LIVCK.cloud

DSGVO-KONFORM · GEHOSTET IN DEUTSCHLAND

AUFTRAGSVERARBEITUNG · ART. 28 DSGVO

Auftragsverarbeitungsvertrag

Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen — gemäß Art. 28 DSGVO.

Versionsstand: 2026-11-18 · Stand: 18. November 2026

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

Versionsstand: 2026-11-18 · Stand: 18. November 2026

Vertragsparteien

Auftraggeber (Verantwortlicher):

(Muster. Beim Abschluss in der Konsole stehen hier Firma, Anschrift und USt-IdNr. des Auftraggebers.)
(nachfolgend „Auftraggeber")

Auftragnehmer (Auftragsverarbeiter):

LIVCK.cloud – René Roscher (Einzelunternehmen) Hauptstraße 1, 25813 Schwesing, Deutschland
(nachfolgend „Auftragnehmer")

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Rahmen der Bereitstellung der LIVCK Cloud Plattform für Uptime-Monitoring und Incident-Kommunikation.

(2) Der Gegenstand der Verarbeitung umfasst insbesondere:

- Bereitstellung und Betrieb der SaaS-Plattform LIVCK Cloud
- Uptime-Monitoring von digitalen Services des Auftraggebers (HTTP, TCP, DNS, ICMP, SSL)
- Betrieb öffentlicher Statuspages zur Incident-Kommunikation
- Versand von Incident-Benachrichtigungen (E-Mail, SMS, Voice/TTS)
- Verwaltung von Statuspage-Abonnenten (Subscribers)
- Bereitstellung von Metriken und Auswertungen (Uptime, Response Times)

(3) Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages (Nutzungsvertrages) zwischen Auftraggeber und Auftragnehmer. Sie beginnt mit dem Zeitpunkt, zu dem der Auftraggeber erstmals personenbezogene Daten über die Plattform bereitstellt oder verarbeiten lässt (in der Regel mit der Registrierung, die zugleich die Akzeptanz der AGB umfasst), und endet mit der vollständigen Löschung aller personenbezogenen Daten nach Vertragsende gemäß § 10 dieses Vertrages.

§ 2 Art und Zweck der Verarbeitung

(1) Die Verarbeitung personenbezogener Daten erfolgt ausschließlich zum Zweck der Erbringung der vertraglich vereinbarten Dienstleistungen gemäß dem Hauptvertrag (AGB / Nutzungsbedingungen).

(2) Die Art der Verarbeitung umfasst:

- Erheben, Erfassen und Speichern von Nutzer- und Kontaktdaten
- Verarbeiten und Übermitteln von Benachrichtigungen (E-Mail, SMS, Voice)
- Speichern und Bereitstellen von Subscriber-Daten für Statuspages
- Anzeigen und Auswerten von Monitoring-Daten
- Protokollierung von Aktivitäten (Audit Log)
- Löschen von Daten nach Vertragsende oder auf Weisung

(3) Die Protokollierung von Aktivitäten (Audit Log) erfolgt zudem zur Erfüllung der Rechenschaftspflicht des Auftragnehmers gem. Art. 5 Abs. 2 DSGVO sowie zur Erfüllung der Nachweispflichten gem. Art. 28 Abs. 3 lit. h DSGVO. Diese Protokollierung kann nicht per Weisung des Auftraggebers eingeschränkt oder abgeschaltet werden.

---

§ 3 Art der personenbezogenen Daten

Folgende Arten personenbezogener Daten sind Gegenstand der Verarbeitung:

3.1 Nutzerkonto- und Authentifizierungsdaten

- Vor- und Nachname
- E-Mail-Adresse
- Passwort (kryptografisch gehasht nach Stand der Technik)
- Zwei-Faktor-Authentifizierungsdaten (verschlüsselt gespeichert)
- Profilbild-URL (optional)
- Sprach- und Zeitzoneneinstellung
- Letzte Login-IP-Adresse und -Zeitpunkt

3.2 Organisations- und Teamdaten

- Organisationsname und Kennung
- Teammitgliedschaften und Rollen
- Einladungs-E-Mail-Adressen

3.3 Kontaktdaten für Benachrichtigungen

- E-Mail-Adressen (für Incident-Alerts)
- Telefonnummern inkl. Ländervorwahl (für SMS- und Voice-Alerts)
- Webhook-URLs (vom Auftraggeber konfiguriert)

3.4 Statuspage-Subscriber-Daten

- E-Mail-Adressen der Abonnenten
- Anzeigename (optional)
- Gewählte Benachrichtigungskanäle und -Endpunkte
- Komponentenpräferenzen (welche Services der Subscriber abonniert hat)
- Abonnement-Status und Zeitstempel

3.5 Abrechnungsdaten

- Firmenname und Kontaktperson
- Rechnungsadresse (Straße, PLZ, Ort, Land)
- E-Mail-Adresse für Rechnungen
- Umsatzsteuer-Identifikationsnummer (optional)

Hinweis: Die eigentliche Zahlungsabwicklung (Kreditkarten-, SEPA-Daten) erfolgt durch Mollie B.V. als eigenständig Verantwortlichen gem. Art. 4 Nr. 7 DSGVO. Zahlungsdaten werden nicht beim Auftragnehmer gespeichert. Der Auftraggeber weist den Auftragnehmer an, die zur Zahlungsabwicklung erforderlichen Daten (Name, E-Mail-Adresse) an Mollie B.V. zu übermitteln (siehe Anlage 2).

3.6 Technische Nutzungsdaten

- Session-Daten (IP-Adresse, User-Agent) — Speicherdauer: Dauer der aktiven Session, max. 120 Tage
- API-Token-Metadaten (Name, Nutzungszeitpunkt, IP) — Speicherdauer: Lebensdauer des Tokens
- Login-IP-Adressen — Speicherdauer: 90 Tage
- Aktivitäts- und Audit-Protokolle (Wer, Was, Wann, Vorher/Nachher) — Speicherdauer: je nach Tarif 30 Tage bis 2 Jahre

3.7 Benachrichtigungs-Zustellprotokolle

- Empfänger (E-Mail, Telefonnummer)
- Zustellstatus (gesendet, zugestellt, fehlgeschlagen)
- Zeitstempel der Zustellung
- Fehlermeldungen bei fehlgeschlagener Zustellung
- Speicherdauer: 90 Tage

3.8 Daten des Server-Monitoring-Agenten

Setzt der Auftraggeber den Server-Monitoring-Agenten auf eigenen Systemen ein, übermittelt dieser zusätzlich:

- Systemkennung: Hostname, vom Agenten erzeugte Instanz-Kennung, Hardware-Kennung (nur als kryptografischer Hash), Boot-Kennung, ggf. Instanz-ID des Cloud-Anbieters
- Systemprofil: Betriebssystem und Version, Kernel, Architektur, Virtualisierung, CPU-Modell und Kernanzahl, Arbeitsspeichergröße, Startzeitpunkt, Agent-Version
- Netzadressen des überwachten Systems: vom Agenten gemeldete private und öffentliche IP-Adressen sowie die bei der Verbindung beobachtete Absenderadresse
- Messwerte: numerische Kennzahlen zu Auslastung, Speicher, Datenträgern, Netzwerk und, sofern vorhanden, Grafik- und Laufwerksgesundheit. Sie enthalten Bezeichner der gemessenen Objekte, insbesondere Einhängepunkte, Gerätenamen und Netzwerkschnittstellen — Speicherdauer: entsprechend der tariflichen Datenaufbewahrung (30 bis 365 Tage)
- Ereignisse des überwachten Systems: Neustart, unerwarteter Neustart, Speicherengpass, volles oder schreibgeschütztes Dateisystem, Zeitabweichung, jeweils mit Zeitpunkt
- Erreichbarkeitsprüfungen: vom Auftraggeber vergebene Bezeichnung sowie Zieladresse und Port des zu prüfenden Systems

Der Agent liest keine Protokolldateien, keine Prozessnamen oder Kommandozeilen und keine Dateiinhalte; er verfügt über keinen Kommandokanal. Der Quelltext ist unter der MIT-Lizenz öffentlich einsehbar (github.com/LIVCK/agent).

Die Angaben können mittelbar Personenbezug aufweisen — insbesondere IP-Adressen, Hostnamen sowie frei vergebene Bezeichnungen und Pfadangaben, soweit der Auftraggeber dort Personennamen verwendet. Der Auftraggeber entscheidet über den Einsatz des Agenten und über die Wahl dieser Bezeichnungen.

§ 4 Kategorien betroffener Personen

Von der Verarbeitung sind folgende Kategorien betroffener Personen betroffen:

1. **Nutzer des Auftraggebers (Org-Members):** Mitarbeiter und Beauftragte des Auftraggebers, die Zugang zur LIVCK Cloud Plattform haben (Administratoren, Team-Mitglieder, Operator)
2. **Statuspage-Abonnenten (Subscribers):** Kunden oder Nutzer des Auftraggebers, die Statuspage-Benachrichtigungen über Incidents und Wartungsarbeiten abonniert haben
3. **Rechnungskontakte:** Personen, die im Rahmen der Abrechnung als Kontaktperson hinterlegt sind

§ 5 Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten gemäß den geltenden Datenschutzvorschriften verantwortlich (Art. 4 Nr. 7 DSGVO).

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten feststellt.

(3) Der Auftraggeber ist verantwortlich für die Einholung etwaiger erforderlicher Einwilligungen der betroffenen Personen, insbesondere:

- Einwilligung der Statuspage-Abonnenten zum Erhalt von Benachrichtigungen
- Information der eigenen Mitarbeiter über die Nutzung der Plattform
- Rechtsgrundlage für die Übermittlung von Kontaktdaten an die Plattform

(4) Der Auftraggeber erteilt dem Auftragnehmer die generelle Weisung, Statuspage-Subscriber-Daten bei Abmeldung (Unsubscribe) des Subscribers vollständig zu löschen. Die Abmeldung durch den Subscriber über die bereitgestellte Abmeldefunktion gilt als dokumentierte Weisung des Auftraggebers zur Löschung.

(5) Der Auftraggeber ist für die Konfiguration von Drittanbieter-Integrationen (z.B. Slack, Discord, Microsoft Teams, Telegram, Custom Webhooks) selbst verantwortlich. Die technische Übermittlung von Benachrichtigungsdaten an diese Dienste erfolgt durch den Auftragnehmer auf dokumentierte Weisung des Auftraggebers (Aktivierung der jeweiligen Integration in den Plattform-Einstellungen). Der Auftraggeber trägt die alleinige Verantwortung für die Rechtmäßigkeit der Datenübermittlung an diese Drittdienste, einschließlich etwaiger Drittlandtransfers gem. Art. 44–49 DSGVO (siehe § 9 Abs. 5).

§ 6 Pflichten des Auftragnehmers

6.1 Weisungsgebundenheit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO), es sei denn, er ist nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt.

(3) Die Weisungen des Auftraggebers werden in der Regel über die Plattform (Konfiguration, Einstellungen), per E-Mail oder über das Support-System erteilt. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

6.2 Vertraulichkeit

(1) Der Auftragnehmer gewährleistet, dass alle mit der Verarbeitung personenbezogener Daten betrauten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

(2) Diese Verpflichtung besteht auch nach Beendigung des Vertragsverhältnisses fort.

6.3 Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten. Die Maßnahmen sind in **Anlage 1 (Technisch-Organisatorische Maßnahmen)** im Detail beschrieben.

(2) Der Auftragnehmer überprüft die Wirksamkeit dieser Maßnahmen regelmäßig und passt sie dem Stand der Technik an.

6.4 Unterstützung des Auftraggebers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Pflichten bezüglich:

- Betroffenenrechte (Art. 15–22 DSGVO): Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch
- Meldepflichten bei Datenschutzverletzungen (Art. 33, 34 DSGVO)
- Datenschutz-Folgenabschätzungen (Art. 35, 36 DSGVO), soweit erforderlich

(2) Der Auftragnehmer stellt dem Auftraggeber hierzu geeignete technische und organisatorische Mittel zur Verfügung, insbesondere Export- und Löschfunktionen innerhalb der Plattform.

6.5 Meldung von Datenschutzverletzungen

(1) Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten **unverzüglich**, in der Regel innerhalb von **48 Stunden** nach Bekanntwerden (Art. 33 Abs. 2 DSGVO).

(2) Die Meldung enthält mindestens:

- Art der Verletzung
- Betroffene Datenkategorien und ungefähre Anzahl betroffener Personen
- Wahrscheinliche Folgen der Verletzung
- Ergriffene und vorgeschlagene Maßnahmen zur Behebung

---

§ 7 Unterauftragsverhältnisse (Sub-Auftragsverarbeiter)

7.1 Allgemeine Genehmigung

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine schriftliche Genehmigung, weitere Auftragsverarbeiter (Sub-Auftragsverarbeiter) hinzuzuziehen, sofern die Bedingungen gemäß Absatz 2 und 3 eingehalten werden (Art. 28 Abs. 2 DSGVO).

7.2 Informationspflicht und Widerspruchsrecht

(1) Der Auftragnehmer informiert den Auftraggeber **mindestens 14 Tage** vor einer beabsichtigten Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Sub-Auftragsverarbeitern in Textform (z.B. per E-Mail an die hinterlegte Kontaktadresse). Die Aufnahme eines **zusätzlichen** Mess-Standorts, der dem Auftraggeber lediglich zur Auswahl gestellt wird und ohne dessen Auswahl keine Daten erhält (§ 9 Abs. 2), ist keine Hinzuziehung im Sinne dieser Vorschrift; sie wird in der öffentlichen Subprozessorenliste und in den Release-Notes bekanntgegeben. Die Vorankündigungsfrist gilt uneingeschränkt für Sub-Auftragsverarbeiter, die der Auftraggeber bereits nutzt, sowie für deren Ersetzung und für die Verlagerung eines genutzten Standorts.

(2) Der Auftraggeber kann gegen die Hinzuziehung oder Ersetzung eines Sub-Auftragsverarbeiters innerhalb von **14 Tagen** nach Erhalt der Information aus datenschutzrechtlich begründetem Anlass Einspruch erheben. Erhebt der Auftraggeber innerhalb dieser Frist keinen Einspruch, gilt die Änderung als genehmigt.

(3) Im Falle eines begründeten Einspruchs wird der Auftragnehmer zunächst versuchen, die Dienstleistung ohne den betreffenden Sub-Auftragsverarbeiter oder mit einer gleichwertigen Alternative zu erbringen. Ist dies mit zumutbarem Aufwand nicht möglich, steht dem Auftraggeber ein Sonderkündigungsrecht hinsichtlich der betroffenen Leistung mit einer Frist von 30 Tagen zum Monatsende zu.

(4) Abweichend von Absatz 1 darf der Auftragnehmer einen Sub-Auftragsverarbeiter ohne Einhaltung der Vorankündigungsfrist unverzüglich hinzuziehen oder ersetzen, wenn dies aus dringenden Gründen erforderlich ist — insbesondere zur Aufrechterhaltung der Verfügbarkeit oder Sicherheit der Dienste, bei unvorhergesehenem Ausfall oder Wegfall eines bestehenden Sub-Auftragsverarbeiters oder aufgrund einer rechtlichen Verpflichtung. Der Auftragnehmer informiert den Auftraggeber in diesem Fall unverzüglich nach der Änderung in Textform. Das Einspruchs- und Sonderkündigungsrecht gemäß Absatz 2 und 3 bleibt unberührt und kann ab Zugang der nachträglichen Information ausgeübt werden.

7.3 Vertragliche Absicherung

(1) Der Auftragnehmer stellt sicher, dass mit jedem Sub-Auftragsverarbeiter ein Vertrag geschlossen wird, der mindestens die gleichen Datenschutzpflichten enthält wie dieser Vertrag (Art. 28 Abs. 4 DSGVO).

(2) Der Auftragnehmer haftet gegenüber dem Auftraggeber für die Einhaltung der Datenschutzpflichten durch seine Sub-Auftragsverarbeiter.

7.4 Aktuelle Liste der Sub-Auftragsverarbeiter

Die zum Zeitpunkt des Vertragsschlusses eingesetzten Sub-Auftragsverarbeiter sind in **Anlage 2 (Sub-Auftragsverarbeiter)** aufgeführt.

---

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, die Einhaltung der datenschutzrechtlichen Vorschriften und der Bestimmungen dieses Vertrages beim Auftragnehmer zu überprüfen (Art. 28 Abs. 3 lit. h DSGVO), vorrangig durch:

- Einholen von Auskünften des Auftragnehmers
- Einsichtnahme in Zertifizierungen, Auditberichte, Dokumentation oder Gutachten unabhängiger Prüfer

(2) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen.

(3) Vor-Ort-Inspektionen sind nur in begründeten Fällen zulässig, insbesondere wenn die Überprüfung durch Einsichtnahme in Dokumentation und Berichte nicht ausreicht. Sie bedürfen einer Vorankündigung von mindestens 14 Tagen, sind auf die üblichen Geschäftszeiten beschränkt und dürfen den Geschäftsbetrieb nicht unverhältnismäßig beeinträchtigen. Der Auftraggeber trägt die angemessenen Kosten der Inspektion, sofern keine Verstöße festgestellt werden.

§ 9 Drittlandtransfer

(1) Die Verarbeitung und persistente Speicherung personenbezogener Daten durch den Auftragnehmer und seine Sub-Auftragsverarbeiter erfolgt **innerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR)**, vorbehaltlich der in Absatz 5, 6 und 7 geregelten Ausnahmen.

(2) Die persistente Speicherung und Verarbeitung personenbezogener Daten durch Sub-Auftragsverarbeiter erfolgt in Rechenzentren innerhalb der EU/EWR (siehe Anlage 2), vorbehaltlich der in Absatz 6 und 7 geregelten transienten Verarbeitung durch Probe-Worker. Mess-Standorte (Probe-Worker) werden dem Auftraggeber lediglich zur Auswahl bereitgestellt. Eine Übermittlung von Check-Konfigurationen an einen Standort erfolgt erst, wenn der Auftraggeber diesen in den Plattform-Einstellungen auswählt; ein nicht ausgewählter Standort erhält keine Daten des Auftraggebers.

(3) Zum Zeitpunkt des Vertragsschlusses findet keine persistente Speicherung personenbezogener Daten in Drittländern (außerhalb EU/EWR) statt. Die transiente Verarbeitung an Drittland-Probe-Standorten ohne Angemessenheitsbeschluss erfolgt nur bei expliziter Aktivierung durch den Auftraggeber (Abs. 6); für Probe-Standorte in Drittländern mit EU-Angemessenheitsbeschluss gilt Abs. 7.

(4) Sollte eine Übermittlung in Drittländer künftig erforderlich werden, wird der Auftragnehmer den Auftraggeber vorab informieren und sicherstellen, dass geeignete Garantien gemäß Art. 44–49 DSGVO bestehen (z.B. Standardvertragsklauseln, Angemessenheitsbeschluss).

(5) Ausgenommen von den Absätzen 1–3 sind Datenübermittlungen, die der Auftraggeber durch Aktivierung von Drittanbieter-Integrationen (z.B. Slack, Discord, Microsoft Teams, Telegram, Custom Webhooks) eigenverantwortlich veranlasst. Diese Übermittlungen erfolgen auf dokumentierte Weisung des Auftraggebers. Die Verantwortung für die Einhaltung der Art. 44–49 DSGVO liegt in diesen Fällen ausschließlich beim Auftraggeber.

(6) Für die Durchführung von Verfügbarkeitsprüfungen (Monitoring-Checks) betreibt der Auftragnehmer Probe-Worker auch an Standorten in Drittländern ohne EU-Angemessenheitsbeschluss (siehe Anlage 2, Abschnitt „Monitoring-Probe-Infrastruktur"). Diese Standorte sind standardmäßig **nicht aktiviert**. Der Auftraggeber kann die Nutzung von Probe-Standorten außerhalb der EU/EWR explizit in den Plattform-Einstellungen aktivieren. Erst mit Aktivierung weist der Auftraggeber den Auftragnehmer an, Check-Konfigurationen an den betreffenden Standort zu übermitteln. Die Verarbeitung erfolgt transient: Ergebnisdaten werden unmittelbar nach der Prüfung verschlüsselt an die zentrale Infrastruktur (Hetzner, DE) übermittelt. Ist diese Übermittlung vorübergehend nicht möglich (z. B. Netzstörung), werden die Ergebnisse bis zur erfolgreichen Zustellung in einem lokalen, größenbegrenzten Zwischenspeicher (max. 100 MB) auf dem Probe-Server vorgehalten und danach gelöscht. Eine darüber hinausgehende dauerhafte Speicherung personenbezogener Daten findet auf den Probe-Servern nicht statt. Die dauerhafte Speicherung aller Ergebnisdaten erfolgt ausschließlich innerhalb der EU/EWR. Der Auftragnehmer stellt sicher, dass für die Verarbeitung an Standorten außerhalb der EU/EWR geeignete Garantien gem. Art. 44–49 DSGVO bestehen (vorrangig: EU-Standardvertragsklauseln (SCCs) gem. Art. 46 Abs. 2 lit. c DSGVO; ergänzend das EU-U.S. Data Privacy Framework, soweit der jeweilige Empfänger DPF-zertifiziert ist).

(7) Betreibt der Auftragnehmer Probe-Worker an Standorten in Drittländern, für die ein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 DSGVO besteht (derzeit: Schweiz, siehe Anlage 2), so ist die Übermittlung ohne zusätzliche Garantien zulässig. Diese Standorte werden wie Standorte innerhalb der EU/EWR behandelt und stehen standardmäßig zur Verfügung. Die Verarbeitung erfolgt transient: Ergebnisdaten werden unmittelbar nach der Prüfung verschlüsselt an die zentrale Infrastruktur (Hetzner, DE) übermittelt. Ist diese Übermittlung vorübergehend nicht möglich (z. B. Netzstörung), werden die Ergebnisse bis zur erfolgreichen Zustellung in einem lokalen, größenbegrenzten Zwischenspeicher (max. 100 MB) auf dem Probe-Server vorgehalten und danach gelöscht. Eine darüber hinausgehende dauerhafte Speicherung personenbezogener Daten findet auf den Probe-Servern nicht statt.

(8) Für persönliche Benachrichtigungskanäle, bei denen der Auftragnehmer selbst Vertragspartner des Anbieters ist (derzeit: WhatsApp und Pushover, siehe Anlage 2, Abschnitt „Messenger- und Push-Benachrichtigungen"), gilt: Eine Übermittlung an den jeweiligen Anbieter findet ausschließlich statt, wenn eine betroffene Person diesen Kontaktweg in ihren persönlichen Benachrichtigungseinstellungen selbst hinterlegt und bestätigt hat. Ohne bestätigten Kontaktweg werden keine Daten übermittelt; ein Widerruf setzt die Bestätigung zurück und beendet jede weitere Übermittlung. Der Auftraggeber kann diese Kanäle darüber hinaus für seine gesamte Organisation deaktivieren. Abweichend von Absatz 5 bleibt die Rolle des Auftragnehmers als Auftragsverarbeiter unberührt, da der Auftragnehmer den Anbieter selbst beauftragt; die Verantwortung nach Art. 44–49 DSGVO geht insoweit nicht auf den Auftraggeber über. Anbieter, die außerhalb der EU/EWR verarbeiten, sind in Anlage 2 entsprechend gekennzeichnet.

---

§ 10 Löschung und Rückgabe personenbezogener Daten

(1) Nach Beendigung des Hauptvertrages löscht der Auftragnehmer sämtliche personenbezogenen Daten des Auftraggebers, sofern nicht eine gesetzliche Aufbewahrungspflicht besteht (Art. 28 Abs. 3 lit. g DSGVO).

(2) Der Auftraggeber hat das Recht, vor der Löschung eine **Rückgabe der Daten** in einem gängigen, maschinenlesbaren Format (z.B. JSON, CSV) zu verlangen. Der Auftragnehmer stellt hierfür Exportfunktionen innerhalb der Plattform bereit.

(3) Die Löschung erfolgt innerhalb von **30 Tagen** nach Vertragsende, sofern der Auftraggeber keinen Export angefordert hat. Bei Exportanforderung beginnt die 30-Tage-Frist nach Bereitstellung des Exports.

(4) Daten, die aufgrund gesetzlicher Aufbewahrungspflichten (z.B. steuer- und handelsrechtliche Fristen, § 147 AO, § 257 HGB) nicht gelöscht werden können, werden gesperrt und nach Ablauf der gesetzlichen Frist gelöscht. Der Auftragnehmer informiert den Auftraggeber über Art und Umfang der betroffenen Daten.

(5) Aggregierte, anonymisierte Metriken sind von der Löschpflicht ausgenommen. Die Anonymisierung erfolgt irreversibel durch Aggregation auf Organisations- und Serviceebene, wobei kein Rückschluss auf einzelne betroffene Personen möglich ist (z.B. Uptime-Prozentsätze, durchschnittliche Antwortzeiten).

(6) Der Auftragnehmer bestätigt die vollständige Löschung auf Anfrage in Textform.

---

§ 11 Haftung

(1) Die Haftung der Parteien richtet sich nach Art. 82 DSGVO.

(2) Der Auftragnehmer haftet gegenüber dem Auftraggeber für Schäden, die durch eine nicht den Bestimmungen der DSGVO oder dieses Vertrages entsprechende Verarbeitung entstehen.

(3) Der Auftragnehmer haftet ferner für das Verschulden seiner Sub-Auftragsverarbeiter wie für eigenes Verschulden.

(4) Weitergehende Haftungsregelungen, insbesondere Haftungsbegrenzungen für mittelbare Schäden und Folgeschäden, richten sich nach dem Hauptvertrag (AGB / Nutzungsbedingungen), soweit diese nicht im Widerspruch zu Art. 82 DSGVO stehen.

§ 12 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform (§ 126b BGB). Dies gilt auch für die Aufhebung dieses Formerfordernisses. Die elektronische Form ist gem. Art. 28 Abs. 9 DSGVO ausreichend.

(2) Sollte eine Bestimmung dieses Vertrages unwirksam oder undurchführbar sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die unwirksame Bestimmung ist durch eine wirksame Bestimmung zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.

(3) Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland. Gerichtsstand ist Husum, soweit gesetzlich zulässig.

(4) Dieser Vertrag ist Bestandteil des Hauptvertrages (AGB / Nutzungsbedingungen) und tritt mit Akzeptanz der AGB in Kraft.

Unterzeichnung

Für den Auftragnehmer (Auftragsverarbeiter):

(Muster, im Vertragsexemplar unterschrieben)

René Roscher, Inhaber — LIVCK.cloud Schwesing, den 18. November 2026

Für den Auftraggeber (Verantwortlicher):

Der Auftraggeber schließt diesen Vertrag durch elektronische Bestätigung in der LIVCK-Plattform ab (Art. 28 Abs. 9 DSGVO, Textform gem. § 126b BGB). Name, Funktion und Organisation der weisungsberechtigten Person, Zeitpunkt sowie Versionsstand der Annahme werden elektronisch dokumentiert und im abgeschlossenen Vertragsexemplar ausgewiesen.

(Muster. Abgeschlossen wird der Vertrag elektronisch in der Konsole unter Einstellungen › Abrechnung › AVV. Dort werden die abschließende Person, deren Funktion, der Zeitpunkt und der Versionsstand ausgewiesen.)

Anlagen

- **Anlage 1:** Technisch-Organisatorische Maßnahmen (TOMs)
- **Anlage 2:** Sub-Auftragsverarbeiter
- **Anlage 3:** Weisungsberechtigte Personen und Ansprechpartner

Anlage 1: Technisch-Organisatorische Maßnahmen (TOMs)

gemäß Art. 32 DSGVO

Der Auftragnehmer hat folgende technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten implementiert:

---

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren:

- Die zentrale Plattform (Anwendung, Datenbanken, Zwischenspeicher, Metrik-Speicher) wird in ISO 27001-zertifizierten Rechenzentren der Hetzner Online GmbH in Deutschland betrieben; Hetzner verfügt über ein BSI-C5-Testat (Typ 2)
- Objektspeicher und Datenbank-Backups liegen bei der STACKIT GmbH & Co. KG in Deutschland, die ebenfalls über ein BSI-C5-Testat (Typ 2) verfügt
- Physischer Zugang zu den Rechenzentren ist durch mehrstufige Zugangskontrollen gesichert (Biometrie, Chipkarte, Schleuse)
- Zutrittsprotokollierung durch den Rechenzentrumsbetreiber
- Keine eigenen physischen Server – ausschließlich Cloud-Infrastruktur bei zertifizierten Anbietern

1.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden:

- Authentifizierung über individuelle Benutzerkonten mit E-Mail und Passwort
- Passwörter werden ausschließlich als Hashwert gespeichert; zum Einsatz kommt ein anerkanntes, saltbasiertes Hash-Verfahren nach Stand der Technik
- Unterstützung und Förderung von Zwei-Faktor-Authentifizierung (TOTP)
- 2FA-Secrets werden anwendungsseitig mit einem anerkannten Verschlüsselungsverfahren nach Stand der Technik verschlüsselt gespeichert
- Rate Limiting bei Login-Versuchen zur Eindämmung von Brute-Force-Angriffen
- Session-Timeout nach konfigurierbarer Inaktivitätszeit
- API-Tokens werden ausschließlich gehasht gespeichert; der Rohtoken wird nur einmalig bei Erstellung angezeigt

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass Nutzer nur auf die ihnen zugewiesenen Daten zugreifen:

- Rollenbasiertes Zugriffskonzept (RBAC) auf Organisationsebene
- Fein granulierte Berechtigungen über klar definierte Berechtigungsrollen
- Organisationsinhaber hat stets volle Berechtigung (kann nicht eingeschränkt werden)
- Jeder Datenzugriff wird gegen die Organisationszugehörigkeit geprüft (Tenant Isolation)
- API-Tokens mit eingeschränkbaren Berechtigungen und optionalem Ablaufdatum
- Alle Autorisierungsprüfungen erfolgen serverseitig (Frontend-Prüfungen dienen nur der UX)

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass Daten verschiedener Auftraggeber getrennt verarbeitet werden:

- Logische Mandantentrennung auf Organisationsebene (Multi-Tenancy)
- Jede Datenbankabfrage wird durch den Organisationskontext gefiltert
- Zwischenspeicher (Cache) mit organisationsspezifischer Segmentierung (kein organisationsübergreifender Zugriff)
- Metrik-/Zeitreihendaten werden pro Service und Organisation getrennt gespeichert
- Hochgeladene Dateien werden pro Organisation getrennt im Objektspeicher abgelegt

---

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Maßnahmen, die verhindern, dass Daten bei der Übertragung unbefugt gelesen oder verändert werden:

- Sämtliche externe Kommunikation ausschließlich über TLS 1.2+ verschlüsselt (HTTPS)
- Interne Kommunikation zwischen den Diensten der Plattform erfolgt über verschlüsselte Verbindungen
- E-Mail-Versand über TLS-verschlüsselte API-Verbindungen zu den Mail-Providern
- SMS-Versand über TLS-verschlüsselte API-Verbindungen
- Webhook-Payloads werden mit HMAC-SHA256 signiert (`X-Livck-Signature` Header)
- Verbindungen zu kundeneigenen Domains (Custom Domains) werden automatisch TLS-verschlüsselt
- Datenbank-Verbindungen innerhalb der Infrastruktur über verschlüsselte Kanäle

2.2 Verschlüsselung ruhender Daten (Encryption at Rest)

Maßnahmen zum Schutz gespeicherter Daten:

- Sensible Anwendungsdaten (2FA-Secrets, Webhook-Secrets) werden anwendungsseitig mit einem anerkannten Verschlüsselungsverfahren nach Stand der Technik verschlüsselt gespeichert
- Zugangsdaten für Prüfungen (Werte eigener HTTP-Header, Token, Passwörter und API-Schlüssel der Authentifizierung, Client-Zertifikate mit privatem Schlüssel sowie CA-Zertifikate) werden anwendungsseitig verschlüsselt gespeichert und verschlüsselt an die Probe-Worker übermittelt. Entschlüsselt werden sie erst unmittelbar vor der jeweiligen Prüfung im Arbeitsspeicher; auf den Probe-Servern werden sie nicht gespeichert
- Der Objektspeicher (STACKIT, Deutschland) und seine Kopie (OVH, Deutschland) verschlüsseln alle gespeicherten Objekte serverseitig mit AES-256
- Datenbank-Backups werden ausschließlich über TLS-verschlüsselte Verbindungen übertragen und verschlüsselt im Objektspeicher (STACKIT, Deutschland) sowie in dessen Kopie (OVH, Deutschland) gespeichert
- Der Zugang zur Serverinfrastruktur ist durch SSH-Key-Authentifizierung (keine Passwort-Logins), Firewall-Regeln und die physischen Sicherheitsmaßnahmen der ISO 27001-zertifizierten Rechenzentren geschützt

2.3 Eingabekontrolle

Maßnahmen, die nachträglich die Überprüfung ermöglichen, ob und von wem Daten eingegeben, verändert oder entfernt worden sind:

- Umfassendes Audit-Log: Alle Änderungen an kritischen Entitäten werden protokolliert (Wer, Was, Wann, Vorher/Nachher-Werte)
- Audit-Log-Aufbewahrung je nach Tarif (30 Tage bis 2 Jahre)
- Session-Protokollierung mit IP-Adresse und User-Agent
- API-Token-Nutzungsprotokollierung (letzte Nutzung, IP)
- Benachrichtigungs-Zustellprotokolle mit vollständigem Delivery-Status

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DSGVO)

3.1 Verfügbarkeitskontrolle

Maßnahmen zum Schutz gegen zufällige oder vorsätzliche Zerstörung oder Verlust:

- Container-orchestrierte Infrastruktur mit automatischem Neustart ausgefallener Komponenten und redundant ausgelegten Instanzen
- Automatisierte, verschlüsselte Backups der Datenbanken im Objektspeicher (STACKIT, DE) mit redundanter Kopie (OVH, DE)
- Persistente Speicherung der Zwischenspeicher-Daten zur Wiederherstellung nach Neustarts
- Metriken-Speicher mit automatischer Datenaggregation und fristbasierter Archivierung sowie einer laufend aktualisierten Ausfallkopie in einem zweiten Rechenzentrum (OVH, Frankreich)
- Monitoring der eigenen Infrastruktur mit automatischer Alarmierung
- DDoS-Schutz auf Netzwerkebene durch den Hosting-Provider (Hetzner)

3.2 Rasche Wiederherstellbarkeit

Maßnahmen zur raschen Wiederherstellung nach einem Zwischenfall:

- Automatisiert bereitgestellte Infrastruktur ermöglicht eine rasche Wiederherstellung der Dienste
- Wiederherstellung der Datenbanken aus verschlüsselten, automatisierten Backups (STACKIT + OVH)
- Geografisch getrennte Backup-Speicherung in zwei verschiedenen Rechenzentren innerhalb Deutschlands (STACKIT + OVH)

---

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

4.1 Datenschutzmanagement

- Regelmäßige Überprüfung und Aktualisierung der technisch-organisatorischen Maßnahmen
- Dokumentierte Prozesse für Betroffenenrechte (Auskunft, Löschung, Export)
- Incident-Response-Prozess für Datenschutzverletzungen mit definierter Meldekette
- Sensibilisierung und Verpflichtung aller mit der Datenverarbeitung betrauten Personen auf das Datengeheimnis und die DSGVO-Anforderungen
- Bei Einsatz weiterer Mitarbeiter oder Auftragnehmer: dokumentierte Einweisung in die datenschutzrelevanten Prozesse vor Aufnahme der Tätigkeit

4.2 Auftragskontrolle

- Sorgfältige Auswahl von Sub-Auftragsverarbeitern nach Datenschutzkriterien
- Vertragliche Absicherung aller Sub-Auftragsverarbeiter gemäß Art. 28 DSGVO
- Regelmäßige Überprüfung der Sub-Auftragsverarbeiter

Anlage 2: Sub-Auftragsverarbeiter

Stand: 18. November 2026

Der Auftragnehmer setzt derzeit folgende Sub-Auftragsverarbeiter ein:

Infrastruktur & Hosting

Unternehmen	Standort (Sitz)	Standort (Daten)	Zweck der Verarbeitung	Betroffene Daten
Hetzner Online GmbH	Gunzenhausen, Deutschland	Rechenzentren in Deutschland (Falkenstein, Nürnberg)	Cloud-Hosting der gesamten Plattform-Infrastruktur (Kubernetes-Cluster, Datenbanken, Cache, Message Queue, Metrik-Speicher)	Alle personenbezogenen Daten gemäß § 3
STACKIT GmbH & Co. KG	Neckarsulm, Deutschland	Rechenzentren in Deutschland; CDN: Auslieferungsknoten in der EU	S3-kompatibler Objektspeicher (public/private/artifacts) für hochgeladene Dateien (Logos, Profilbilder, Exporte, Rechnungen, Check-Artefakte, Statuspage-Assets) sowie verschlüsselte Datenbank-Backups; alle Objekte serverseitig mit AES-256 verschlüsselt. Außerdem primäres Auslieferungsnetz (STACKIT CDN) für öffentlich abrufbare Dateien; STACKIT setzt dafür die BUNNYWAY d.o.o. (Ljubljana, Slowenien) als weiteren Unterauftragnehmer ein. Zwischenspeicherung zur Auslieferung, kein Zugriff auf nicht-öffentliche Speicherbereiche.	Hochgeladene Dateien, Exportdaten, Rechnungsdokumente, Check-Artefakte (können HTTP-Response-Daten einschließlich Headers und Body enthalten), verschlüsselte PostgreSQL- und Metrik-Backups; über das CDN nur öffentlich abrufbare Dateien (Statuspage-Assets, Logos, Profilbilder)
OVH SAS (OVHcloud)	Roubaix, Frankreich	Deutschland (Limburg) für den Objektspeicher; Frankreich (Gravelines) für die Ausfallkopie des Metrik-Speichers	Zweiter Objektspeicher als Ausweichkopie des primären Speichers (STACKIT). Der Abgleich erfolgt fortlaufend zwischen den Speicherbereichen des Auftragnehmers und umfasst denselben Inhalt; alle Objekte serverseitig mit AES-256 verschlüsselt. Außerdem eine laufend aktualisierte Ausfallkopie des Metrik-Speichers (ClickHouse) auf einem eigenen Server.	Objektspeicher: dieselben Kategorien wie beim primären Objektspeicher (hochgeladene Dateien, Exportdaten, Rechnungsdokumente, Check-Artefakte, verschlüsselte PostgreSQL- und Metrik-Backups). Metrik-Speicher: technische Messdaten der Prüfungen (Service-IDs, Antwortzeiten, Statuscodes, Fehlermeldungen, Monitoring-Ziel-Adressen)
G-Core Labs S.A. (Gcore CDN)	Contern, Luxemburg	Auslieferungsknoten des Anbieters	Ausweich-Auslieferungsnetz für öffentlich abrufbare Dateien, wenn das primäre Auslieferungsnetz (STACKIT CDN) nicht verfügbar ist. Zwischenspeicherung zur Auslieferung; keine dauerhafte Datenhaltung und kein Zugriff auf nicht-öffentliche Speicherbereiche.	Öffentlich abrufbare Dateien: Statuspage-Assets sowie hochgeladene Bilder (Logos, Profilbilder)

E-Mail-Versand

Unternehmen	Standort (Sitz)	Standort (Daten)	Zweck der Verarbeitung	Betroffene Daten
Scaleway SAS (Transactional Email)	Paris, Frankreich	Paris, Frankreich	Primärer Versand von transaktionalen E-Mails und Incident-Alerts	Empfänger-E-Mail-Adresse, E-Mail-Betreff, E-Mail-Inhalt
MINDBAZ SAS (Sweego)	Lille, Frankreich	Frankreich (OVH, Roubaix)	Fallback-Versand von transaktionalen E-Mails und Incident-Alerts	Empfänger-E-Mail-Adresse, E-Mail-Betreff, E-Mail-Inhalt

SMS- und Voice-Versand

Soweit die reine Nachrichtenübermittlung über öffentliche Telekommunikationsnetze als Telekommunikationsdienst gem. § 2 Nr. 61 TKG einzuordnen ist, unterliegt dieser Aspekt dem TKG/TDDDG (Art. 95 DSGVO). Die darüber hinausgehende Verarbeitung personenbezogener Daten durch die nachfolgenden Anbieter — insbesondere Zustellprotokolle, Metadaten, Logbuch und Adressbuch — unterliegt der DSGVO und ist durch diesen AVV erfasst.

Unternehmen	Standort (Sitz)	Standort (Daten)	Zweck der Verarbeitung	Betroffene Daten
seven communications GmbH & Co. KG (Seven.io)	Kiel, Deutschland	Deutschland (Hetzner Online AG)	Primärer Versand von SMS-Benachrichtigungen für Incident-Alerts. BNetzA-registrierter TK-Anbieter. Sub-Processor-Liste: https://www.seven.io/de/subunternehmer/	Empfänger-Telefonnummer, Nachrichteninhalt, Zustellstatus
LOX24 GmbH	Berlin, Deutschland	Deutschland (Hetzner RZ Falkenstein/Nürnberg), Backups: EU (AWS EMEA SARL, Luxemburg)	Fallback-Versand von SMS-Benachrichtigungen und Voice/Text-to-Speech-Anrufen für Incident-Alerts. BNetzA-registrierter TK-Anbieter gem. § 3 TKG.	Empfänger-Telefonnummer, Nachrichteninhalt, Zustellstatus

Hinweis zu LOX24-Sub-Auftragsverarbeitern: LOX24 setzt ihrerseits Hetzner Online GmbH (Hosting, DE) und AWS EMEA SARL (Backups, Luxemburg/EU) als Sub-Auftragsverarbeiter ein. Alle Daten verbleiben innerhalb der EU.

Messenger- und Push-Benachrichtigungen

Die nachfolgenden Anbieter werden **ausschließlich dann** eingesetzt, wenn eine betroffene Person den jeweiligen Kontaktweg in ihren persönlichen Benachrichtigungseinstellungen selbst hinterlegt und bestätigt hat (§ 9 Abs. 8). Es handelt sich um persönliche Kontaktwege einzelner Nutzer, nicht um eine organisationsweite Voreinstellung; standardmäßig ist für neue Nutzer allein der Kontaktweg E-Mail eingerichtet. Ohne bestätigten Kontaktweg werden keine Daten an diese Anbieter übermittelt.

Unternehmen	Standort (Sitz)	Standort (Daten)	Zweck der Verarbeitung	Betroffene Daten
WhatsApp Ireland Limited	Dublin, Irland	Irland/EU sowie USA (Meta-Konzern)	Zustellung von Incident-Alerts und Statusmeldungen an eine vom Nutzer bestätigte WhatsApp-Rufnummer. Nur bestätigte Kontaktwege werden beliefert.	Empfänger-Rufnummer, Schweregrad, Servicename, Titel des Vorfalls, Bestätigungscode
Pushover, LLC	USA	USA	Zustellung von Incident-Alerts und Statusmeldungen an die Pushover-App eines Nutzers. Nur bestätigte Kontaktwege werden beliefert.	Pushover-Benutzerschlüssel, Schweregrad, Servicename, Titel des Vorfalls, Bestätigungslink

Hinweis zur Bestätigung: Die Bestätigung eines Kontaktwegs erfolgt durch Zustellung eines Codes über den jeweiligen Anbieter. Dieser Bestätigungsvorgang ist damit die erste Übermittlung an den Anbieter. Ein Widerruf durch die betroffene Person setzt die Bestätigung zurück und beendet jede weitere Übermittlung.

Hinweis zur Drittlandsverarbeitung: Pushover, LLC verarbeitet auf Servern in den USA. Der Auftraggeber kann diesen Kanal für seine Organisation vollständig deaktivieren; die übrigen Benachrichtigungskanäle bleiben davon unberührt.

Monitoring-Probe-Infrastruktur

Die Monitoring-Probe-Worker führen Verfügbarkeitsprüfungen (HTTP, TCP, DNS, ICMP, SSL) an den vom Auftraggeber konfigurierten Monitoring-Zielen durch. Die Verarbeitung erfolgt transient: Ergebnisdaten werden unmittelbar nach der Prüfung verschlüsselt an die zentrale Infrastruktur (Hetzner, DE) übermittelt. Ist diese Übermittlung vorübergehend nicht möglich (z. B. Netzstörung), werden die Ergebnisse bis zur erfolgreichen Zustellung in einem lokalen, größenbegrenzten Zwischenspeicher (max. 100 MB) auf dem Probe-Server vorgehalten und danach gelöscht. Eine darüber hinausgehende dauerhafte Speicherung personenbezogener Daten findet auf den Probe-Servern nicht statt. Die Ergebnisdaten werden verschlüsselt an die zentrale Infrastruktur (Hetzner, DE) übermittelt.

EU/EWR-Standorte (standardmäßig verfügbar):

Unternehmen	Standort (Sitz)	Standort (Daten)	Probe-Standort
Dataforest GmbH	Kriftel, Deutschland	Deutschland (maincubes FRA01, Frankfurt)	Frankfurt (DE)
Hetzner Online GmbH	Gunzenhausen, Deutschland	Deutschland	Nürnberg (DE)
EmeraldHost UG (haftungsbeschr.)	Köln, Deutschland	Deutschland	Köln (DE)
WindCloud 4.0 GmbH	Enge-Sande, Schleswig-Holstein, Deutschland	Deutschland (GreenTEC Campus, Enge-Sande)	Enge-Sande / Nordfriesland (DE)
netcup GmbH	Karlsruhe, Deutschland	Österreich (Wien)	Wien (AT)
OVHcloud (OVH SAS)	Roubaix, Frankreich	Polen (Warschau)	Warschau (PL)
UpCloud Oy	Aleksanterinkatu 15 B, 00100 Helsinki, Finnland	Finnland (Helsinki, Rechenzentrum HEL2)	Helsinki (FI)

Standorte in Drittländern mit EU-Angemessenheitsbeschluss (standardmäßig verfügbar):

Für diese Standorte besteht ein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 DSGVO; eine Übermittlung ist ohne zusätzliche Garantien zulässig und wird wie eine Verarbeitung innerhalb der EU/EWR behandelt (siehe § 9 Abs. 7).

Unternehmen	Standort (Sitz)	Standort (Daten)	Probe-Standort	Garantie
Infomaniak Network SA	Genf (Acacias), Schweiz	Genf, Schweiz (eigenes Rechenzentrum, Plan-les-Ouates)	Genf (CH)	EU-Angemessenheitsbeschluss für die Schweiz (Art. 45 DSGVO; Kommissionsbeschluss 2000/518/EG, durch die EU-Kommission am 15.01.2024 bestätigt); ergänzend gilt das revidierte Schweizer Datenschutzgesetz (revDSG)

Drittland-Standorte ohne Angemessenheitsbeschluss (nur bei expliziter Aktivierung durch den Auftraggeber, siehe § 9 Abs. 6):

Unternehmen	Standort (Sitz)	Standort (Daten)	Probe-Standort	Garantien
Contabo GmbH	München, Deutschland	Carlstadt, New Jersey, USA	New York (US)	EU-Standardvertragsklauseln (SCC, Modul 3 — Auftragsverarbeiter an Auftragsverarbeiter) gem. Art. 46 Abs. 2 lit. c DSGVO als Bestandteil des mit Contabo geschlossenen Auftragsverarbeitungsvertrags

Hinweis zu Contabo-Unterauftragnehmern: Vertragspartner des Auftragnehmers ist die Contabo GmbH (München, Deutschland). Den Betrieb des Rechenzentrums am US-Standort übernimmt gemäß Anlage 3 des mit Contabo geschlossenen Auftragsverarbeitungsvertrags die Contabo Inc., 711 N Tucker Blvd. STE 420, 63101 St. Louis, Missouri, USA.

Probe-Worker erhalten ausschließlich Check-Konfigurationen für diejenigen Prüfungen, die der Auftraggeber dem jeweiligen Standort zugewiesen hat. Auth-Credentials für authentifizierte Checks werden nur an den betreffenden Probe-Standort übermittelt und nicht persistiert.

Hinweis zu weiteren Diensten

Folgende Dienste werden **nicht** als Sub-Auftragsverarbeiter eingestuft, da sie entweder keine personenbezogenen Daten verarbeiten, als eigenständige Verantwortliche agieren oder vom Auftraggeber selbst konfiguriert werden:

Dienst	Begründung
Mollie B.V. (Amsterdam, NL)	Eigenständig Verantwortlicher gem. Art. 4 Nr. 7 DSGVO — Mollie verarbeitet Zahlungsdaten nicht im Auftrag des Auftragnehmers, sondern als unabhängiger Verantwortlicher auf Basis eigener vertraglicher und regulatorischer Pflichten (PSD2, Zahlungsdiensteaufsichtsgesetz). Der Auftragnehmer übermittelt auf Weisung des Auftraggebers (§ 3.5) Name und E-Mail-Adresse an Mollie zur Kundenerstellung. Siehe Mollie GDPR-Dokumentation.
Let's Encrypt / ZeroSSL	Certificate Authorities – verarbeiten nur Domainnamen (keine personenbezogenen Daten) im Rahmen der TLS-Zertifikatsausstellung
Cloudflare (USA), Gcore (Luxemburg), ClouDNS (Bulgarien)	DNS-Anbieter (autoritative Nameserver) für die eigenen Domains des Auftragnehmers (Cloudflare) sowie für Statuspage-/Custom-Domain-Verkehr (Gcore, ClouDNS). Verarbeiten ausschließlich technische DNS-Anfragen (Domainname sowie i. d. R. die IP des anfragenden Resolvers, nicht des Endnutzers) – **keine personenbezogenen Anwendungsdaten** (Art. 28 nicht einschlägig); aus Transparenzgründen aufgeführt. Über diese Anbieter fließen weder Inhalte noch Anwendungs-Traffic. Die Einstufung als „kein Auftragsverarbeiter" gilt für Cloudflare ausdrücklich nur, solange Cloudflare ausschließlich als autoritativer DNS-Dienst (ohne Proxy-/CDN-Funktion) eingesetzt wird; bei Aktivierung einer Proxy-/CDN-Funktion wird diese Einstufung neu bewertet und Cloudflare ggf. als Sub-Auftragsverarbeiter aufgenommen. Cloudflare (USA): Drittland – etwaige Übermittlung erfolgt vorrangig auf Basis der EU-Standardvertragsklauseln (SCCs); ergänzend das EU-U.S. Data Privacy Framework, soweit Cloudflare DPF-zertifiziert ist.
Slack, Discord, Microsoft Teams, Telegram	Vom Auftraggeber selbst konfigurierte Integrationen – der Auftraggeber entscheidet eigenverantwortlich über die Nutzung und Datenübermittlung an diese Dienste

Alle Sub-Auftragsverarbeiter verarbeiten personenbezogene Daten innerhalb der EU/EWR oder in einem Drittland mit EU-Angemessenheitsbeschluss (Schweiz). Ausgenommen sind nur Verarbeitungen, die der Auftraggeber oder einzelne Nutzer selbst aktivieren: der Probe-Standort New York sowie die persönlichen Kontaktwege WhatsApp und Pushover.

Der Probe-Standort Genf (Schweiz, Infomaniak Network SA) steht standardmäßig zur Verfügung; die Übermittlung erfolgt auf Grundlage des EU-Angemessenheitsbeschlusses für die Schweiz (Art. 45 DSGVO) und wird wie eine Verarbeitung innerhalb der EU/EWR behandelt (§ 9 Abs. 7). Der Probe-Standort New York (USA) verarbeitet Daten nur bei expliziter Aktivierung durch den Auftraggeber, transient im Sinne von § 9 Abs. 6 (unmittelbare verschlüsselte Übermittlung an die zentrale Infrastruktur, lokaler Zwischenspeicher nur bis zur Zustellung) und unter den dort genannten Garantien.

Anlage 3: Ansprechpartner

Beim Auftragnehmer (LIVCK Cloud)

Funktion	Name	Kontakt
Inhaber / Geschäftsleitung	René Roscher	r.roscher@livck.com
Datenschutz-Ansprechpartner	René Roscher	datenschutz@livck.com
Technischer Ansprechpartner	René Roscher	support@livck.com

Beim Auftraggeber

Die weisungsberechtigten Personen des Auftraggebers werden bei Vertragsabschluss (Registrierung) festgelegt. Weisungsberechtigt sind:

- Der Inhaber der Organisation (Owner)
- Von diesem benannte Administratoren

Dieser Auftragsverarbeitungsvertrag wurde zuletzt aktualisiert am: 18. November 2026