

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

Stand Oktober 2026 · Version 2026-10 · LH Printing, Inhaber Lars Hölker, Philippenkuhle 5, 52538 Gangelt

Entwurf – vor Veröffentlichung prüfen. Markierte Stellen müssen noch ausgefüllt werden.

Version 2026-10 · Stand Oktober 2026 · Auftragsverarbeiter: Lars Hölker, LH Printing, Philippenkuhle 5, 52538 Gangelt

Diese Anlage beschreibt die Maßnahmen, mit denen LH Printing die Sicherheit der Verarbeitung bei Revisio gewährleistet. Sie gliedert sich in Maßnahmen der Software (in jeder Installation wirksam), Maßnahmen des Betriebs und Maßnahmen des Rechenzentrums. Die Maßnahmen werden regelmäßig überprüft und dem Stand der Technik angepasst.

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

1.1 Zutrittskontrolle (Rechenzentrum)

Sämtliche Systeme von Revisio (Anwendung, Datenbank, Dateiablage, Mailserver und externe Kopie der Datensicherung) werden ausschließlich bei der Hetzner Online GmbH in deren Rechenzentren in Deutschland betrieben (Anlage 2). Mit Hetzner besteht ein Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO. Hetzner sichert den physischen Zutritt nach seinen technischen und organisatorischen Maßnahmen (Anlage zum AVV von Hetzner), insbesondere:

- elektronische Zutrittskontrolle mit Protokollierung, Zutritt nur für berechtigtes Personal,
- Videoüberwachung, Einbruchmeldetechnik und Sicherheitspersonal rund um die Uhr,
- abgeschlossene Serverräume bzw. -schränke,
- Informationssicherheits-Managementsystem nach ISO/IEC 27001 (zertifiziert für die Rechenzentren von Hetzner).

LH Printing selbst unterhält keine Räume, in denen Kundendaten gespeichert werden. Arbeitsgeräte des Inhabers sind durch Gerätesperre und Festplattenverschlüsselung geschützt; Kundendaten werden auf ihnen nicht dauerhaft gespeichert.

1.2 Zugangskontrolle (Systeme)

Anwendung Revisio

- Anmeldung mit persönlichem Konto; Passwörter mit bcrypt gehasht, mindestens 10 Zeichen mit Buchstaben und Ziffern; Einladung per E-Mail statt Passwortvergabe durch Dritte.
- **Zwei-Faktor-Anmeldung (TOTP)** für alle Nutzer und Kundenportal-Zugänge verfügbar; die Organisation kann sie für Administratoren verpflichtend machen. Abschalten nur mit aktuellem Passwort.
- Begrenzung von Anmeldeversuchen (5 je Minute je Adresse und IP, 30 je Minute je IP) mit Protokollierung von Sperren.
- E-Mail-Benachrichtigung bei Anmeldung von einem unbekannten Gerät; Übersicht bekannter Geräte und aktiver Sitzungen; Passwortänderung beendet alle anderen Sitzungen.
- Erneute Passwortbestätigung vor folgenreichen Aktionen (u. a. Benutzer- und Rollenänderungen, Datenauskunft, Anonymisierung, Löschfristen), gültig höchstens drei Stunden.
- Sitzungscookies HttpOnly, Secure, SameSite=Lax; begrenzte Sitzungsdauer.

- **Techniker-App:** Gerätetoken je Gerät mit begrenzter Laufzeit; Geräte können zentral gesperrt und aus der Ferne gelöscht werden.

Betreiberzugang

- Der Betreiberbereich von LH Printing hat eine eigene Anmeldung, getrennt von den Konten der Kunden; Zwei-Faktor-Anmeldung ist verpflichtend. Handlungen im Betreiberbereich werden protokolliert.
- Administrativer Zugang zu den Servern nur für den Inhaber bzw. ausdrücklich berechtigte Personen, ausschließlich über verschlüsselte Verbindungen per SSH mit Schlüssel; die Anmeldung mit Passwort ist abgeschaltet.
- Das Kundenkonto bei Hetzner (Verwaltung von Servern, Netz, Speicher und Datensicherung) ist mit Zwei-Faktor-Anmeldung geschützt.
- Firewall: von außen erreichbar sind nur HTTPS (und HTTP zur Weiterleitung) sowie der administrative Zugang; Datenbank, Cache und interne Dienste sind nur im internen Netz der Container erreichbar.

1.3 Zugriffskontrolle (Berechtigungen)

- Rollen- und Rechtekonzept je Organisation (u. a. Administration, Disposition, Technik, Nur lesen, Kundenportal) mit einzeln vergebaren Rechten; Technikerinnen und Techniker sehen standardmäßig nur ihnen zugewiesene Aufträge; Kundenportal-Zugänge sehen nur Daten ihres Kunden.
- Dateien werden nur über geprüfte Abrufe mit Rechteprüfung ausgeliefert (keine öffentlichen Dateipfade); in der App über zeitlich begrenzte, signierte Adressen zusätzlich mit Gerätetoken.
- Support-Zugriffe auf Inhalte einer Organisation nur nach Freigabe durch deren Administration, zeitlich begrenzt und protokolliert (AVV § 13).

1.4 Trennungskontrolle (Mandantentrennung)

- Jeder Datensatz ist einer Organisation zugeordnet; jede Datenbankabfrage ist auf die Organisation des angemeldeten Benutzers beschränkt. Ohne gesetzten Mandanten liefert eine Abfrage keine Daten; Verweise auf fremde Datensätze ergeben „nicht gefunden“.
- Dateien liegen in getrennten Pfaden je Organisation.
- Ein automatischer Test ruft bei jeder Änderung der Software alle Routen mit Kennungen einer fremden Organisation auf und schlägt bei jedem Zugriff fehl, der nicht abgewiesen wird.
- Jede Organisation hat **eigene kryptografische Schlüssel** (Abschnitt 1.5); ein in einen fremden Datensatz kopierter verschlüsselter Wert lässt sich nicht entschlüsseln.
- Getrennte Systeme für Entwicklung und Test; Tests verwenden keine echten Kundendaten.

1.5 Verschlüsselung und Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

- **Transport:** ausschließlich HTTPS mit TLS (aktuelle Protokollversionen, Zertifikate von Let's Encrypt), HSTS. E-Mails werden über einen eigenen Mailserver von LH Printing bei Hetzner versandt und per TLS an die empfangenden Mailserver übertragen, soweit diese TLS unterstützen.
- **Datenbank – Feldverschlüsselung:** Personenbezogene und vertrauliche Felder der Kundendaten werden vor dem Speichern mit **AES-256-GCM** (authentifizierte Verschlüsselung, zufällige Nonce) verschlüsselt, u. a. Namen, Anschriften, Kontaktdaten und Notizen von Kunden, Objekten und Kontakten, Zugangshinweise, Koordinaten, Kundenportal-Zugänge, Unterschriftenamen, Störungs- und Auftragsfreitexte, Versandprotokolle, Berichts-Snapshots und die Werte dieser Felder im Änderungsprotokoll.
- **Schlüsselhierarchie:** Jede Organisation hat einen eigenen Datenschlüssel, der nur mit einem **Hauptschlüssel außerhalb der Datenbank** (Umgebungsvariable bzw. Secret-Datei auf dem Server) verschlüsselt gespeichert wird. Ein Abzug der Datenbank oder eine Datensicherung allein lässt keinen Rückschluss auf Namen, Adressen

oder Telefonnummern zu. Hauptschlüssel und Datenschlüssel können gewechselt werden; die Datenschlüssel einer gelöschten Organisation werden vernichtet (Crypto-Shredding).

- **Fail closed:** Ohne gültigen Hauptschlüssel starten Anwendung, Hintergrundprozesse und Zeitplan nicht; es wird niemals Klartext anstelle verschlüsselter Werte geschrieben.
- **Suche über Blind-Indizes:** Genaue Suche (z. B. E-Mail-Adressen) über HMAC-SHA256 mit einem Schlüssel je Organisation, Teilwortsuche über gekürzte, verschlüsselte Trigramm-Merkmale; eine ordnungserhaltende Verschlüsselung wird nicht verwendet.
- **Techniker-App:** Offline-Daten (Namen, Adressen, Kontaktdaten, Freitexte, Unterschriften, Fotos, Dokumente) werden auf dem Gerät mit AES-256-GCM (WebCrypto) verschlüsselt. Der Schlüssel ist an die Anmeldung des Geräts gebunden und wird beim Abmelden, bei Sperre oder Fernlöschung vernichtet.
- **Datensicherungen:** verschlüsselt mit XChaCha20-Poly1305 und einem eigenen, vom Datenschlüssel verschiedenen Sicherungsschlüssel; ein unverschlüsselter Datenbankabzug entsteht nie auf einem Datenträger.
- **Dateien** (Fotos, Dokumente, PDFs) liegen außerhalb der Datenbank verschlüsselt auf dem Server; der Datenträger der Dateiablage ist vollständig verschlüsselt.
- Namen, E-Mail-Adressen und Telefonnummern der internen Nutzer (Beschäftigte des Kunden) werden für Zuweisung, Kalender und Auswertungen nicht feldverschlüsselt; sie sind durch Rechtekonzept, Mandantentrennung und die Verschlüsselung von Datenträger und Sicherungen geschützt.
- **Pseudonymisierung/Anonymisierung:** Werkzeuge zum Anonymisieren von Kontakten, Portalzugängen und ehemaligen Mitarbeitenden; Kürzung von Empfängeradressen in Versandprotokollen auf die Domain nach einstellbarer Frist.
- **Fotos:** Metadaten (EXIF, GPS-Position) werden beim Hochladen entfernt.

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

2.1 Weitergabekontrolle

- Übertragungen nur verschlüsselt (Abschnitt 1.5). Datenexporte und Datenauskünfte nur für berechtigte Nutzer, mit Rate-Limit und Protokollierung; Auskunftsd Dateien werden nach der Auslieferung sofort gelöscht.
- Versand von E-Mails nur an vom Kunden hinterlegte bzw. ausgewählte Empfänger; Versandprotokolle ohne Inhalte und Anhänge.
- Keine Weitergabe von Kundendaten an Dritte außer an die Unterauftragsverarbeiter nach Anlage 2; keine Analyse-, Werbe- oder KI-Dienste.
- Kartenbilder eines externen Kachelserver werden erst nach Zustimmung des einzelnen Nutzers geladen; dabei verlassen keine Kunden-, Objekt- oder Anlagendaten den Server.

2.2 Eingabekontrolle

- **Änderungsprotokoll** für An- und Abmeldungen, Fehlversuche, Benutzer- und Rechteänderungen, Stammdaten, Aufträge, Berichte, Dateien, Importe, Anonymisierungen und Datenauskünfte, jeweils mit Benutzer, Gerät, IP-Adresse, Zeitpunkt und Vorher/Nachher-Werten. Einträge sind in der Anwendung unveränderlich.
- **Hash-Kette:** Jeder Protokolleintrag wird je Organisation mit SHA-256 an seinen Vorgänger gekettet; Löschen, Ändern oder Umsortieren fällt bei der täglichen automatischen Prüfung auf. Der Kopf der Kette wird zusätzlich im signierten Manifest jeder Datensicherung und täglich per E-Mail an die Verantwortlichen der Organisation abgelegt.
- Prüfberichte werden aus einem eingefrorenen Stand erzeugt und mit einer Prüfsumme gegen Veränderung gesichert (Echtheitsprüfung per Prüfcode).
- Schwärzung personenbezogener Inhalte im Protokoll (Art. 17 DSGVO) ohne Bruch der Kette und mit eigenem, nachvollziehbarem Protokolleintrag.

2.3 Schutz vor Schadcode und Angriffen

- **Uploads:** Erkennung des Dateityps aus dem Inhalt, Freigabeliste erlaubter Typen, Prüfung der Dateieindung, Ablehnung aktiver Inhalte (HTML, SVG, Skripte, Programme), Größenbegrenzung; nicht sicher darstellbare Typen nur als Download.
- **HTTP-Sicherheitsheader:** Content-Security-Policy mit Nonce je Anfrage (keine fremden Skripte), nosniff, Schutz gegen Einbetten in fremde Seiten, restriktive Permissions-Policy (kein Zugriff auf Standort, Mikrofon, Zahlungs- oder USB-Schnittstellen; Kamera nur für die eigene Anwendung), Referrer-Policy.
- **Rate-Limits** für Anmeldung, Passwortfunktionen, Suche, Exporte, E-Mail-Versand, öffentliche Links und die App-Schnittstelle.
- Schutz gegen Cross-Site-Request-Forgery; Validierung aller Eingaben serverseitig, Fremdschlüssel nur innerhalb der eigenen Organisation.
- Abhängigkeiten werden vor jeder Veröffentlichung auf bekannte Sicherheitslücken geprüft (composer audit, npm audit); Sicherheitsupdates von Betriebssystem und Container-Images werden zeitnah eingespielt.

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

- **Datensicherung:** täglich automatisch für Datenbank und Dateiablage, verschlüsselt und signiert; Aufbewahrung von 7 täglichen, 4 wöchentlichen und 12 monatlichen Ständen. Eine Kopie liegt außerhalb des Anwendungsservers in einem getrennten Speicher bei Hetzner in Deutschland (Anlage 2); sie ist ausschließlich verschlüsselt, der Sicherungsschlüssel liegt nicht beim Speicher.
- **Wiederherstellungsprobe:** wöchentlich automatisches Einspielen der jüngsten Sicherung in eine Prüfdatenbank mit Abgleich von Prüfsummen, Zeilenzahlen, Protokoll-Kette und Schlüssel; Ergebnis im Systemstatus.
- Schlüssel (Haupt-, Sicherungs- und Anwendungsschlüssel) werden getrennt von den Sicherungen und zusätzlich offline verwahrt.
- **Überwachung:** Systemstatus mit Warteschlangen, Zeitplan, Speicher, Datensicherung und Wiederherstellungsprobe; Erreichbarkeitsprüfung über einen Gesundheitsendpunkt. [OFFEN: externe Erreichbarkeitsüberwachung einrichten.]
- Papierkorb: gelöschte Stammdaten und Aufträge sind 30 Tage wiederherstellbar.
- Technische Ausstattung der Rechenzentren von Hetzner (redundante Stromversorgung mit USV und Notstrom, Klimatisierung, Brandfrüherkennung, redundante Netzanbindung) nach den Angaben von Hetzner.
- Die Techniker-App arbeitet bei Netzausfall offline weiter und synchronisiert später mit Konfliktbehandlung.

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

- Automatisierte Tests bei jeder Änderung der Software, u. a. für Mandantentrennung, Rechte, Dateizugriff, Uploads, Sicherheitsheader, Rate-Limits, Verschlüsselung (kein Klartext in der Datenbank), Datensicherung, Protokoll-Kette.
- Tägliche Prüfung der Protokoll-Kette, wöchentliche Wiederherstellungsprobe.
- Überprüfung dieser Maßnahmen mindestens jährlich und anlassbezogen (z. B. bei Sicherheitsvorfällen, wesentlichen Änderungen, neuen Unterauftragsverarbeitern).
- Prozess für Sicherheitsvorfälle: Bewertung, Eindämmung, Meldung an betroffene Kunden innerhalb von 48 Stunden (AVV § 10), Dokumentation und Nachbereitung.

5. Datenschutz durch Technikgestaltung und Voreinstellungen (Art. 25 DSGVO)

- Datensparsame Voreinstellungen: Kartenbilder erst nach Zustimmung; keine Standortabfrage der App; keine Tracking-, Analyse- oder Werbedienste; keine Weitergabe an KI-Dienste.

- Löschkonzept in der Anwendung: einstellbare Löschrufen (Kontakte archivierter Kunden, ehemalige Mitarbeitende, gesperrte Portalzugänge, Versandprotokolle), feste Fristen (Fehlerprotokoll 90 Tage ohne Auftreten, Benachrichtigungen 180 Tage, Beispielzeilen aus Importen 180 Tage, Papierkorb 30 Tage, Dateien ohne Verwendung 30 Tage), Anonymisierung auf Anforderung; Löschung der Organisation nach Vertragsende (AVV § 11).
- Fehlerprotokolle werden bereinigt gespeichert (ohne Passwörter, Tokens, SQL-Werte, Anfrageinhalte und IP-Adressen); Serverprotokolle werden rotiert und nach höchstens 14 Tagen gelöscht.
- Werkzeuge für Auskunft, Anonymisierung und Verzeichnis der Verarbeitungstätigkeiten für den Kunden.

6. Organisatorische Maßnahmen

- Verpflichtung aller Personen mit Zugriff auf Kundendaten auf Vertraulichkeit und Datenschutz; Einweisung in die Sicherheitsregeln.
- Zugriff auf Produktivsysteme nach dem Prinzip der minimalen Berechtigung; Entzug aller Zugänge beim Ausscheiden.
- Einziger Unterauftragsverarbeiter ist die Hetzner Online GmbH (Anlage 2), mit Vertrag nach Art. 28 DSGVO und Verarbeitung in Deutschland. Weitere Unterauftragsverarbeiter werden nur nach Prüfung ihres Sicherheitsniveaus und nach Ankündigung gemäß § 7 AVV eingesetzt.
- E-Mails versendet LH Printing über einen eigenen Mailserver; ein externer Versanddienst wird nicht eingesetzt.
- Dokumentierte Verfahren für Datensicherung, Wiederherstellung, Schlüsselverwaltung und Updates (Betriebshandbuch).
- Ansprechpartner für Datenschutz ist Lars Hölker, contact@lhprinting.de. Eine Pflicht zur Benennung eines Datenschutzbeauftragten besteht nicht (§ 38 BDSG, Art. 37 DSGVO).