Security & Compliance

Wie CoGen KI-Implementierungen
DSGVO-konform und souverän betreibt.

Dokument	Security & Compliance Whitepaper
Version	1.0
Stand	April 2026
Herausgeber	Finology Systems GmbH (CoGen)
Kontakt	datenschutz@cogen.ai

1. Executive Summary

CoGen implementiert KI-Agenten, Chat- und Voicebots sowie Automatisierungen für Enterprises und KMU im deutschsprachigen Raum. Dieses Whitepaper fasst die wichtigsten Maßnahmen zu Datenschutz, Informationssicherheit, EU-AI-Act-Compliance und betrieblicher Resilienz zusammen, die wir in jedem Kundenprojekt anwenden.

Kernprinzipien: Hosting in Deutschland/EU, vertraglicher Ausschluss von Modelltraining mit Kundendaten, modell-agnostische Architektur (inkl. Self-Hosting-Option) sowie strikte Rollen- und Zugriffstrennung.

2. Acht Sicherheits-Säulen

Hosting in Deutschland

Primäre Verarbeitung in deutschen Rechenzentren (Frankfurt/Berlin) auf Basis von Hetzner, STACKIT oder Open Telekom Cloud. EU-Sovereign-Cloud-Optionen verfügbar.

DSGVO-konform

Auftragsverarbeitungsvertrag nach Art. 28 DSGVO, Verzeichnis von Verarbeitungs-tätigkeiten, TOMs nach Art. 32, Unterstützung bei Betroffenenrechten (Art. 15–22).

EU AI Act ready

Risikoklassifizierung jedes Use-Cases, Transparenzpflichten, menschliche Aufsicht und technische Dokumentation gemäß Verordnung (EU) 2024/1689.

Kein Training mit Kundendaten

Vertraglich ausgeschlossen für alle eingesetzten Modelle (OpenAI Enterprise, Anthropic, Azure OpenAI, Mistral, Llama). Zero-Retention-Modus aktivierbar.

Self-Hosted-Option

On-Premise- oder Private-Cloud-Deployment mit Open-Weights-Modellen (Llama, Mistral, Qwen) für maximale Datensouveränität.

Verschlüsselung

TLS 1.3 in Transit, AES-256 at Rest. Key-Management über HSM bzw. Cloud-KMS, kundenseitige Schlüssel (BYOK) auf Anfrage.

ISO 27001 & BSI-Grundschutz

Implementierung an ISO/IEC 27001:2022 und BSI IT-Grundschutz orientiert. Audit-fähige Dokumentation der Kontrollen.

Incident Response

24/7-Bereitschaft, Erstreaktion innerhalb von 4 Stunden, Meldung an Kunden und Aufsichtsbehörden im Rahmen von Art. 33/34 DSGVO.

3. Subprozessoren & Verarbeitungsregionen

Wir setzen ausschließlich Subprozessoren ein, die einen AV-Vertrag nach Art. 28 DSGVO bereitstellen und ihre Verarbeitung in der EU bzw. Deutschland anbieten. Die Auswahl wird projektspezifisch dokumentiert.

Anbieter	Zweck	Region
Hetzner Online GmbH	Compute, Storage	Deutschland (FRA/NBG)
STACKIT (Schwarz IT)	Sovereign Cloud, KI-Hosting	Deutschland
Open Telekom Cloud	Sovereign Cloud, Storage	Deutschland
Microsoft Azure (EU Data Boundary)	Azure OpenAI, Compute	EU
AWS (Frankfurt)	Compute, Managed Services (opt.)	Deutschland (eu-central-1)
OpenAI Ireland Ltd.	LLM-Inferenz (Enterprise, Zero-Retention)	EU / USA*
Anthropic Ireland Ltd.	LLM-Inferenz (Zero-Retention)	EU / USA*

* US-Transfer nur bei expliziter Freigabe und auf Basis EU-Standardvertragsklauseln (SCC 2021/914) inkl. Transfer Impact Assessment.

4. Datenlebenszyklus

Erhebung

Nur projektspezifisch notwendige Daten, Datensparsamkeit nach Art. 5 DSGVO.

Verarbeitung

Innerhalb dedizierter Mandanten, getrennt von anderen Kunden.

Speicherung

AES-256 verschlüsselt, Aufbewahrungsfristen vertraglich definiert.

Löschung

Auf Anforderung oder nach Vertragsende, dokumentiertes Löschkonzept.

5. Identitäts- & Zugriffsmanagement

Single-Sign-On (OIDC/SAML), Multi-Faktor-Authentifizierung, Role-Based Access Control sowie Principle of Least Privilege. Administrative Zugriffe werden protokolliert und revisionssicher 12 Monate aufbewahrt.

6. EU AI Act & Modellauswahl

Jeder Use-Case wird in die Risikoklassen des AI Act eingestuft (minimal, begrenzt, hoch). Hochrisiko-Anwendungen erhalten technische Dokumentation, Logging, Human-in-the-Loop und Conformity-Assessment. Wir sind modell-agnostisch und wählen das Modell nach Datenschutz, Latenz, Qualität und Kosten.

7. Incident Response & Verfügbarkeit

24/7-Bereitschaft mit Eskalationsplan, Erstreaktion ≤ 4 h, regelmäßige Backups, dokumentierter Wiederanlaufplan (RTO/RPO projektspezifisch). Meldepflichten nach Art. 33/34 DSGVO werden eingehalten.

8. Kontakt & Betroffenenrechte

Anfragen zu Auskunft, Berichtigung, Löschung, Einschränkung, Datenüber-tragbarkeit oder Widerspruch richten Sie bitte an **datenschutz@cogen.ai**. Wir antworten innerhalb von 30 Tagen gemäß Art. 12 Abs. 3 DSGVO. Beschwerderecht bei jeder Aufsichtsbehörde (Art. 77 DSGVO).

Verantwortlicher: Finology Systems GmbH, Robert-Bosch-Str. 19 a, 48153 Münster. Geschäftsführer: Stefan Chüo. HRB 22123 (Amtsgericht Münster).