Datenblatt Betrieb und Sicherheit

RescueNext ist die Ausbildungsplattform für die Notfallsanitäter-Ausbildung. Dieses Datenblatt beschreibt, wie Kröhner Software die Plattform für Sie betreibt und wie Ihre Daten geschützt sind.

> **Rollen nach DSGVO:** Sie als Träger des Rettungsdienstes sind **Verantwortlicher** (Art. 4 Nr. 7 DSGVO). Kröhner Software ist **Auftragsverarbeiter** (Art. 28 DSGVO) und übernimmt Betrieb, Wartung, Updates und Sicherung nach Ihrer Weisung. Grundlage ist ein Vertrag zur Auftragsverarbeitung (AV-Vertrag) als Anlage zum Hauptvertrag.

1. Betrieb

Punkt	Leistung
Server	**Eigene, getrennte Instanz je Kunde** mit eigener Datenbank, eigenen Schlüsseln und eigenem internen Netz. Keine gemeinsame Datenhaltung mit anderen Kunden.
Hoster	netcup GmbH, Karlsruhe (Unterauftragsverarbeiter von Kröhner Software)
Standort	Rechenzentrum **Nürnberg (Deutschland)**, kein Drittland
Erreichbarkeit	eigene Adresse für Ihre Einrichtung, ausschließlich über HTTPS (TLS)
Datensicherung	**täglich und verschlüsselt** (AES-256), mit Prüfsummen und automatischer Test-Wiederherstellung bei jeder Sicherung. Der Schlüssel wird getrennt von den Daten aufbewahrt.
Externe Sicherung	täglich auf ein Speichersystem von Kröhner Software in Deutschland, nur verschlüsselt, Abruf über einen Nur-Lese-Zugang, 30 Tage
Updates	Jedes Update wird vorher an einer **Probekopie** der Datenbank geprüft. Vor jedem Update erfolgt eine vollständige Sicherung mit dokumentierter **Rückfallmöglichkeit**.
E-Mail-Versand	Hinweis-Mails enthalten nur Titel und Link, keine Inhalte. Anbieter: ALL-INKL.COM – Neue Medien Münnich, Friedersdorf (Deutschland)
Support	per E-Mail an support@rescuenext.de, **Antwort innerhalb von 2 Werktagen**
Laufzeit	Mindestlaufzeit **12 Monate**, danach Kündigungsfrist **3 Monate**
Vertragsende	**Datenexport** für Sie, danach **Löschung mit Bestätigung**. Format des Exports: **im Rahmen der Einrichtung festzulegen**
Quellcode-Hinterlegung	optional bei einem Treuhänder (Escrow), gegen Aufpreis

2. Datenschutz auf einen Blick

- **Keine US-Dienste im Betrieb:** kein AWS, kein Azure, kein Google. Schriften und Programmteile werden vom eigenen Server geladen, nicht von fremden Servern.
- **Keine Cookies zu Werbezwecken:** nur technisch notwendige Cookies für Anmeldung und Sitzung, kein Tracking, keine Analysewerkzeuge Dritter.
- **KI-Funktionen ausgeschaltet:** Es werden keine Daten an KI-Dienste übertragen.
- **Keine Patientendaten:** Die Formulare weisen darauf hin und verlangen eine Bestätigung. Eine Erkennung warnt bei typischen Mustern (z. B. Geburtsdatum, Name, Einsatznummer). Eine Anonymisierung ist damit nicht garantiert.
- **Betroffenenrechte:** Auskunft als Export je Person, Konten deaktivierbar und nach Frist anonymisierbar. Die Löschfristen legen Sie fest.

- **Beschäftigtendaten:** Ob eine Betriebsvereinbarung nötig ist, klären Sie mit Ihrer Mitarbeitervertretung.

3. Sicherheit (Kurzfassung)

Die ausführliche Beschreibung enthält die Unterlage **„Technische und organisatorische Maßnahmen (TOM)“**.

Anmeldung

- Passwörter nur als Argon2id-Hash gespeichert
- Sperre nach mehreren Fehlversuchen, Begrenzung der Anmeldeversuche
- **Zwei-Faktor-Anmeldung (TOTP) Pflicht** für Praxisanleitung, Ausbildungsleitung und Administration, mit Wiederverwendungsschutz und Wiederherstellungscodes
- Sitzungen enden standardmäßig nach 30 Minuten Leerlauf, spätestens nach 12 Stunden
- Schutz gegen Cross-Site-Angriffe (CSRF- und Herkunftsprüfung)
- kritische Aktionen verlangen eine erneute Anmeldung

Berechtigungen

- jede Berechtigung wird **auf dem Server** geprüft, nicht nur in der Oberfläche
- Rollen lassen sich auf Wachen und Bereiche beschränken; fremde Akten sind nicht sichtbar
- die technische Administration sieht **keine vertraulichen Ausbildungsdaten**
- niemand kann die eigenen Rechte ändern

Verschlüsselung

- Übertragung nur über HTTPS (TLS)
- hochgeladene Dokumente und Zwei-Faktor-Schlüssel in der Anwendung verschlüsselt (AES-256-GCM)
- Datensicherungen verschlüsselt, Schlüssel getrennt aufbewahrt

Nachvollziehbarkeit

- **Audit-Log** für Anmeldungen, Rechteänderungen, Freigaben, Exporte und Downloads, in der Datenbank technisch unveränderlich (Datenbank-Trigger)
- freigegebene Berichte und Einschätzungen mit Prüfsumme gegen nachträgliche Änderung geschützt
- Freigaben sind eine **einfache elektronische Bestätigung**, keine qualifizierte elektronische Signatur

Serverbetrieb

- Anwendung in abgeschotteten Containern (ohne Root-Rechte, schreibgeschützt, internes Datenbanknetz)
- Datenbank nicht aus dem Internet erreichbar, Serverzugang nur per SSH-Schlüssel
- Protokolle ohne Passwörter, Sitzungsschlüssel oder Inhalte

4. Unterlagen und Kontakt

Weitere Unterlagen: Muster-Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO) · Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Kröhner Software · Enrico Kröhner (Einzelunternehmen) · Zollwitzer Ring 31, 04680 Colditz
E-Mail support@rescuenext.de · Telefon 0151 29474676

Dieses Datenblatt beschreibt den technischen Stand der Anwendung. Es ersetzt keinen Vertrag und keine rechtliche Prüfung. Markierte Punkte werden vor Vertragsschluss bzw. im Rahmen der Einrichtung festgelegt.