

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag (Art. 28 DSGVO)

Vorlage für Kunden von Ignis IQ · Fassung 1.1 vom 17.10.2026 · ohne anwaltliche Freigabe, vor Verwendung prüfen lassen

Vertragsparteien

- Verantwortlicher (Auftraggeber): [Firma, Anschrift, vertreten durch] – nachfolgend „Verantwortlicher“
- Auftragsverarbeiter (Auftragnehmer): itcv GmbH, Solmsstr. 71, 60486 Frankfurt am Main, vertreten durch den Geschäftsführer Jürgen Voskuhl, Registergericht Frankfurt am Main, HRB 98502 – nachfolgend „Auftragsverarbeiter“ (Leistung: Ignis IQ)

§ 1 Gegenstand und Dauer

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Rahmen des Erst-Audit-Auftrags und des Servicevertrags „Ignis IQ – Fristen- und Nachweisservice für Rauchwarnmelder“ (Hauptvertrag).

(2) Der Vertrag gilt für die Dauer des Hauptvertrags und darüber hinaus, solange der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen verarbeitet.

(3) Der Vertrag wird vor der ersten Datenübergabe in Textform angenommen (Art. 28 Abs. 9 DSGVO).

§ 2 Art und Zweck der Verarbeitung, Datenarten, Betroffene

(1) Art: Erheben (Import der vom Verantwortlichen gelieferten Daten), Speichern, Ordnen, Auswerten, Bereitstellen über die Web-Anwendung, Erzeugen von Berichten und Nachweismappen, Löschen.

(2) Zweck: Feststellung und Überwachung des Prüfstatus je Einheit, Planung von Prüfterminen, Erfassung von Prüfprotokollen und Mängeln, Bereitstellung von Nachweisen für den Verantwortlichen.

(3) Datenarten:

- Objekt-, Einheiten- und Raumdaten (Adresse, Lage, Wohnungsbezeichnung)
- Gerätedaten der Rauchwarnmelder (Hersteller, Modell, Seriennummer, Einbau- und Austauschdatum)
- Prüf- und Mängeldaten (Datum, Ergebnis, Methode, Prüfer, Bemerkungen)
- Fotos von Rauchwarnmeldern und Montageort (ohne Personen)
- Termin- und Kontaktdaten von Bewohnern, soweit der Verantwortliche sie übermittelt
- Benutzerdaten der Mitarbeitenden des Verantwortlichen und der Prüfer (Name, E-Mail, Rolle)
- Protokolldaten (pseudonyme Nutzerkennung, Zeitstempel, Aktion)

(4) Betroffene: Bewohner und Eigentümer der Einheiten, Mitarbeitende des Verantwortlichen, Prüfer.

§ 3 Weisungen

(1) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Hauptvertrag und dieser Vertrag sind die Weisungen. Einzelweisungen erteilt der Verantwortliche in Textform.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen Datenschutzvorschriften verstößt.

§ 4 Vertraulichkeit

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

§ 5 Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft die Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind. Er darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt; wesentliche Änderungen teilt er mit.

§ 6 Unterauftragsverarbeiter

- (1) Allgemeine Genehmigung: Der Verantwortliche genehmigt die in Anlage 2 genannten Unterauftragsverarbeiter.
- (2) Änderungen: Der Auftragsverarbeiter kündigt die Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters mindestens 30 Tage vorher in Textform an und nennt dabei Name, Anschrift, Leistung, Ort der Verarbeitung und die Garantien. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Bei einem Widerspruch setzt der Auftragsverarbeiter den neuen Unterauftragsverarbeiter für die Daten des Verantwortlichen nicht ein; ist ihm das nicht zumutbar, können beide Parteien den Hauptvertrag mit einer Frist von 30 Tagen kündigen.
- (3) Gesonderte Genehmigung: Ein Unterauftragsverarbeiter, der personenbezogene Daten in einem Drittland verarbeitet oder auf sie aus einem Drittland zugreift und nicht in Anlage 2 genannt ist, bedarf der vorherigen gesonderten Genehmigung des Verantwortlichen in Textform.
- (4) Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind.
- (5) Kommt ein weiterer Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.
- (6) Prüfbetriebe werden vom Verantwortlichen selbst beauftragt. Sie sind keine Unterauftragsverarbeiter der itcv GmbH. Die itcv GmbH stellt ihnen nach Weisung des Verantwortlichen Zugang zur Plattform bereit.

§ 7 Übermittlung in Drittländer

- (1) Die ORDIS Co., Ltd., Bangkok, Thailand, ist Unterauftragsverarbeiter für Softwareentwicklung, Betrieb und Support und greift dafür per Fernzugriff auf die Systeme und die darin gespeicherten personenbezogenen Daten zu. Ein Fernzugriff aus Thailand ist eine Übermittlung in ein Drittland (Kapitel V DSGVO).
- (2) Für Thailand besteht kein Angemessenheitsbeschluss der Europäischen Kommission nach Art. 45 DSGVO. Grundlage der Übermittlung sind die Standardvertragsklauseln der Europäischen Kommission nach Art. 46 Abs. 2 lit. c DSGVO (Durchführungsbeschluss (EU) 2021/914), Modul 3 (Auftragsverarbeiter an Auftragsverarbeiter), zwischen der itcv GmbH und der ORDIS Co., Ltd., ergänzt durch eine dokumentierte Transfer-Folgenabschätzung und die zusätzlichen Maßnahmen in Anlage 1.
- (3) Die Daten bleiben auf den Servern in Deutschland gespeichert. Die ORDIS Co., Ltd. greift per Fernzugriff zu und legt keine dauerhaften Kopien außerhalb dieser Server an.
- (4) Auf Anfrage erhält der Verantwortliche eine Kopie der Standardvertragsklauseln einschließlich der Anhänge sowie eine Zusammenfassung der Transfer-Folgenabschätzung.
- (5) Jede weitere Übermittlung in ein Drittland erfolgt nur nach § 3 Abs. 1 und § 6 Abs. 3.

§ 8 Unterstützung des Verantwortlichen

- (1) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen (Art. 12 bis 23 DSGVO). Anfragen, die direkt bei ihm eingehen, leitet er unverzüglich weiter. Die Unterstützung erfolgt binnen 5 Werktagen.
- (2) Er unterstützt den Verantwortlichen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation) unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen.
- (3) Verletzungen des Schutzes personenbezogener Daten meldet er dem Verantwortlichen unverzüglich, spätestens binnen 24 Stunden nach Kenntnis.

§ 9 Löschung und Rückgabe

- (1) Nach Ende des Hauptvertrags erhält der Verantwortliche binnen 14 Tagen einen Herausgabe-Export (CSV und PDF mit Hash-Manifest). Danach löscht der Auftragsverarbeiter die Daten binnen 30 Tagen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht. Sicherungen werden im Rotationszyklus überschrieben (14 tägliche, 8 wöchentliche, 6 monatliche Sicherungen), spätestens sechs Monate nach der Löschung.
- (2) Die Löschung bestätigt der Auftragsverarbeiter in Textform.

§ 10 Nachweise und Überprüfungen

- (1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung.
- (2) Er ermöglicht Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten Prüfer und trägt dazu bei. Inspektionen werden 14 Tage vorher angekündigt und finden zu den Geschäftszeiten statt. Für die Rechenzentren genügt als Nachweis das Prüfprotokoll des Unterauftragsverarbeiters zu dessen technischen und organisatorischen Maßnahmen.
- (3) Überprüfungen durch die zuständige Aufsichtsbehörde (Art. 58 DSGVO) bleiben unberührt.

§ 11 Haftung

Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gilt die Haftungsregelung des Hauptvertrags, soweit sie mit Art. 82 DSGVO vereinbar ist. Gegenüber betroffenen Personen wird die Haftung nicht beschränkt.

§ 12 Schlussbestimmungen

- (1) Änderungen und Ergänzungen bedürfen der Textform.
- (2) Bei Widersprüchen geht dieser Vertrag dem Hauptvertrag in Fragen des Datenschutzes vor.
- (3) Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam.
- (4) Es gilt deutsches Recht.

Ort, Datum, Unterschrift Verantwortlicher: _____

Frankfurt am Main, Datum, Unterschrift itcv GmbH: _____

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

Vertraulichkeit

- Zutrittskontrolle: Server ausschließlich in Rechenzentren der Hetzner Online GmbH in Deutschland (Nürnberg/Falkenstein); Zutrittsschutz nach den Maßnahmen von Hetzner (Prüfprotokoll im Hetzner-Kundenkonto).
- Zugangskontrolle: Administrativer Zugang nur per SSH-Schlüssel; Firewall lässt nur HTTPS, HTTP (Weiterleitung) und SSH zu; Sperre nach wiederholten Fehlversuchen (fail2ban); Verwaltungsoberfläche des Identity Providers nur über SSH-Tunnel erreichbar.
- Anmeldung der Benutzer: selbst betriebener Identity Provider (Keycloak) auf demselben Server; Passwortrichtlinie (mindestens 12 Zeichen); vorübergehende Sperre nach wiederholten Fehlversuchen.
- Zugriffskontrolle: Rollen (Admin, Verwalter, Prüfer, Lesend); jeder Zugriff ist auf den eigenen Mandanten beschränkt (Mandantentrennung in jeder Abfrage, durch automatische Tests geprüft).
- Trennungskontrolle: logische Trennung der Mandanten in der Datenbank; Test- und Vorführungsumgebungen enthalten nur synthetische Daten.
- Fernzugriff der ORDIS Co., Ltd.: nur mit persönlichen SSH-Schlüsseln je Person über eine verschlüsselte Verbindung (SSH, bei Bedarf zusätzlich VPN); minimale Berechtigungen je Aufgabe (Entwicklung ohne Produktionszugang, Betrieb und Support nur mit dem dafür nötigen Zugang); Protokollierung jeder administrativen Anmeldung mit Person und Zeitpunkt; Entzug der Schlüssel bei Ausscheiden; quartalsweise Kontrolle der Berechtigungen durch die itcv GmbH.
- Pseudonymisierung und Datenminimierung: Protokolleinträge speichern eine pseudonyme Nutzerkennung; Fotos werden vor dem Speichern von Metadaten (EXIF/GPS) bereinigt; Anwendungslogs enthalten keine Inhalte, keine IP-Adressen und keine Namen.

Integrität

- Übertragung ausschließlich verschlüsselt (TLS, HSTS).
- Änderungen an Bestands- und Prüfdaten werden mit Zeitstempel und Nutzerkennung im Audit-Log protokolliert; Audit-Einträge können weder über die Anwendung noch in der Datenbank geändert oder gelöscht werden (Datenbank-Trigger); ihre Integrität ist über eine Hash-Kette prüfbar.
- Nachweismappen enthalten ein Manifest mit SHA-256-Prüfsummen.

Verfügbarkeit und Belastbarkeit

- Tägliche Sicherung aller Datenbanken und Fotos, verschlüsselt (GPG), lokal und auf einer Hetzner Storage Box in Deutschland; Aufbewahrung gestaffelt (täglich, wöchentlich, monatlich).
- Restore-Tests mit Prüfung der Prüfsummen und Zeilenzahlen; dokumentierter Wiederherstellungsablauf.
- Begrenzung der Anfragen je Benutzer und IP-Adresse; automatische Sicherheitsupdates des Betriebssystems.

Verfahren zur regelmäßigen Überprüfung

- Automatische Tests bei jeder Änderung der Software; Überprüfung dieser Maßnahmen mindestens jährlich und nach wesentlichen Änderungen.

Anlage 2 – Genehmigte Unterauftragsverarbeiter

- Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland – Leistung: Betrieb der Server (Cloud-Server) und Speicherung der Sicherungen (Storage Box) – Ort der Verarbeitung: Rechenzentren in Nürnberg und Falkenstein, Deutschland – Garantien: Auftragsverarbeitungsvertrag der Hetzner Online GmbH (Standardvertrag) mit der itcv GmbH vom 16.10.2026.
- ORDIS Co., Ltd., 128/196 Phayathai Plaza, 18th floor, Bangkok, Thailand (Steuernummer 0105559029458) – Leistung: Softwareentwicklung, Betrieb und Support mit Fernzugriff – Ort der Verarbeitung: Fernzugriff aus Thailand, Speicherung der Daten nur auf den Servern in Deutschland – Garantien: Standardvertragsklauseln (EU) 2021/914 Modul 3 mit der itcv GmbH, Transfer-Folgenabschätzung, Maßnahmen nach Anlage 1.