

Vertrag zur Auftragsverarbeitung

Muster nach Art. 28 DSGVO für die Zusammenarbeit mit Elektrobetrieben und anderen Unternehmen. Stand: 30.08.2026

Zwischen

dem Auftraggeber – nachfolgend „Verantwortlicher“

Firma: _____

Anschrift: _____

Vertreten durch: _____

Ansprechpartner Datenschutz: _____

und

dem Auftragnehmer – nachfolgend „Auftragsverarbeiter“

RaumFaktum Rheinland GmbH (Marke MyKonnex)

Kohlenstraße 1, 42555 Velbert

Vertreten durch: Dennis Jan Ott

Kontakt Datenschutz: info@raumfaktum.de

§ 1 Gegenstand, Dauer und Zweck

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Rahmen der zwischen den Parteien vereinbarten Leistungen. Das sind insbesondere:

- Erstellung und Bearbeitung von ETS-Projekten (Fernprojektierung)
- Ferndiagnose bei Störungen (Notdienst)
- Auswertung übergebener Projektdateien (Kurzcheck und Audit)
- Erstellung von Übergabedokumentationen

(2) Der Vertrag beginnt mit der Beauftragung und endet mit Abschluss des jeweiligen Auftrags, bei laufender Zusammenarbeit mit deren Beendigung.

(3) Die Verarbeitung findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt. Eine Verarbeitung in einem Drittland erfolgt nicht.

§ 2 Art der Daten und Kreis der Betroffenen

(1) Gegenstand der Verarbeitung sind folgende Datenarten:

- Angaben aus ETS-Projektdateien, soweit sie einen Personenbezug aufweisen – etwa Raum- und Gerätebezeichnungen mit Namen, Projektbezeichnungen mit Kundennamen, Bearbeitervermerke
- Kontaktdaten der Ansprechpartner des Verantwortlichen und seiner Kunden
- Zugangsdaten für den befristeten Fernzugriff auf eine Anlage
- Anlagen- und Betriebsdaten, die während einer Ferndiagnose sichtbar werden, insbesondere Präsenz-, Schalt- und Verbrauchsdaten
- Objektbezogene Angaben wie Anschriften und Grundrisse

(2) Betroffene Personen sind:

- Kunden des Verantwortlichen und deren Haushaltsangehörige
- Beschäftigte des Verantwortlichen
- Nutzer der betreuten Gebäudeautomation

(3) Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht Gegenstand des Auftrags. Der Verantwortliche übermittelt solche Daten nicht.

§ 3 Weisungsbindung

(1) Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Die vertraglich vereinbarte Leistungserbringung gilt als Weisung.

(2) Weisungen erfolgen in Textform. Mündliche Weisungen werden unverzüglich in Textform bestätigt.

(3) Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies unverzüglich mit. Er ist berechtigt, die Ausführung auszusetzen, bis die Weisung bestätigt oder geändert wird.

§ 4 Vertraulichkeit

(1) Der Auftragsverarbeiter verpflichtet alle mit der Verarbeitung befassten Personen zur Vertraulichkeit, soweit sie nicht bereits einer gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Die Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft die in **Anlage 1** beschriebenen Maßnahmen nach Art. 32 DSGVO und hält sie während der Vertragsdauer aufrecht.

(2) Maßnahmen dürfen angepasst werden, solange das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert.

§ 6 Unterauftragsverarbeiter

(1) Der Verantwortliche stimmt dem Einsatz der in **Anlage 2** genannten Unterauftragsverarbeiter zu.

(2) Weitere Unterauftragsverarbeiter werden vorher mitgeteilt. Der Verantwortliche kann innerhalb von vierzehn Tagen widersprechen; bei berechtigtem Widerspruch besteht ein Sonderkündigungsrecht.

(3) Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter auf ein Schutzniveau, das diesem Vertrag entspricht.

(4) Nicht als Unterauftragsverarbeitung gelten Nebenleistungen wie Telekommunikation, Reinigung oder die Wartung von Hardware ohne Zugriff auf Auftragsdaten.

§ 7 Unterstützung des Verantwortlichen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Beantwortung von Anträgen betroffener Personen nach Art. 12 bis 23

DSGVO.

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet er das Anliegen unverzüglich weiter und beantwortet es nicht selbst.

(3) Der Auftragsverarbeiter unterstützt bei den Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei einer Datenschutz-Folgenabschätzung.

(4) Verletzungen des Schutzes personenbezogener Daten meldet der Auftragsverarbeiter unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, in Textform an den Verantwortlichen.

§ 8 Löschung und Rückgabe

(1) Nach Abschluss des Auftrags gibt der Auftragsverarbeiter die Daten nach Wahl des Verantwortlichen zurück oder löscht sie, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

(2) Ergänzend gelten folgende Fristen:

- Dateien aus dem kostenlosen Kurzcheck: automatische Löschung nach neunzig Tagen, auf Wunsch früher
- Projektdaten laufender Aufträge: Aufbewahrung bis zum Abschluss zuzüglich der gesetzlichen Fristen für Nachweis und Gewährleistung
- Zugangsdaten für Fernzugriff: Löschung unmittelbar nach dem Termin

(3) Die Löschung wird auf Anforderung in Textform bestätigt.

§ 9 Nachweise und Kontrollen

(1) Der Auftragsverarbeiter weist die Einhaltung der Pflichten auf Anfrage in geeigneter Weise nach, insbesondere durch Auskunft und Vorlage der Dokumentation zu Anlage 1.

(2) Der Verantwortliche kann nach vorheriger Ankündigung mit angemessener Frist während der üblichen Geschäftszeiten Kontrollen durchführen oder durchführen lassen. Der Auftragsverarbeiter kann Prüfer ablehnen, die zu ihm im Wettbewerb stehen.

(3) Kontrollen dürfen den Geschäftsbetrieb nicht unangemessen beeinträchtigen. Über den ersten Kontrolltermin je Kalenderjahr hinausgehende Kontrollen kann der Auftragsverarbeiter nach Aufwand berechnen, sofern kein Anlass in seiner Sphäre besteht.

§ 10 Schlussbestimmungen

(1) Dieser Vertrag geht bei Widersprüchen den übrigen Vereinbarungen der Parteien im Hinblick auf den Datenschutz vor.

(2) Änderungen bedürfen der Textform. Das gilt auch für die Aufhebung dieses Formerfordernisses.

(3) Es gilt das Recht der Bundesrepublik Deutschland.

(4) Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Unterschrift, Name in Druckbuchstaben

Unterschrift, Name in Druckbuchstaben

Anlage 1: Technische und organisatorische Maßnahmen

Vertraulichkeit

- **Zutrittskontrolle:** Geschäftsräume verschlossen, Serverstandort in einem Rechenzentrum in Deutschland mit Zutrittssicherung durch den Betreiber
- **Zugangskontrolle:** individuelle Benutzerkonten, Zwei-Faktor-Authentifizierung bei Administrationszugängen, Passwortrichtlinie, verschlüsselte Datenträger auf allen Arbeitsgeräten
- **Zugriffskontrolle:** Zugriff auf Auftragsdaten nur für Personen, die sie zur Auftragserfüllung benötigen; Fernzugriff auf Kundenanlagen ausschließlich für den vereinbarten Termin, danach Schließung durch den Verantwortlichen oder dessen Kunden
- **Trennungskontrolle:** getrennte Ablage je Auftraggeber und Projekt

Integrität

- **Weitergabekontrolle:** Übertragung ausschließlich verschlüsselt (TLS), kein Versand unverschlüsselter Projektdaten, kein Einsatz von Cloud-Diensten außerhalb der EU für Auftragsdaten

- **Eingabekontrolle:** Protokollierung administrativer Zugriffe und der Fernzugriffe auf Kundenanlagen

Verfügbarkeit und Belastbarkeit

- Regelmäßige Sicherung der Auftragsdaten, Ablage getrennt vom Produktivsystem
- Aktuelle Betriebssysteme und zeitnahes Einspielen sicherheitsrelevanter Updates
- Virenschutz und Firewall auf allen eingesetzten Systemen
- Unterbrechungsfreie Stromversorgung und Brandschutz im Rechenzentrum des Betreibers

Verfahren zur Überprüfung und Bewertung

- **Auftragskontrolle:** Verarbeitung nur auf dokumentierte Weisung, schriftliche Verpflichtung aller Beteiligten auf Vertraulichkeit
- **Löschkonzept:** automatische Löschung der Kurzcheck-Dateien nach neunzig Tagen durch einen täglich laufenden Prozess; dokumentierte Löschung auf Anforderung
- **Datenschutz durch Voreinstellung:** Erhebung nur der Daten, die für den jeweiligen Auftrag erforderlich sind; Hinweis an Auftraggeber, Projektdateien vor Übergabe zu anonymisieren, soweit möglich
- Überprüfung der Maßnahmen mindestens jährlich sowie bei wesentlichen Änderungen

Anlage 2: Unterauftragsverarbeiter

Dienstleister	Leistung	Standort
IONOS SE	Hosting, E-Mail	Deutschland
_____	_____	_____

Die Liste wird auf Anfrage aktuell zur Verfügung gestellt. Änderungen werden nach § 6 Abs. 2 mitgeteilt.

Dieses Muster ist ein fachlich erstellter Entwurf und ersetzt keine rechtliche Prüfung. Lassen Sie es vor dem Einsatz durch einen Rechtsanwalt oder Ihren Datenschutzbeauftragten prüfen.

RaumFaktum Rheinland GmbH · Kohlenstraße 1 · 42555 Velbert · 02052 / 88 59 730 · info@raumfaktum.de