

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Präambel: Dieser Vertrag (AVV) konkretisiert die Datenschutzpflichten der Parteien im Rahmen des zwischen ihnen geschlossenen SaaS-Vertrages. Verantwortlicher ist der Kunde; Auftragsverarbeiter ist Thomas Gersmann, GeDaD – Gersmann Development and Design, Velsen 5, 48231 Warendorf.

§0 Bezug und Abschluss des AVV

(1) Dieser Auftragsverarbeitungsvertrag (AVV) ist Anlage zu und Bestandteil des zwischen dem Kunden (Verantwortlicher) und GeDaD (Auftragsverarbeiter) geschlossenen SaaS-Vertrages. Er gilt für die gesamte Dauer der Verarbeitung personenbezogener Daten im Rahmen dieses SaaS-Vertrages.

(2) Der AVV kommt mit dem Abschluss des SaaS-Vertrages zustande. Erfolgt der Vertragsschluss bzw. die Aktivierung des Zugangs elektronisch (z. B. über einen von GeDaD übersandten Aktivierungslink), so erklärt der Kunde mit der Aktivierung zugleich die Annahme dieses AVV in der zum Zeitpunkt der Aktivierung abrufbaren Fassung. SaaS-AGB und AVV werden dem Kunden vor der Aktivierung abrufbar bereitgestellt.

(3) GeDaD protokolliert den Zeitpunkt der Aktivierung, den aktivierenden Kunden bzw. Account sowie die akzeptierte Dokumentversion zum Nachweis gemäß Art. 28 Abs. 9 DSGVO (Textform/elektronische Form).

(4) Die in den Anlagen 1 (TOM) und 2 (Unterauftragsverarbeiter) genannten Maßnahmen und Unternehmen sind Bestandteil dieses AVV.

§1 Gegenstand und Dauer: Gegenstand ist die Verarbeitung personenbezogener Daten durch GeDaD ausschließlich zur Erbringung der im SaaS-Vertrag vereinbarten Leistungen. Die Dauer entspricht der Laufzeit des SaaS-Vertrages.

§2 Art, Umfang, Zweck: Erfassung, Speicherung und Bereitstellung von Verbrauchs-, Geräte- und Zuordnungsdaten zur Energie- und Zugangssteuerung. Verarbeitung ausschließlich auf dokumentierte Weisung des Verantwortlichen.

§3 Datenarten / Betroffene: Nutzungs-/Verbrauchsdaten, Geräte- und Verbindungsdaten, ggf. Zuordnungsdaten zu Stellplätzen/Personen. Betroffene: Gäste/Endnutzer des Verantwortlichen.

§4 Pflichten GeDaD: Verarbeitung nur auf Weisung; Vertraulichkeitsverpflichtung der Mitarbeiter; technische und organisatorische Maßnahmen nach Art. 32 DSGVO; Unterstützung bei Betroffenenrechten und Meldepflichten (Art. 33/34); Löschung oder Rückgabe nach Vertragsende nach Wahl des Verantwortlichen; Nachweis der Einhaltung.

§5 Unterauftragsverarbeiter: Einsatz nur mit Genehmigung; benannt sind insbesondere der Hosting-/Rechenzentrumsanbieter (Open Telecom Cloud / OTC) sowie ggf. der SIM-Konnektivitätsdienstleister. Weiterverpflichtung auf gleichwertige Pflichten.

§6 Ort der Verarbeitung: Verarbeitung innerhalb der EU/des EWR. Drittlandtransfers nur bei Vorliegen der Voraussetzungen der Art. 44 ff. DSGVO.

§7 TOM: Anlage mit technischen und organisatorischen Maßnahmen (Zugangs-/Zugriffskontrolle, Verschlüsselung TLS/DTLS, Backup, Mandantentrennung, Protokollierung) ist Bestandteil dieses Vertrages.

GeDaD Gersmann Development and Design, Velsen 5, 48231 Warendorf; Thomas Gersmann

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

Stand der Maßnahmen zum oben genannten Datum. GeDaD passt die Maßnahmen dem Stand der Technik fortlaufend an; eine Aktualisierung berührt das Schutzniveau nicht nachteilig.

1. Vertraulichkeit

Zutrittskontrolle: Verarbeitung in professionellen Rechenzentren des Infrastrukturanbieters (Open Telecom Cloud / OTC, Standorte in Deutschland) mit gesicherter Gebäude-/Serverraum-Zutrittskontrolle des Betreibers. Keine eigene On-Premise-Hardware mit personenbezogenen Daten.

Zugangskontrolle: Zugang zu Servern und Plattform ausschließlich über authentifizierte Administratorzugänge; SSH-Zugriff schlüsselbasiert; Plattformzugriff (ThingsBoard) über individuelle Benutzerkonten mit rollenbasierten Rechten; Firewall (UFW) auf den Servern, segmentiertes Subnetz, eingeschränkte Port-Freigaben.

Zugriffskontrolle: Mandanten-/Kundentrennung über getrennte Tenants bzw. Kundenzuordnung in der Plattform; rollenbasierte Berechtigungen; Beschränkung der Datenzugriffe auf das für die Leistungserbringung Erforderliche; Supportzugriff auf Kundendatensätze nur anlassbezogen und zeitlich auf die Supportmaßnahme begrenzt.

Trennungskontrolle: Logische Trennung der Kundendaten je Mandant/Kunde; getrennte Verarbeitungskontexte; Test-/Diagnoseumgebungen mit eigener Dienstkennung und ohne Vermischung produktiver Kundendaten.

Pseudonymisierung: Geräte-/Telemetriedaten werden technisch über Geräte-/Zugriffstoken adressiert; Personenbezug entsteht erst durch die Zuordnung beim Verantwortlichen.

2. Integrität

Übertragungskontrolle: Transportverschlüsselung sämtlicher Kommunikationswege: TLS für Web-/API-/MQTT-Zugriffe (TLS-Terminierung über HAProxy), DTLS für die CoAP-Geräteanbindung über NB-IoT/LTE-M; Let's-Encrypt-Zertifikate serverseitig. Keine unverschlüsselte Übertragung personenbezogener Nutzdaten über öffentliche Netze.

Eingabekontrolle: Protokollierung sicherheitsrelevanter System- und Zugriffsereignisse (Logfiles, journalctl); Nachvollziehbarkeit administrativer Eingriffe; serverseitige Plattformlogs.

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle: Regelmäßige Datensicherungen der Datenbestände; Wiederherstellungsprozedur auf Anforderung; Betrieb auf virtualisierter Cloud-Infrastruktur mit Strom-/Klima-/Netzredundanz des Rechenzentrumsbetreibers; Firewalling; Monitoring zentraler Systemparameter (u. a. Heap-/Ressourcenüberwachung, Alarmierung bei Schwellwertüberschreitung).

Rasche Wiederherstellbarkeit: Wiederherstellung aus Backups nach definierter Prozedur; Containerisierung zentraler Dienste ermöglicht zeitnahe Wiederinbetriebnahme.

Hinweis: Es wird keine bestimmte Verfügbarkeits-/Wiederherstellungszeit als Service Level zugesichert (siehe SaaS-AGB §§ 4, 9).

GeDaD Gersmann Development and Design, Velsen 5, 48231 Warendorf; Thomas Gersmann

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d)

- Verfahren zur Wahrnehmung von Betroffenenrechten und zur Löschung/Einschränkung auf Weisung des Verantwortlichen.
- Datenschutzfreundliche Voreinstellungen und Berücksichtigung bei Auswahl von Hard-/Software und Verfahren (Privacy by Design/Default).
- Auftragskontrolle: Verarbeitung ausschließlich auf dokumentierte Weisung; Unterauftragsverarbeiter nur gemäß Anlage 2 und unter Weiterverpflichtung.
- Vorfallsmanagement: Erkennung, Bewertung und Meldung von Datenschutzverletzungen an den Verantwortlichen ohne schuldhaftes Zögern zur Unterstützung der Pflichten nach Art. 33/34 DSGVO.

Anlage 2 – Genehmigte Unterauftragsverarbeiter

Der Verantwortliche genehmigt mit Abschluss des AVV den Einsatz der folgenden Unterauftragsverarbeiter. GeDaD informiert über beabsichtigte Änderungen; der Verantwortliche kann begründet widersprechen.

Unternehmen	Leistung	Ort der Verarbeitung	Grundlage Drittland
Open Telecom Cloud (OTC), betrieben durch T-Systems International GmbH	Hosting, Rechen-/Speicherkapazität, Rechenzentrumsinfrastruktur	Deutschland (EU)	entfällt (EU)
1NCE GmbH	Mobilfunk-Konnektivität (NB-IoT/LTE-M) für die Geräteanbindung	EU	entfällt (EU)