Anlage: Technische und organisatorische Maßnahmen

Fassung: September 2026

1. Ziel und Geltungsbereich

Diese Anlage beschreibt technische und organisatorische Maßnahmen des Auftragnehmers für die Verarbeitung personenbezogener Daten im Rahmen von Coveniq AI. Die Maßnahmen sind als Mindestniveau zu verstehen und können weiterentwickelt werden, sofern das erreichte Schutzniveau nicht unterschritten wird.

2. Übersicht der Schutzlogik von Coveniq AI

1. Nutzer geben Prompts oder Dokumentinhalte über die Coveniq-AI-Oberfläche ein.
2. Die Inhalte werden im Coveniq-Backend verarbeitet und vor einer möglichen Weitergabe an angebundene KI-Modelle durch den Privacy Guard analysiert.
3. Erkannte personenbezogene Angaben werden durch neutrale Platzhalter ersetzt.
4. Die Zuordnung zwischen Originalwerten und Platzhaltern verbleibt innerhalb der Coveniq-Infrastruktur.
5. Das angebundene KI-Modell erhält grundsätzlich nur den mitigierten Prompt. Nach Eingang der Antwort werden Platzhalter soweit erforderlich wieder zurückübersetzt und dem Nutzer angezeigt.

Hinweis: Der Privacy Guard reduziert Datenschutzrisiken, ersetzt aber nicht die Verantwortung des Auftraggebers für rechtmäßige Eingabe, Zweckbindung, Datenminimierung und interne Nutzungsregeln.

3. Zutrittskontrolle

1. Betrieb der Plattform in professionellen Rechenzentrums- oder Cloud-Infrastrukturen mit physischer Zugangskontrolle.
2. Kein Betrieb produktiver Systeme auf privaten Endgeräten.
3. Zugriffe auf Hosting- oder Cloud-Verwaltungsoberflächen nur für berechtigte Personen.

4. Zugangskontrolle

1. Benutzerkonten mit individueller Authentifizierung.
2. Rollen- und Rechtekonzept für Administratoren, Nutzer und interne Support- und Betriebsrollen.
3. Starke Passwortrichtlinien beziehungsweise Integration geeigneter Identity-Provider, soweit verfügbar.
4. Administrative Zugänge nur nach Need-to-know-Prinzip; Nutzung zusätzlicher Schutzmechanismen wie Multi-Faktor-Authentifizierung, soweit technisch verfügbar.

5. Zugriffskontrolle

1. Mandantenbezogene Trennung von Kundendaten.
2. Beschränkung interner Zugriffe auf Produktivdaten auf Betrieb, Support, Sicherheit und Fehleranalyse.

3. Protokollierung sicherheitsrelevanter administrativer Zugriffe, soweit technisch möglich.
4. Regelmäßige Überprüfung interner Berechtigungen.

6. Weitergabekontrolle

1. Transportverschlüsselung für Datenübertragungen, zum Beispiel TLS oder HTTPS.
2. Einsatz des Privacy Guard vor Weitergabe an angebundene KI-Modelle.
3. Keine Weitergabe von Originalwerten und Re-Identifikationsmapping an externe KI-Modellanbieter, sofern nicht ausdrücklich vereinbart.
4. Dokumentation eingesetzter Unterauftragsverarbeiter und Drittlandübermittlungen.

7. Eingabekontrolle und Nachvollziehbarkeit

1. Technische Protokollierung ausgewählter System-, Sicherheits- und Administrationsereignisse.
2. Zeitstempel und Nutzer- oder Mandantenbezug, soweit für Sicherheit, Fehleranalyse und Nachweiszwecke erforderlich.
3. Begrenzung der Log-Inhalte auf erforderliche Informationen; keine unnötige Speicherung vollständiger Inhaltsdaten in technischen Logs.

8. Auftragskontrolle

1. Verarbeitung personenbezogener Daten nur auf dokumentierte Weisung des Auftraggebers.
2. Vertragliche Einbindung von Unterauftragsverarbeitern mit angemessenen Datenschutzpflichten.
3. Interne Prozesse zur Bearbeitung von Weisungen, Supportanfragen, Löschanfragen und Sicherheitsvorfällen.

9. Verfügbarkeitskontrolle

1. Backup- und Wiederherstellungskonzepte entsprechend Betriebsmodell.
2. Schutz vor unbeabsichtigtem Datenverlust durch geeignete Sicherungs- und Wiederherstellungsverfahren.
3. Monitoring zentraler Plattformkomponenten, soweit produktiv eingerichtet.
4. Incident-Response-Prozess für technische Störungen und Datenschutzvorfälle.

10. Trennungsgebot

1. Logische Trennung von Mandanten und Kundenumgebungen.
2. Trennung von Entwicklungs-, Test- und Produktivumgebungen, soweit technisch und organisatorisch umgesetzt.
3. Keine Verwendung produktiver Kundendaten für Entwicklungs- oder Demonstrationszwecke ohne Anonymisierung oder gesonderte Vereinbarung.

11. Verschlüsselung und Pseudonymisierung

1. Verschlüsselung der Datenübertragung.

2. Pseudonymisierung beziehungsweise Maskierung erkannter personenbezogener Angaben durch den Privacy Guard vor Weitergabe an KI-Modelle.
3. Schutz der Mapping-Tabelle zwischen Originalwerten und Platzhaltern innerhalb der Coveniq-Infrastruktur.
4. Optionale oder künftige Verschlüsselung ruhender Daten ist produktspezifisch zu dokumentieren.

12. Privacy Guard spezifische Maßnahmen

1. Automatisierte Analyse von Prompts und Inhaltsdaten auf personenbezogene Angaben.
2. Ersetzung erkannter Angaben durch typisierte Platzhalter, zum Beispiel [PERSON_1], [EMAIL_1], [PHONE_1], [ORG_1].
3. Rückübersetzung der Antwort an der Benutzeroberfläche, sofern Platzhalter in der Modellantwort enthalten sind.
4. Begrenzung externer Modellaufrufe auf mitigierte Inhalte, soweit technisch möglich und konfiguriert.
5. Fehler- und Qualitätsverbesserung des Privacy Guard anhand technischer Tests und Feedback, ohne Nutzung produktiver personenbezogener Daten zu Trainingszwecken, sofern nicht gesondert vereinbart.
6. Transparenter Hinweis: Vollständige Erkennung aller personenbezogenen oder vertraulichen Informationen kann technisch nicht garantiert werden.

13. Kein Modelltraining und keine Speicherung bei den Anbietern

1. Kundendaten werden nicht zum Training eigener oder fremder KI-Modelle verwendet, sofern dies nicht ausdrücklich gesondert vereinbart wurde.
2. Für die eingesetzten Anbieter OpenAI und Anthropic ist Zero Data Retention vereinbart und konfiguriert: übermittelte Inhalte werden dort nach Beantwortung der Anfrage nicht gespeichert.
3. Vor der Freischaltung eines weiteren Anbieters wird geprüft, ob eine gleichwertige Zusage besteht. Anderenfalls erfolgt keine Freischaltung ohne gesonderte Vereinbarung mit dem Auftraggeber.
4. Abweichungen sind dem Auftraggeber transparent zu machen und gesondert zu vereinbaren.

14. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

1. Datenminimierung bei Protokollierung und Supportzugriffen.
2. Rollenbasierte Zugriffsbeschränkung.
3. Produktseitige Hinweise zur verantwortungsvollen Nutzung von KI und personenbezogenen Daten.
4. Möglichkeit zur Definition kundenindividueller Nutzungsregeln und Datenkategorien, soweit produktspezifisch umgesetzt.

15. Überprüfung, Bewertung und Evaluierung

1. Regelmäßige Überprüfung zentraler Sicherheits- und Datenschutzmaßnahmen.

2. Dokumentation wesentlicher Änderungen an Privacy Guard, Unterauftragsverarbeitern und Hosting- oder Modellarchitektur.
3. Bearbeitung von Sicherheitsvorfällen, Schwachstellen und Datenschutzfeedback nach internem Prozess.
4. Angemessene Tests des Privacy Guard mit Testdaten und simulierten Anwendungsfällen.

16. Produktspezifische Angaben

Thema	Angabe
Hosting-Anbieter und Region	Vercel, Frankfurt, Deutschland (West-EU), eu-central-1 (fra1)
Datenbank und Speicher	Supabase, eu-central-1 (Frankfurt)
KI-Modellanbieter	Eingesetzt: OpenAI, Anthropic. Vorsorglich benannt, aber nicht freigeschaltet: Perplexity AI, Gamma AI, Mistral AI, KI-Modelle über AWS Bedrock.
Speicherfristen Chatverläufe	Bis zur Löschung durch den Nutzer oder zur Schließung des Accounts
Speicherfristen technische Logs	30 Tage
Multi-Faktor-Authentifizierung	Verfügbar