Vertrag zur Auftragsverarbeitung

gemäß Art. 28 Abs. 3 DSGVO

> **Muster – vor Verwendung rechtlich prüfen lassen.** Dieses Muster ist ein Entwurf von Kröhner Software und keine Rechtsberatung. Es muss vor Abschluss von einer rechtskundigen Stelle (z. B. Anwalt für IT-Recht, Datenschutzbeauftragte/r des Kunden) geprüft und an den Einzelfall angepasst werden. Eckige Klammern [ ] kennzeichnen Angaben, die einzutragen oder festzulegen sind.

Vertragsparteien

Verantwortlicher (im Folgenden „Auftraggeber")	[Name des Trägers des Rettungsdienstes] [Anschrift] vertreten durch [Name, Funktion]
Auftragsverarbeiter (im Folgenden „Auftragnehmer")	Kröhner Software, Inhaber Enrico Kröhner (Einzelunternehmen) Zollwitzer Ring 31, 04680 Colditz support@rescuenext.de · Telefon 0151 29474676

§ 1 Gegenstand und Dauer des Auftrags

1. Gegenstand des Auftrags ist der Betrieb der Ausbildungsplattform **RescueNext** für den Auftraggeber. Der Auftragnehmer stellt die Anwendung auf einem eigenen Server für den Auftraggeber bereit und übernimmt Betrieb, Wartung, Updates, Datensicherung und Support. Einzelheiten regelt der Hauptvertrag vom [Datum] (im Folgenden „Hauptvertrag").
2. Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrags. Der Vertrag endet nicht, solange der Auftragnehmer noch personenbezogene Daten des Auftraggebers verarbeitet (insbesondere bis zur vollständigen Rückgabe und Löschung nach § 10).

§ 2 Art und Zweck der Verarbeitung

1. **Art der Verarbeitung:** Speicherung, Bereitstellung, Sicherung, Wiederherstellung, Aktualisierung der Software, Fehleranalyse und -behebung sowie Unterstützung der Nutzerinnen und Nutzer (Support), jeweils soweit für den Betrieb der Anwendung erforderlich.
2. **Zweck der Verarbeitung:** Organisation, Dokumentation und Unterstützung der Ausbildung im Rettungsdienst (insbesondere Notfallsanitäter-Ausbildung) beim Auftraggeber. Die Anwendung dient nicht der Diagnose, Therapie oder Entscheidungsunterstützung in der Patientenversorgung.
3. Die Verarbeitung findet ausschließlich in Deutschland statt. Eine Verarbeitung in einem Drittland bedarf der vorherigen dokumentierten Weisung des Auftraggebers und der Erfüllung der Voraussetzungen der Art. 44 ff. DSGVO.

§ 3 Art der Daten und Kreis der Betroffenen

1. **Arten personenbezogener Daten:**
   - Stammdaten: Name, dienstliche E-Mail-Adresse, Rolle, Wache, Ausbildungsjahr
   - Ausbildungsdaten: Berichtsheft, Klinik- und Wachennachweise, Ausbildungsziele, Kompetenzeinschätzungen, Gespräche, Praxisaufträge, hochgeladene Dokumente

- Lerndaten: Lernfortschritt, Quiz- und Simulatorergebnisse
- Kommunikationsdaten: Nachrichten und Hinweise innerhalb der Anwendung
- Protokolldaten: Anmeldungen, Rechteänderungen, Freigaben, Exporte und Downloads (Audit-Log), Sitzungsdaten
- [weitere Datenarten nach Festlegung des Auftraggebers]

2. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand der Verarbeitung. **Patientendaten sollen nicht verarbeitet werden**; die Anwendung weist in den Formularen darauf hin. Es handelt sich um Beschäftigtendaten.
3. **Kreis der Betroffenen:**
   - Auszubildende (Notfallsanitäter-Auszubildende; Rettungssanitäter/innen in Praktikum oder Einarbeitung)
   - Praxisanleiterinnen und Praxisanleiter
   - Ausbildungsleitung
   - technische Administration des Auftraggebers
   - ggf. Ansprechpersonen der Schule
   - [weitere Betroffene nach Festlegung des Auftraggebers]

§ 4 Weisungsbefugnis des Auftraggebers

1. Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach dem Recht der Union oder Deutschlands zur Verarbeitung verpflichtet (Art. 28 Abs. 3 lit. a DSGVO). In diesem Fall teilt er dem Auftraggeber diese Anforderung vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.
2. Weisungen erteilt der Auftraggeber grundsätzlich in Textform (z. B. E-Mail). Mündliche Weisungen bestätigt er unverzüglich in Textform. Weisungsberechtigte Personen und Empfänger der Weisungen nennt Anlage 3.
3. Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er den Auftraggeber unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO). Er darf die Ausführung der Weisung aussetzen, bis der Auftraggeber sie bestätigt oder ändert.
4. Der Auftragnehmer verwendet die Daten nicht für eigene Zwecke.

§ 5 Vertraulichkeit

1. Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).
2. Die Verpflichtung gilt auch nach Beendigung dieses Vertrags fort.

§ 6 Technische und organisatorische Maßnahmen

1. Der Auftragnehmer trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Sie sind in **Anlage 1** beschrieben (Unterlage „Technische und organisatorische Maßnahmen (TOM)“, Stand 27.11.2026).
2. Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie durch gleichwertige oder bessere Maßnahmen ersetzen; das Schutzniveau darf nicht unterschritten werden. Wesentliche Änderungen dokumentiert er und teilt sie dem Auftraggeber mit.

§ 7 Unterauftragsverarbeiter

1. Der Auftraggeber genehmigt die in **Anlage 2** genannten Unterauftragsverarbeiter.
2. Der Auftragnehmer informiert den Auftraggeber vor jeder beabsichtigten Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters in Textform, mindestens [Frist eintragen] im Voraus. Der Auftraggeber kann der Änderung innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen (Art. 28 Abs. 2 DSGVO). [Folgen eines Widerspruchs, z. B. Sonderkündigungsrecht, im Hauptvertrag festlegen.]
3. Der Auftragnehmer erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind (Art. 28 Abs. 4 DSGVO). Er haftet gegenüber dem Auftraggeber für die Einhaltung dieser Pflichten durch den Unterauftragsverarbeiter.
4. Keine Unterauftragsverhältnisse im Sinne dieser Regelung sind Nebenleistungen, bei denen kein Zugriff auf personenbezogene Daten des Auftraggebers vorgesehen ist (z. B. Telekommunikationsleistungen).

§ 8 Unterstützung des Auftraggebers

1. Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen (Art. 12 bis 22 DSGVO). Die Anwendung stellt dafür u. a. einen Export je Person (Auskunft), die Deaktivierung und die Anonymisierung von Konten bereit.
2. Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet er das Anliegen unverzüglich an den Auftraggeber weiter und beantwortet es nicht selbst.
3. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung und Benachrichtigung bei Datenschutzverletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).
4. [Vergütung für Unterstützungsleistungen, die über den Hauptvertrag hinausgehen, im Hauptvertrag festlegen.]

§ 9 Meldung von Verletzungen des Schutzes personenbezogener Daten

1. Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten **unverzüglich**, nachdem sie ihm bekannt geworden ist (Art. 33 Abs. 2 DSGVO), damit der Auftraggeber die Frist von 72 Stunden nach Art. 33 Abs. 1 DSGVO einhalten kann.
2. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO: Art der Verletzung, Kategorien und ungefähre Zahl der Betroffenen und Datensätze, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Maßnahmen. Informationen, die noch nicht vorliegen, reicht er unverzüglich nach.
3. Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen und stimmt sie mit dem Auftraggeber ab.
4. Meldungen an die Aufsichtsbehörde und Benachrichtigungen der Betroffenen nimmt der Auftraggeber vor.

§ 10 Löschung und Rückgabe nach Ende des Auftrags

1. Nach Beendigung der Verarbeitungsleistungen stellt der Auftragnehmer dem Auftraggeber nach dessen Wahl die personenbezogenen Daten als **Datenexport** zur Verfügung (Format: **im Rahmen der Einrichtung festzulegen**) und **löscht** sie anschließend, sofern nicht nach dem Recht der Union oder Deutschlands eine Pflicht zur Speicherung besteht (Art. 28 Abs. 3 lit. g DSGVO).

2. Die Löschung umfasst auch Kopien auf dem Server und in Datensicherungen. Datensicherungen werden spätestens mit Ablauf ihrer Aufbewahrungsfrist gelöscht ([Frist eintragen]).
3. Der Auftragnehmer **bestätigt die Löschung** in Textform.

§ 11 Nachweise und Kontrollrechte

1. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung (Art. 28 Abs. 3 lit. h DSGVO).
2. Der Auftraggeber oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer kann Überprüfungen einschließlich Inspektionen durchführen. Sie werden in der Regel mit einer Frist von [Frist eintragen] angemeldet und zu den üblichen Geschäftszeiten durchgeführt, ohne den Betrieb unverhältnismäßig zu stören.
3. Die Kontrolle beim Rechenzentrumsbetreiber erfolgt in erster Linie über dessen Nachweise (z. B. Zertifizierungen, Prüfberichte).
4. [Kostentragung für Kontrollen im Hauptvertrag festlegen.]

§ 12 Haftung

Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregeln des Hauptvertrags. [Abstimmung mit dem Hauptvertrag rechtlich prüfen lassen.]

§ 13 Schlussbestimmungen

1. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen in Fragen des Datenschutzes die Regelungen dieses Vertrags vor.
2. Änderungen und Ergänzungen bedürfen der Textform. Das gilt auch für den Verzicht auf dieses Formerfordernis.
3. Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
4. **Kirchliche Träger:** Unterliegt der Auftraggeber kirchlichem Datenschutzrecht (z. B. KDG oder DSG-EKD), sind die Verweise dieses Vertrags auf die entsprechenden Vorschriften anzupassen. [Rechtlich prüfen lassen.]
5. Gerichtsstand ist [Ort eintragen], soweit gesetzlich zulässig.

Auftraggeber	Auftragnehmer
Ort, Datum: _____	Ort, Datum: _____
_____	_____
[Name, Funktion]	Enrico Kröhner, Kröhner Software

MUSTER

Anlage 1 – Technische und organisatorische Maßnahmen

Es gilt die Unterlage **„Technische und organisatorische Maßnahmen (TOM) nach Art. 32 DSGVO“**, Stand 27.11.2026, in der jeweils dem Auftraggeber mitgeteilten Fassung.

Anlage 2 – Unterauftragsverarbeiter

Leistung	Unterauftragsverarbeiter	Ort der Verarbeitung
Bereitstellung von Server und Rechenzentrum (kein Zugriff auf Inhalte vorgesehen)	netcup GmbH, Daimlerstraße 25, 76185 Karlsruhe	Rechenzentrum Nürnberg (Deutschland)
E-Mail-Versand von Hinweis-Mails (nur Titel und Link, keine Inhalte)	ALL-INKL.COM – Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf	Deutschland
Externe Datensicherung (nur verschlüsselte Sicherungskopien)	keine Unterbeauftragung: eigenes Speichersystem von Kröhner Software	Deutschland

Es werden **keine US-Cloud-Dienste** eingesetzt. KI-Dienste sind nicht beteiligt; die KI-Funktionen der Anwendung sind ausgeschaltet.

Anlage 3 – Weisungsberechtigte Personen und Ansprechpartner

	Auftraggeber	Auftragnehmer
Weisungsberechtigt bzw. Empfänger von Weisungen	[Name, Funktion, E-Mail]	Enrico Kröhner, support@rescuenext.de
Vertretung	[Name, Funktion, E-Mail]	[**im Rahmen der Einrichtung festzulegen**]
Datenschutzbeauftragte/r	[Name, Kontakt]	[falls benannt, eintragen]
Meldungen nach § 9 an	[E-Mail, Telefon]	–

Muster – vor Verwendung rechtlich prüfen lassen. Stand 27.11.2026.

MUSTER