Datenschutz und Sicherheit

LIVCK Cloud ist eine Plattform für Uptime-Monitoring, Vorfallkommunikation und Statusseiten. Dieses Datenblatt fasst für Datenschutz und Informationssicherheit zusammen, wo Daten verarbeitet werden, wie sie geschützt sind und welche Verträge gelten. Rechtlich maßgeblich ist der Auftragsverarbeitungsvertrag (AVV) mit seinen Anlagen.

Betrieb in Deutschland

Plattform und Datenbanken laufen bei Hetzner in Deutschland, mit BSI-C5-Testat (Typ 2) und ISO 27001.

Speicher und Backups in Deutschland

Dateien und verschlüsselte Backups bei STACKIT (Schwarz Gruppe), mit BSI-C5-Testat (Typ 2). Zweite Kopie bei OVH in Limburg.

Durchgehend verschlüsselt

Übertragung nur per TLS 1.2 oder höher. Backups und hinterlegte Geheimnisse liegen verschlüsselt.

AVV direkt in der Konsole

Vertrag nach Art. 28 DSGVO mit TOM und Unterauftragsverarbeitern, online abschließbar.

Rollen und Daten

Für die Daten, die Kunden in LIVCK Cloud verarbeiten, ist LIVCK Auftragsverarbeiter nach Art. 28 DSGVO. Dazu gehören Teammitglieder, Kontaktdaten für Alarme, Abonnenten der Statusseiten, Inhalte von Vorfällen und die Ziele der Prüfungen. Für Registrierungs- und Rechnungsdaten ist LIVCK selbst Verantwortlicher. Messdaten werden je nach Tarif 30 bis 365 Tage gespeichert.

Wo Daten verarbeitet werden

ZWECK	ANBIETER	ORT
Plattform, Datenbanken, Zwischenspeicher	Hetzner Online GmbH C5 Typ 2	Deutschland
Objektspeicher und verschlüsselte Backups	STACKIT GmbH & Co. KG C5 Typ 2	Deutschland
Zweite Kopie von Objektspeicher und Backups	OVH SAS	Limburg, Deutschland
E-Mail-Versand	Scaleway SAS, Ausweichweg MINDBAZ SAS (Sweego)	Frankreich
SMS und Sprachanrufe	seven communications, Ausweichweg LOX24	Deutschland
Messstandorte nach Auswahl des Kunden	Rechenzentrumsbetreiber je Standort, siehe AVV Anlage 2	Deutschland, Österreich, Polen, Finnland, Schweiz

Die vollständige Liste steht in Anlage 2 des AVV und öffentlich unter livck.cloud/de/subprozessoren. Die Schweiz hat einen Angemessenheitsbeschluss der EU. Außerhalb davon wird nur verarbeitet, was der Kunde selbst wählt: der Messstandort New York auf Basis der EU-Standardvertragsklauseln sowie die persönlichen Alarmwege WhatsApp und Pushover, die einzelne Nutzer selbst einrichten. Pushover lässt sich für die ganze Organisation abschalten. Messstandorte erhalten nur die Prüfungen, die ihnen zugewiesen sind, und speichern Ergebnisse nur bis zur Übermittlung nach Deutschland.

Technische und organisatorische Maßnahmen

Anmeldung und Zugang

- Persönliche Konten, Passwörter nur als Hash
- Zwei-Faktor-Anmeldung (TOTP)
- Single Sign-on per OpenID Connect auf Anfrage
- Begrenzte Anmeldeversuche, Abmeldung nach Inaktivität
- API-Tokens gehasht, mit begrenzten Rechten und Ablaufdatum

Berechtigungen und Mandantentrennung

- Rollen mit fein abgestuften Rechten je Organisation
- Jede Datenabfrage ist an die Organisation gebunden
- Dateien und Zwischenspeicher je Organisation getrennt
- Berechtigungen werden auf dem Server geprüft

Übertragung

- Externe Verbindungen nur per TLS 1.2 oder höher
- Interne Verbindungen und Datenbank verschlüsselt
- Webhooks mit HMAC-SHA256 signiert
- Statusseiten unter eigener Domain automatisch per TLS

Speicherung

- 2FA- und Webhook-Schlüssel verschlüsselt gespeichert
- Zugangsdaten für Checks (Header, Tokens, Client-Zertifikate) verschlüsselt, erst beim Check im Arbeitsspeicher entschlüsselt
- Dateien und Backups bei beiden Speicheranbietern mit AES-256 verschlüsselt
- Serverzugang nur per SSH-Schlüssel

Nachvollziehbarkeit

- Audit-Log: wer, was, wann, Werte vorher und nachher
- Audit-Log je nach Tarif 30 Tage bis 2 Jahre
- Sitzungen mit IP-Adresse und Browser erfasst
- Zustellprotokoll für jede Benachrichtigung

Verfügbarkeit

- Redundante Infrastruktur mit automatischem Neustart
- Verschlüsselte Backups in zwei Rechenzentren in Deutschland
- Eigene Überwachung mit Alarmierung
- DDoS-Schutz auf Netzwerkebene durch Hetzner

Vertrag und Rechte der Kunden

- **AVV nach Art. 28 DSGVO:** in der Konsole unter Einstellungen › Abrechnung › AVV abschließbar und als PDF abrufbar, mit TOM, Unterauftragsverarbeitern und Ansprechpartnern als Anlagen.
- **Neue Unterauftragsverarbeiter:** Ankündigung mindestens 14 Tage vorher in Textform, mit Recht auf Einspruch.
- **Datenschutzverletzungen:** Meldung unverzüglich, in der Regel innerhalb von 48 Stunden.
- **Vertragsende:** Export in maschinenlesbarem Format, Löschung innerhalb von 30 Tagen, Bestätigung auf Anfrage.
- **Kontrolle:** Auskünfte und Einsicht in Nachweise jederzeit, Prüfung vor Ort in begründeten Fällen.

Zertifizierungen

Die Rechenzentren von Hetzner und STACKIT verfügen über ein **BSI-C5-Testat (Typ 2)**, die von Hetzner zusätzlich über **ISO 27001**. LIVCK selbst verfügt derzeit über kein eigenes C5-Testat und keine eigene ISO-27001-Zertifizierung.

DATENSCHUTZ
datenschutz@livck.com

TECHNIK
support@livck.com

AUFSICHTSBEHÖRDE
ULD Schleswig-Holstein