Technische und organisatorische Maßnahmen (TOM)

nach Art. 32 DSGVO für den Betrieb von RescueNext durch Kröhner Software

> **Geltungsbereich:** Diese Beschreibung gilt für den Betrieb der Ausbildungsplattform RescueNext durch Kröhner Software als Auftragsverarbeiter (Art. 28 DSGVO) für den Kunden als Verantwortlichen. Sie ist **Anlage 1** zum Vertrag zur Auftragsverarbeitung.
>
> **Betriebsmodell:** eigene, getrennte Instanz je Kunde (eigene Container, Datenbank, Schlüssel und internes Netz) auf einem Server der netcup GmbH, Karlsruhe, im Rechenzentrum Nürnberg (Deutschland).
>
> **Stand:** 27.11.2026. Die Beschreibung wird bei wesentlichen Änderungen fortgeschrieben. Markierte Punkte werden vor Vertragsschluss bzw. im Rahmen der Einrichtung festgelegt. Die Unterlage beschreibt den technischen Stand der Anwendung und ersetzt keine rechtliche Prüfung.

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

1.1 Zutrittskontrolle

Ziel: Unbefugte erhalten keinen Zutritt zu den Anlagen, auf denen Daten verarbeitet werden.

- Die Server stehen im Rechenzentrum der netcup GmbH in Deutschland. Den physischen Zutritt regelt und kontrolliert der Rechenzentrumsbetreiber.
- Kröhner Software hat keinen physischen Zutritt zu den Servern. Verwaltet wird ausschließlich über verschlüsselte Fernverbindungen.
- Nachweise des Rechenzentrumsbetreibers (z. B. Zertifizierungen) und dessen AV-Vertrag werden **vor Vertragsschluss abgerufen**.

1.2 Zugangskontrolle

Ziel: Unbefugte können die Systeme nicht nutzen.

Server

- Serverzugang zur Verwaltung nur per SSH-Schlüssel
- Datenbank nicht aus dem Internet erreichbar (nur internes Netz zwischen Anwendung und Datenbank)
- Anwendung nur über HTTPS erreichbar
- Betriebssystem Debian (stabile Version) mit automatischen Sicherheitsupdates; Einrichtung auf dem Kundenserver im Rahmen der Einrichtung
- Fernwartung nur per SSH-Schlüssel über ein eigenes Betriebskonto (keine Root-Anmeldung, keine Passwörter), Sperre nach Fehlanmeldungen; Arbeitsplatzrechner mit aktuellem Betriebssystem und Virenschutz

Anwendung

- Passwörter nur als Argon2id-Hash gespeichert
- allgemeine Fehlermeldung bei der Anmeldung, ohne Hinweis, ob ein Konto existiert
- Sperre nach 5 Fehlversuchen für 15 Minuten, Begrenzung der Anmeldeversuche je Minute
- **Zwei-Faktor-Anmeldung (TOTP) Pflicht** für Praxisanleitung, Ausbildungsleitung und Administration, mit Wiederverwendungsschutz, Wiederherstellungscodes und Sperre nach Fehlversuchen
- Sitzungen: zufälliges 256-Bit-Token, in der Datenbank nur als SHA-256-Hash; Cookie `HttpOnly`, `Secure`, `SameSite=Lax`; neue Sitzungskennung nach der Zwei-Faktor-Anmeldung

- Sitzungsende standardmäßig nach 30 Minuten Leerlauf, spätestens nach 12 Stunden; Abmelden beendet die Sitzung auf dem Server
- Schutz gegen Cross-Site-Angriffe: sitzungsgebundenes CSRF-Token und Herkunftsprüfung (Origin/Referer) bei jeder ändernden Anfrage
- kritische Aktionen verlangen eine erneute Anmeldung

1.3 Zugriffskontrolle

Ziel: Berechtigte sehen und bearbeiten nur die Daten, die sie für ihre Aufgabe brauchen.

- **Rollenmodell** mit fünf Rollen: technische Administration, Ausbildungsleitung, Praxisanleitung, NFS-Auszubildende, Rettungssanitäter/innen (RS)
- jede Berechtigung wird **auf dem Server** geprüft, bei jeder Anfrage, nicht nur in der Oberfläche
- **Datenumfang je Rolle:** Praxisanleitungen sehen nur die ihnen aktuell zugeordneten Auszubildenden, Auszubildende nur die eigene Akte. Rollen lassen sich auf Wachen und Bereiche beschränken.
- Zugriffe auf fremde Akten werden mit „nicht gefunden" beantwortet; die Existenz der Akte wird nicht offengelegt
- die **technische Administration sieht keine vertraulichen Ausbildungsdaten**; die entsprechenden Rechte sind auf dem Server gesperrt, auch in Rollenkombinationen. Kröhner Software arbeitet in der Anwendung mit diesem Konto.
- niemand kann die eigenen Rollen oder Rechte ändern; das letzte Administrationskonto ist geschützt
- Ausbildungsleitung und technische Administration ernennt nur die technische Administration
- Dateiuploads: Prüfung von Dateiendung **und** Dateisignatur, Größenbegrenzung, zufällige Speicherschlüssel; Download nur als Anhang mit abgeschotteter Darstellung
- technischer Zugriff von Kröhner Software auf Server und Datenbank nur zur Erfüllung des Auftrags (Betrieb, Wartung, Sicherung, Fehlerbehebung); Protokollierung dieser Zugriffe: **im Rahmen der Einrichtung festzulegen**
- getrennte Datenbankkonten (Anwendung ohne Rechte zum Ändern der Datenbankstruktur oder zum Abschalten der Schutz-Trigger): technisch vorbereitet, Einsatz **im Rahmen der Einrichtung festzulegen**

1.4 Trennungskontrolle

Ziel: Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden getrennt verarbeitet.

- **eigene Instanz und eigene Datenbank je Kunde** (eigene Container, Schlüssel und internes Netz); keine gemeinsame Datenhaltung mit anderen Kunden
- Vorführ- und Testumgebungen nur mit synthetischen Daten; der Vorführmodus startet technisch nur mit einer eigens dafür bestimmten, getrennten Datenbank
- die Probekopie der Datenbank für die Prüfung eines Updates ist isoliert und kurzlebig und wird danach wieder entfernt
- Lernaktivitäten (Punkte, Stufen, Abzeichen) sind von den offiziellen Ausbildungsnachweisen getrennt; keine öffentlichen Ranglisten

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

- Übertragung nur über HTTPS (TLS)
- hochgeladene Dokumente und Zwei-Faktor-Schlüssel in der Anwendung verschlüsselt (AES-256-GCM); Zugangsdaten für den E-Mail-Versand verschlüsselt gespeichert
- Passwörter nur als Hash (Argon2id), Sitzungstokens nur als Hash (SHA-256)
- Datensicherungen verschlüsselt (AES-256, Schlüsselableitung PBKDF2); Schlüssel getrennt von den Daten aufbewahrt
- Festplattenverschlüsselung des Servers: **im Rahmen der Einrichtung festzulegen**
- Konten können deaktiviert und nach Frist anonymisiert werden

- Protokolle ohne Passwörter, Sitzungsschlüssel oder Inhalte; Exporte der Systemdiagnose ohne Personendaten

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

2.1 Weitergabekontrolle

Ziel: Daten werden bei Übertragung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt.

- Übertragung zwischen Browser und Server nur über HTTPS (TLS)
- **keine US-Dienste im Betrieb** (kein AWS, Azure oder Google), keine Verarbeitung in Drittländern
- keine Abrufe von fremden Servern: Schriften und Programmteile liefert der eigene Server; strenge Content-Security-Policy ohne externe Quellen
- keine Cookies zu Werbezwecken, kein Tracking, keine Analysewerkzeuge Dritter
- **KI-Funktionen im Auslieferungszustand ausgeschaltet**; es werden keine Daten an KI-Dienste übertragen
- Hinweis-Mails enthalten nur Titel und Link, keine vertraulichen Inhalte. Anbieter für den E-Mail-Versand: ALL-INKL.COM (Deutschland)
- Exporte und Downloads werden im Audit-Log protokolliert
- die App-Installation auf dem Handy (PWA) speichert keine Antworten des Servers zwischen
- Sicherungen werden vor dem Verlassen des Servers verschlüsselt; eine externe Kopie wird nur verschlüsselt übertragen. Die externe Kopie liegt verschlüsselt auf einem Speichersystem von Kröhner Software in Deutschland (Abruf über einen Nur-Lese-Zugang)
- Datenexport für den Kunden bei Vertragsende; Format: **im Rahmen der Einrichtung festzulegen**

2.2 Eingabekontrolle

Ziel: Es ist nachvollziehbar, wer wann welche Daten eingegeben, verändert oder entfernt hat.

- **Audit-Log** für Anmeldungen, Fehlversuche, Zwei-Faktor-Ereignisse, Rollen- und Rechteänderungen, alle fachlichen Statuswechsel, Exporte und Downloads
- das Audit-Log ist in der Datenbank technisch unveränderlich (Datenbank-Trigger)
- freigegebene Berichte, Versionen, Prüfentscheidungen und Einschätzungen sind per Trigger gegen Änderung geschützt; jede Version erhält eine prüfbare SHA-256-Prüfsumme
- Freigaben sind kontogebunden, mit Vier-Augen-Gegenzeichnung und Manipulationserkennung. Sie sind eine **einfache elektronische Bestätigung**, keine qualifizierte elektronische Signatur.
- Eingaben werden auf dem Server geprüft (Schemas, Längenbegrenzung); Datenbankabfragen nur parametrisiert
- Lösch- und Aufbewahrungsfristen legt der Kunde fest; der automatische Aufbewahrungslauf ist standardmäßig aus und wird erst nach Festlegung eingeschaltet

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

Ziel: Daten sind gegen Verlust geschützt und nach einem Zwischenfall rasch wiederherstellbar.

- **tägliche Datensicherung** von Datenbank, Dateispeicher und Konfiguration, verschlüsselt
- Prüfsummen (SHA-256) über alle Dateien jeder Sicherung, sofort nach dem Erstellen geprüft
- **Test-Wiederherstellung bei jeder Sicherung** in eine temporäre Datenbank; schlägt sie fehl, wird die Sicherung als fehlerhaft gemeldet
- lokale Aufbewahrung standardmäßig 14 Tage; die letzten 3 Sicherungen werden nie automatisch gelöscht
- externe Sicherung außerhalb des Servers: täglich, verschlüsselt, 30 Tage Aufbewahrung

- Überwachung alle 5 Minuten auf dem Server und alle 10 Minuten von außen (Erreichbarkeit, Dienste, Zertifikate, Speicher, Sicherung) mit Alarm per E-Mail
- Stand der letzten Sicherung in der Administration der Anwendung sichtbar
- dokumentierte Verfahren für Wiederherstellung und Notfallwiederherstellung bei Totalverlust des Servers
- Updates: vorher an einer Probekopie der Datenbank geprüft, vollständige Sicherung vor jedem Update, dokumentierte Rückfallmöglichkeit
- Anwendung in abgeschotteten Containern (ohne Root-Rechte, schreibgeschütztes Dateisystem, ohne zusätzliche Systemrechte) mit Begrenzung von Arbeitsspeicher und Prozessen
- Begrenzung von Anfragegröße und Anmeldeversuchen gegen Überlastung
- Zustandsprüfungen (Health-Endpunkte) und Systemstatus-Seite
- Verfügbarkeitszusage und Wartungsfenster: **im Hauptvertrag festzulegen**

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

- automatisierte Tests für Anmeldung, Rechte und Sicherheitsfunktionen vor jedem Update
- Prüfung der eingesetzten Programmbibliotheken auf bekannte Schwachstellen
- Sicherheitsentscheidungen werden in einem fortlaufenden Entscheidungsprotokoll dokumentiert
- datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO): KI-Funktionen aus, automatische Löschläufe erst nach Festlegung durch den Kunden, E-Mail-Versand nur nach Einrichtung
- externe Sicherheitsprüfung (Penetrationstest): bisher nicht erfolgt; optional, **im Rahmen der Einrichtung festzulegen**

Auftragskontrolle

- Verarbeitung nur nach dokumentierter Weisung des Kunden (siehe AV-Vertrag)
- Personen, die im Auftrag tätig werden, sind zur Vertraulichkeit verpflichtet
- Unterauftragsverarbeiter nur mit eigenem AV-Vertrag und nach Information des Kunden (Liste in Anlage 2 des AV-Vertrags)
- Datenschutzverletzungen meldet Kröhner Software dem Kunden **unverzüglich**, damit dieser die Frist von 72 Stunden (Art. 33 DSGVO) einhalten kann

5. Übersicht der festzulegenden Punkte

Punkt	Stand
Standort des Rechenzentrums (netcup GmbH)	Nürnberg (Deutschland)
Nachweise des Rechenzentrumsbetreibers	**vor Vertragsschluss abzurufen**
Anbieter für den E-Mail-Versand	ALL-INKL.COM – Neue Medien Münnich, Friedersdorf
Anbieter und Ort der externen Sicherung	Kröhner Software, Deutschland (verschlüsselt)
Festplattenverschlüsselung des Servers	beim VPS nicht vorgesehen; Dokumente, Schlüssel und Sicherungen gesondert verschlüsselt
Absicherung der Fernwartung	SSH-Schlüssel, eigenes Betriebskonto, keine Passwörter
Protokollierung technischer Zugriffe auf Server und Datenbank	**im Rahmen der Einrichtung festzulegen**

Punkt	Stand
getrennte Datenbankkonten	im Rahmen der Einrichtung festzulegen
Format des Datenexports bei Vertragsende	im Rahmen der Einrichtung festzulegen
Lösch- und Aufbewahrungsfristen	legt der Kunde fest
Penetrationstest	im Rahmen der Einrichtung festzulegen
Verfügbarkeitszusage und Wartungsfenster	im Hauptvertrag festzulegen