Feldmelder

Auftragsverarbeitungsvertrag

Stand: 30. Oktober 2026

Auftragsverarbeitungsvertrag nach Art. 28 DSGVO zwischen dem Kunden als Verantwortlichem (im Folgenden „Auftraggeber“) und dem Anbieter als Auftragsverarbeiter (im Folgenden „Auftragnehmer“):

Feldmelder ist ein Angebot eines Einzelunternehmens, Albert-Altwicker-Straße 31, 47445 Moers, Deutschland (im Folgenden „Anbieter“; Inhaber und vollständige Angaben im Impressum).

1. Gegenstand und Dauer

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers, um die im Hauptvertrag vereinbarten Leistungen von Feldmelder zu erbringen (Portal, Datenempfang von den Feldmelder Boxen, Alarmierung, Auswertungen, Export). Der Vertrag gilt für die Dauer des Hauptvertrags.

2. Art und Zweck der Verarbeitung

Empfangen, Speichern, Auswerten und Anzeigen von Anlagendaten; Versand von Alarmmeldungen an die vom Auftraggeber hinterlegten Kontakte; Verwaltung der Nutzerkonten des Auftraggebers; Protokollierung sicherheitsrelevanter Aktionen; Erstellung von Exporten und Berichten; Datensicherung.

3. Datenarten

- Nutzerdaten: E-Mail-Adresse, Rolle, Spracheinstellung, Anmeldeprotokolle (Zeitpunkt, IP-Adresse), Audit-Log-Einträge, Telegram-Chat-ID;
- Kontaktdaten für Alarme: Name, E-Mail-Adresse, Telefonnummer, Telegram-Chat-ID;
- Anlagen- und Betriebsdaten (Winkel, Betriebsart, Wetterwerte, Alarme, Befehle und Quittungen), soweit sie einer Person zugeordnet werden können;
- Inhalte von Exporten und Berichten.

4. Kreis der Betroffenen

Beschäftigte und Beauftragte des Auftraggebers, die das Portal nutzen oder als Alarmkontakt hinterlegt sind, sowie Personen, denen der Auftraggeber Zugang gewährt (z. B. Wartungsdienstleister).

5. Weisungen

Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers; der Hauptvertrag und die Einstellungen, die der Auftraggeber im Portal vornimmt, gelten als Weisung. Weitere Weisungen erteilt der Auftraggeber in Textform. Hält der Auftragnehmer eine Weisung für rechtswidrig, teilt er dies unverzüglich mit. Eine Verarbeitung aufgrund gesetzlicher Pflicht teilt er vorher mit, soweit das Gesetz dies nicht verbietet.

6. Vertraulichkeit

Der Auftragnehmer setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.

7. Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft die in der Anlage beschriebenen Maßnahmen nach Art. 32 DSGVO. Er darf sie durch gleichwertige oder bessere Maßnahmen ersetzen und dokumentiert Änderungen.

8. Unterauftragsverarbeiter

Der Auftraggeber genehmigt die folgenden Unterauftragsverarbeiter:

- Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA – DNS, Reverse Proxy und TLS-Terminierung für Website und Portal; Übermittlung auf Grundlage des EU-US Data Privacy Framework und der Standardvertragsklauseln;
- Sendinblue SAS (Brevo), 106 boulevard Haussmann, 75008 Paris, Frankreich – Versand von E-Mails (Alarmmeldungen, Einladungen, Passwort-Zurücksetzen);
- vorgesehen für den Produktivbetrieb: Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland – Serverbetrieb im Rechenzentrum in Deutschland. Der Auftragnehmer kündigt den Wechsel vorher an.

Über neue oder geänderte Unterauftragsverarbeiter informiert der Auftragnehmer mindestens vier Wochen vorher in Textform; der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund widersprechen. Telegram ist kein Unterauftragsverarbeiter: Meldungen über Telegram versendet der Auftragnehmer nur, wenn der Auftraggeber diesen Kanal für einen Kontakt einrichtet.

9. Unterstützung des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber im angemessenen Umfang bei der Beantwortung von Anträgen betroffener Personen, bei der Meldung von Datenschutzverletzungen und bei Datenschutz-Folgenabschätzungen. Er meldet dem

Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich, nachdem sie ihm bekannt geworden sind.

10. Löschung und Rückgabe

Nach Ende des Hauptvertrags stellt der Auftragnehmer dem Auftraggeber auf Wunsch die Daten als Export bereit und löscht sie anschließend, spätestens drei Monate nach Vertragsende, soweit keine gesetzliche Pflicht zur Aufbewahrung besteht. Datensicherungen werden im Rahmen der regulären Rotation überschrieben.

11. Nachweise und Kontrollen

Der Auftragnehmer stellt dem Auftraggeber die zum Nachweis der Pflichten nötigen Informationen zur Verfügung und ermöglicht Überprüfungen nach rechtzeitiger Anmeldung in Textform, während der üblichen Geschäftszeiten und ohne Störung des Betriebs. Zunächst genügt in der Regel eine schriftliche Auskunft.

12. Haftung

Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregeln des Hauptvertrags.

Anlage: Technische und organisatorische Maßnahmen

- **Verschlüsselung der Übertragung:** Website und Portal nur über HTTPS (TLS); die Feldmelder Boxen übertragen über MQTT mit TLS.
- **Geräteidentität:** jede Box weist sich mit einem eigenen Client-Zertifikat aus (mTLS); widerrufene Zertifikate werden über eine Sperrliste abgewiesen.
- **Befehle:** Fernbefehle an Anlagen sind digital signiert und nur kurze Zeit gültig; die Box prüft Signatur und Gültigkeit vor der Ausführung.
- **Zugang:** Passwörter nur als Argon2id-Hash; Zwei-Faktor-Anmeldung für Administratoren und alle, die Befehle senden dürfen; Begrenzung von Anmeldeversuchen.
- **Berechtigungen:** rollenbasierte Rechte; strikte Trennung der Daten verschiedener Kunden (Mandanten).
- **Nachvollziehbarkeit:** Audit-Log sicherheitsrelevanter Aktionen, Protokollierung von Anmeldungen und Befehlen.
- **Verfügbarkeit:** tägliche Datensicherung mit getesteter Wiederherstellung; die Box steuert die Anlage auch ohne Verbindung zum Portal weiter und puffert Daten bis zur Wiederverbindung.
- **Standort:** Server in Deutschland.
- **Betrieb:** Protokollierung des Server- und Anwendungsbetriebs; Stückliste der Softwarekomponenten mit automatischer Prüfung auf bekannte Schwachstellen.

Ort, Datum, Unterschrift Auftraggeber

Ort, Datum, Unterschrift Auftragnehmer