ 11 Vertragsende und Löschung

(1) **Rückgabe.** Der Verantwortliche kann seine Daten bis Vertragsende selbst exportieren. Auf Anforderung stellt der Auftragsverarbeiter nach Vertragsende einen Gesamtexport in einem strukturierten, gängigen und maschinenlesbaren Format bereit (§ 16 Abs. 2 AGB).

(2) **Löschung.** Spätestens 30 Tage nach Vertragsende löscht der Auftragsverarbeiter alle personenbezogenen Daten des Verantwortlichen aus dem laufenden System. Kopien in Datensicherungen werden mit Ablauf ihrer Aufbewahrungsfrist nach Anhang 1 Nr. 3.1 gelöscht, spätestens nach 12 Monaten. Bis dahin werden sie nicht verarbeitet und nur für eine Wiederherstellung vorgehalten. Die Löschung bestätigt der Auftragsverarbeiter auf Anforderung in Textform.

(3) **Aufbewahrungspflichten.** Daten, für die gesetzliche Aufbewahrungspflichten bestehen, werden nach Ablauf der jeweiligen Frist gelöscht und bis dahin nur für diesen Zweck aufbewahrt.

§ 12 Schlussbestimmungen

- (1) Änderungen dieser AVV gelten wie Änderungen der AGB (§ 17 Abs. 2 AGB). Änderungen, die gesetzliche Vorgaben umsetzen oder die Maßnahmen in Anhang 1 verbessern, darf der Auftragsverarbeiter mit Mitteilung in Textform vornehmen; das Schutzniveau darf dabei nicht sinken.
- (2) Bei Widersprüchen zwischen Hauptvertrag und dieser AVV geht die AVV in Fragen des Datenschutzes vor.
- (3) Ist eine Bestimmung unwirksam, bleibt die AVV im Übrigen wirksam.
- (4) Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts. Gerichtsstand ist Aichach, soweit gesetzlich zulässig.

Anhang 1: Technische und organisatorische Maßnahmen (TOM)

Der Auftragsverarbeiter trifft nach Art. 32 DSGVO die folgenden Maßnahmen.

1. Vertraulichkeit

Zutrittskontrolle

- Hosting bei IONOS in zertifizierten Rechenzentren in Deutschland mit physischer Zugangskontrolle
- Kein direkter physischer Zugang des Auftragsverarbeiters zur Server-Hardware

Zugangskontrolle

- Persönliche Benutzerkonten mit Passwortrichtlinien, Passwörter als bcrypt-Hash
- Pflicht zur Zwei-Faktor-Anmeldung (TOTP) für administrative Rollen
- SSH-Zugang zum Server nur mit Schlüssel
- Kontosperre nach 5 Fehlversuchen für 15 Minuten, Begrenzung der Anmeldeversuche

Zugriffskontrolle

- Rollenbasiertes Berechtigungskonzept
- Trennung der Mandanten über eine Mandantenkennung in jeder Fachtabelle, geprüft auf Anwendungsebene
- Audit-Log sicherheitsrelevanter Aktionen mit Mandant, Benutzer und Zeitstempel
- Automatisierte Tests gegen mandantenübergreifende Zugriffe vor jedem Release

Trennung

- Getrennte Produktiv- und Entwicklungsumgebung mit eigener Datenbank
- Mandantenbezogene Wiederherstellung aus Sicherungen möglich

Verschlüsselung und Hashing

- Passwörter ausschließlich als bcrypt-Hash
- TOTP-Geheimnisse verschlüsselt

2. Integrität

Weitergabekontrolle

- Übertragung nur verschlüsselt per HTTPS (TLS) mit Let's-Encrypt-Zertifikaten
- HSTS erzwingt verschlüsselte Verbindungen

Eingabekontrolle

- Audit-Log aller Änderungen an Bestellungen mit Benutzer und Zeitstempel
- Versionierte Speicherung von Preisänderungen mit Gültigkeitszeitraum

- Protokollierung administrativer Aktionen

3. Verfügbarkeit und Belastbarkeit

3.1 Datensicherung

- Tägliche Sicherung der Datenbank, aufbewahrt 14 Tage
- Wöchentliche Kopie an einem zweiten Ort, aufbewahrt 12 Wochen
- Monatliche Sicherung, aufbewahrt 12 Monate
- Dokumentierte Wiederherstellungsübungen zweimal im Jahr

3.2 Wiederherstellung

- Wiederherstellungszeit (RTO) 4 Stunden, maximaler Datenverlust (RPO) 24 Stunden

3.3 Schutz und Überwachung

- Ubuntu LTS mit automatischen Sicherheitsupdates
- Firewall mit minimaler Portöffnung (22, 80, 443), Fail2Ban gegen Brute-Force-Angriffe
- Regelmäßige Updates aller Abhängigkeiten
- Überwachung der Erreichbarkeit alle 5 Minuten mit Alarmierung

4. Regelmäßige Überprüfung

- Jährliche Überprüfung dieser Maßnahmen
- Penetrationstests vor größeren Releases oder wesentlichen Architekturänderungen
- Laufende Beobachtung von Sicherheitslücken in eingesetzten Komponenten
- Datenschutz-Folgenabschätzung bei neuen Funktionen, soweit erforderlich

5. Organisatorische Maßnahmen

- Schriftliche Verpflichtung aller Mitarbeiter auf Vertraulichkeit
- Regelmäßige Datenschutzs Schulungen
- Klare Zuständigkeiten
- Dokumentierte Abläufe für Datenschutzanfragen und Vorfälle

consatic GmbH · Aichacherstraße 16 A · 86551 Aichach · Stand: Oktober 2026