

Vereinbarung zur Auftragsverarbeitung

Vereinbarung nach Art. 28 DSGVO · Stand September 2026

zwischen dem Kunden (nachfolgend „Verantwortlicher“) und der KMK IT-Schutz GmbH, Lilienweg 16, 74388 Talheim (nachfolgend „Auftragsverarbeiter“), als Bestandteil des Vertrags über die Nutzung der Plattform Rekura (rekura.eu).

§ 1 Gegenstand und Dauer

Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen zur Erstellung und Pflege von IT-Notfallplänen über die Plattform Rekura. Gegenstand dieser Vereinbarung ist die dabei erfolgende Verarbeitung personenbezogener Daten im Auftrag. Die Dauer entspricht der Laufzeit des Hauptvertrags.

§ 2 Art, Zweck, Datenarten und Betroffene

Zweck der Verarbeitung ist die Bereitstellung der Plattform einschließlich Plan-Erstellung, Plausibilitätsprüfung, Frage-Delegation, Versionierung, Rechnungsstellung und Hinweisdiensten.

Datenarten

- Konto- und Organisationsdaten (Name, dienstliche E-Mail-Adresse, Organisation, Rolle)
- Kontaktdaten benannter Personen (z. B. Krisenstab, Notfallkontakte: Name, Funktion, dienstliche Erreichbarkeit)
- Daten der Frage-Delegation (dienstliche E-Mail-Adresse und, sofern angegeben, Name der vom Verantwortlichen benannten Person, die von ihr übermittelte Antwort sowie Zeitpunkt und Status der Anfrage)
- Angaben zur IT-Infrastruktur und zu Prozessen (in der Regel ohne Personenbezug; keine Passwörter oder Zugangsdaten)
- Vertrags- und Rechnungsdaten sowie technische Nutzungsdaten (Server-Logs)

Kreis der Betroffenen

Beschäftigte und Funktionsträger des Verantwortlichen sowie von ihm benannte Ansprechpersonen und Dienstleister; hierzu zählen auch Beschäftigte, an die der Verantwortliche einzelne Fragen des Fragebogens zur Beantwortung weitergibt.

§ 3 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen und für die vertraglich vereinbarten Zwecke. Zur Verarbeitung eingesetzte Personen sind zur Vertraulichkeit verpflichtet. Der Auftragsverarbeiter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO gemäß Anlage 1 und passt sie dem Stand der Technik an, ohne das Schutzniveau zu unterschreiten.

§ 4 Subunternehmer

Der Verantwortliche genehmigt die in Anlage 2 genannten Subunternehmer allgemein. Der Auftragsverarbeiter informiert über beabsichtigte Änderungen; der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund widersprechen. Mit jedem Subunternehmer werden Verpflichtungen entsprechend dieser Vereinbarung vereinbart; bei Verarbeitung in Drittländern werden geeignete Garantien (insbesondere EU-Standardvertragsklauseln) sichergestellt.

§ 5 Unterstützung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei der Erfüllung von Betroffenenrechten (Art. 12–23 DSGVO) sowie bei den Pflichten aus Art. 32–36 DSGVO, soweit ihm dies unter Berücksichtigung der Art der Verarbeitung möglich ist.

§ 6 Meldung von Verletzungen

Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden und stellt die zur Erfüllung der Meldepflichten des Verantwortlichen erforderlichen Informationen bereit.

§ 7 Löschung und Rückgabe

Nach Beendigung des Hauptvertrags löscht der Auftragsverarbeiter alle personenbezogenen Daten des Verantwortlichen oder gibt sie zurück, sofern keine gesetzlichen Aufbewahrungspflichten (insbesondere handels- und steuerrechtlich für Rechnungsdaten) entgegenstehen. Der Verantwortliche kann seine Plan-Dokumente vor Vertragsende exportieren.

§ 8 Nachweise und Kontrollen

Der Auftragsverarbeiter stellt dem Verantwortlichen die zum Nachweis der Einhaltung dieser Vereinbarung erforderlichen Informationen zur Verfügung (insbesondere die Dokumentation der Maßnahmen nach Anlage 1) und ermöglicht angemessene Überprüfungen. Kontrollen erfolgen nach Ankündigung, während der Geschäftszeiten und unter Wahrung von Betriebs- und Geschäftsgeheimnissen.

§ 9 Haftung und Schlussbestimmungen

Für die Haftung gilt Art. 82 DSGVO; im Übrigen gelten die Regelungen des Hauptvertrags. Änderungen bedürfen der Textform. Sollte eine Bestimmung unwirksam sein, bleibt die Vereinbarung im Übrigen wirksam. Es gilt deutsches Recht.

Anlage 1 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

1. Vertraulichkeit

- Zutrittskontrolle: Betrieb der Plattform und der Datenbank in ISO-27001-zertifizierten Rechenzentren in Deutschland (Hetzner, Falkenstein); verschlüsselte Sicherungskopien zusätzlich in einem Rechenzentrum in der Europäischen Union (Frankreich); kein physischer Serverzugriff durch Unbefugte.
- Zugangskontrolle: Serverzugang nur per SSH-Schlüsselverfahren; Firewall beschränkt eingehende Verbindungen auf die erforderlichen Dienste; Administrationszugänge mit Zwei-Faktor-Authentisierung; Schutz vor Brute-Force durch Raten-Begrenzung; verpflichtende E-Mail-Verifizierung von Kundenkonten.
- Zugriffskontrolle: rollenbasierte Rechtentrennung zwischen Betreiber- und Kundenkonten; Kunden sehen ausschließlich Daten der eigenen Organisation; Durchsetzung serverseitig.
- Trennungskontrolle: logische Mandantentrennung auf Organisationsebene; getrennte Rechnungsnummernkreise.
- Datenminimierung: Es werden keine Passwörter oder Zugangsdaten zu Kundensystemen und keine IP-Adressen der Kundeninfrastruktur erhoben; erfasst werden lediglich Ablageorte und — auf Wunsch abstrahierte — Systembezeichnungen.
- Speicherkontrolle: Verschlüsselung sensibler Inhalte in der Datenbank (AES-256).

2. Integrität

- Übertragungskontrolle: Transportverschlüsselung (TLS/HTTPS) für sämtliche Verbindungen; E-Mail-Versand über authentifizierte Absenderdomain (SPF, DKIM, DMARC).
- Eingabekontrolle: revisionssichere Versionierung der Plan-Dokumente (unveränderliche Stände); Protokollierung sicherheitsrelevanter Ereignisse.

3. Verfügbarkeit und Belastbarkeit

- Tägliche automatisierte, verschlüsselte Datenbank-Sicherungen mit 14-tägiger lokaler Aufbewahrung sowie eine zusätzliche, clientseitig verschlüsselte Sicherungskopie in einem räumlich und organisatorisch getrennten Rechenzentrum in der Europäischen Union, dort unveränderlich für 30 Tage aufbewahrt (Object Lock). Der Schlüssel zur Entschlüsselung der Sicherungskopien liegt nicht beim Anbieter des Sicherungsspeichers. Die Wiederherstellbarkeit wird wöchentlich automatisiert geprüft; dokumentiertes Wiederherstellungsverfahren.
- Aktuelle Sicherheitsupdates; Kapazitätsüberwachung; Begrenzung automatisierter Anfragen (Rate-Limits).

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Auftragskontrolle: Einsatz von Subunternehmern nur mit Auftragsverarbeitungsvertrag bzw. EU-Standardvertragsklauseln (Anlage 2); Weisungsbindung.
- Regelmäßige Überprüfung der Wirksamkeit der Maßnahmen; laufendes Monitoring relevanter Rechtsänderungen; definierter Prozess zur unverzüglichen Meldung von Datenschutzverletzungen.

Anlage 2 — Genehmigte Subunternehmer

Unternehmen	Leistung	Sitz / Ort	Garantien
Hetzner Online GmbH	Hosting und Server-Infrastruktur	Deutschland (RZ Falkenstein)	Auftragsverarbeitungsvertrag; ISO-27001-zertifizierte Rechenzentren
Sendinblue GmbH (Brevo)	Versand von Transaktions-E-Mails (Rechnungen, Konto-Mails, Hinweise)	Deutschland / EU	Auftragsverarbeitungsvertrag; Versand über authentifizierte Domain
Anthropic PBC	KI-gestützte Texterstellung bei der Plan-Ausformulierung	USA	Auftragsverarbeitung mit EU-Standardvertragsklauseln; keine Nutzung zu Trainingszwecken
Scaleway S.A.S.	Verschlüsselte Off-site-Sicherung der Datenbank (Objektspeicher)	Frankreich / EU (RZ Raum Paris)	Auftragsverarbeitungsvertrag; ausschließlich EU-Rechenzentren; Sicherungskopien clientseitig verschlüsselt (Schlüssel liegt nicht beim Anbieter); unveränderliche Aufbewahrung (Object Lock)
seven communications GmbH & Co. KG (seven.io)	SMS-Versand des Ernstfall-OTP (Break-Glass-Zweitkanal)	Kiel, Deutschland	Auftragsverarbeitungsvertrag (Art. 28 DSGVO), unterzeichnet am 10.09.2026; verarbeitet nur Mobilnummer und OTP-Text

Stand: September 2026. Änderungen werden dem Verantwortlichen mitgeteilt (§ 4).