

Technische und organisatorische Maßnahmen

Maßnahmen nach Art. 32 DSGVO zur Sicherheit der Verarbeitung

- **Auftragnehmer (Auftragsverarbeiter):** Nexode Consulting GmbH („Farion“, „Auftragnehmer“)
- **Anschrift:** Oberwallstraße 6, 10117 Berlin
- **Register / USt-IdNr.:** Amtsgericht Charlottenburg, HRB 234987 B · USt-IdNr. DE347774883
- **Vertreten durch:** Christoph Ebeling (Geschäftsführer)
- **Ansprechpartner Datenschutz:** Christoph Ebeling, info@nexode.de
- **Verantwortlicher (Auftraggeber):** [...]
- **Anschrift Auftraggeber:** [...]
- **Produkt:** Farion - KI-gestützte Application-Security-Plattform (ASPM/ SAST/SCA/DAST)
- **Stand / Version:** Stand: 22.06.2026, Version 1.2
- **Geltungsbereich:** Plattformbetrieb der Farion-Plattform, AWS-Region Frankfurt (eu-central-1), inklusive selbst betriebener Inferenz auf Farion-kontrollierten Kubernetes-Clustern

Hinweis zum Charakter und Stand der Maßnahmen: Diese TOM beschreiben das technische und organisatorische Sicherheitskonzept der Farion-Plattform nach dem Stand der Technik mit Stand 22.06.2026. Die TOM sind Bestandteil des zwischen den Parteien geschlossenen AVV und werden im Rahmen des kontinuierlichen Sicherheitsmanagements fortlaufend fortgeschrieben.

0. Vorbemerkung: Art der verarbeiteten Daten

Farion ist ein Werkzeug zur Sicherheitsanalyse von Software. Gegenstand der Verarbeitung im Auftrag des Kunden sind im Wesentlichen:

- Quellcode und Build-Artefakte des Kunden (Repositories, Abhängigkeits-Manifeste, Container-Images), die zum Scannen bereitgestellt werden;

- Scan-Konfiguration einschließlich verschlüsselter Zugangsdaten zu den Quellcode-Verwaltungssystemen des Kunden (SCM-Token) und optionaler DAST-Login-Daten;
- Konto- und Nutzungsdaten der für den Kunden handelnden Personen (Name, E-Mail-Adresse, Rolle, Authentifizierungs-Identifizier, Audit-Ereignisse).

Personenbezogene Daten entstehen primär aus den Konto- und Nutzungsdaten. Quellcode kann personenbezogene Daten enthalten, zum Beispiel in Kommentaren, Testdaten oder Konfiguration. Farion verarbeitet diese Daten ausschließlich zum Zweck der Sicherheitsanalyse und nicht inhaltlich-auswertend.

- Kundencode wird nicht zum Training oder Fine-Tuning von KI-Modellen verwendet.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle – Schutz vor unbefugtem physischem Zutritt

Die Plattform wird vollständig in der Cloud betrieben; es bestehen keine eigenen Rechenzentren des Auftragnehmers.

- Betrieb ausschließlich in zertifizierten Rechenzentren von Amazon Web Services in der Region Frankfurt (eu-central-1). AWS unterhält für diese Rechenzentren u. a. Zertifizierungen nach ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 und C5 (BSI); physische Zutrittskontrolle (Mehr-Faktor-Zugang, Videoüberwachung, Bewachung) liegt in der Verantwortung von AWS und ist durch diese Nachweise belegt.
- **Arbeitsplätze der Mitarbeiter:** Zugriff auf Produktivsysteme ausschließlich über gesicherte, personalisierte Endgeräte; keine Speicherung von Kundendaten auf lokalen Endgeräten.

1.2 Zugangskontrolle – Schutz vor unbefugter Systemnutzung

- Zentrale Identitäts- und Zugangsverwaltung auf Basis des Ory-Stacks (Kratos = Identitäten, Hydra = OAuth2/OIDC, Keto = Autorisierung, Oathkeeper = API-Gateway/Policy-Enforcement).
- Authentifizierung der Nutzer über E-Mail/Passwort sowie föderiertes Single Sign-On (OIDC) mit den Identity-Providern des Kunden (u. a. GitHub, GitLab, Google, Azure DevOps). OAuth2-Flows mit PKCE.

- Passwörter werden ausschließlich als gesalzene Hashes (über Ory Kratos) gespeichert; Klartext-Passwörter werden nicht persistiert.
- API-Gateway (Oathkeeper) erzwingt Authentifizierung und Autorisierung vor jedem Zugriff auf interne Dienste; nicht authentifizierte Anfragen werden abgewiesen.
- Dienst-zu-Dienst-Authentifizierung über kurzlebige, dienstspezifische Identitäten (AWS IRSA - IAM Roles for Service Accounts); keine geteilten, langlebigen Zugangsdaten zwischen Diensten.
- Administrativer Zugriff auf die Infrastruktur ausschließlich über personalisierte AWS-IAM-Identitäten mit Multi-Faktor-Authentifizierung.

1.3 Zugriffskontrolle — Schutz vor unbefugtem Datenzugriff (Least Privilege)

- Rollenbasierte Zugriffskontrolle (RBAC) über Ory Keto; Rollen (z. B. Admin, Manager, Member, Viewer) steuern den Zugriff auf Workspaces und Scan-Ergebnisse.
- **Need-to-know-Prinzip:** Jeder Microservice erhält über eine eigene IAM-Rolle ausschließlich die für seine Funktion erforderlichen Berechtigungen (S3-Buckets, Secrets, Datenbanken). Keine plattformweiten Sammelrechte.
- **Geheimnisverwaltung:** Zugangsdaten (Datenbank-Credentials, OAuth-Secrets, SMTP) werden nicht im Code oder in Git gehalten, sondern über External Secrets aus dem AWS Secrets Manager zur Laufzeit in den Cluster injiziert (Aktualisierungsintervall 1 h). CI/CD authentifiziert über OIDC ohne langlebige Zugangsdaten.
- Mandantenbezogene Zugangsdaten (SCM-Token, DAST-Login-Daten) werden vor der Persistierung asymmetrisch verschlüsselt (RSA-OAEP, SHA-256) und nur zur Laufzeit des jeweiligen Scans entschlüsselt.

1.4 Trennungskontrolle — Mandantentrennung

- **Logische Mandantentrennung auf Basis von Workspaces:** Jeder Kunde/Mandant ist einer eindeutigen Workspace-ID zugeordnet; sämtliche Zugriffe werden serverseitig gegen die Workspace-Zugehörigkeit autorisiert (Keto).
- Pro-Workspace-Authentifizierungsrichtlinien (zulässige Identity-Provider, E-Mail-Domänen-Regeln) verhindern mandantenübergreifenden Kontozugriff.

- Trennung der Verarbeitungsdomänen über getrennte Datenbank-Cluster pro Dienst (Identität, Anwendungsdaten, Scan-Orchestrierung, Schwachstellen-Service, DAST-Ergebnisse).
- Trennung von Test-, Staging- und Produktivumgebung auf Ebene getrennter Cluster-Overlays.

1.5 Pseudonymisierung und Verschlüsselung

- Verschlüsselung ruhender und übertragener Daten siehe Abschnitt 1.6 und 2.1.
- Mandanten-Zugangsdaten werden ausschließlich verschlüsselt gespeichert (siehe 1.3).
- Wo für die Analyse möglich, werden Bezeichner statt direkter Personenbezüge geführt; KI-Eingaben werden auf den für die Sicherheitsanalyse erforderlichen Kontext beschränkt.

1.6 Verschlüsselung ruhender Daten (Encryption at Rest)

- **Block-Speicher (EBS gp3):** Alle Datenträger der Datenbank- und Anwendungs-Pods sind mit AWS-KMS verschlüsselt.
- **Objektspeicher (S3):** Quellcode-Archive, Property-Graphen, SBOM-Daten und Datenbank-Backups werden serverseitig verschlüsselt (SSE-KMS).
- **Kubernetes-Secrets:** Verschlüsselung der Secrets im etcd über AWS-KMS-Envelope-Encryption.
- Schlüsselverwaltung über AWS KMS; Rotation gemäß AWS-Vorgaben.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle — Verschlüsselung übertragener Daten (Encryption in Transit)

- Externe Verbindungen (Browser/API zum System) ausschließlich über TLS (HTTPS), terminiert am AWS Load Balancer / Ingress.
- **Nachrichtenbus (Apache Kafka, Strimzi):** Dienst-zu-Dienst-Kommunikation über mutual TLS (mTLS) mit X.509-Client-Zertifikaten, mindestens TLS 1.2.
- Datenbankverbindungen TLS-gesichert; Zugangsdaten ausschließlich aus dem Secrets-Management.

- KI-Inferenz erfolgt über TLS-gesicherte interne Dienste innerhalb der Farion-kontrollierten Kubernetes-Umgebung; ergänzend eingesetzte Amazon-Bedrock-Aufrufe erfolgen über TLS-gesicherte AWS-Schnittstellen innerhalb der AWS-Region Frankfurt.

2.2 Eingabekontrolle — Nachvollziehbarkeit von Änderungen

- Audit-Protokollierung sicherheitsrelevanter und datenverändernder Vorgänge (z. B. Statusänderungen, Freigaben, Patch-Vorgänge) in dedizierten Audit-Tabellen mit Zeitstempel und auslösender Identität.
- Kubernetes-Control-Plane-Audit-Logs (API-Server, Authenticator) aktiviert und nach AWS CloudWatch mit umgebungsabhängiger Aufbewahrung exportiert.
- Zentrale, nachvollziehbare Telemetrie (Logs, Traces, Metriken) über OpenTelemetry; Korrelation über Trace-IDs.
- **GitOps-Prinzip:** Alle Infrastruktur- und Konfigurationsänderungen erfolgen versioniert über Git (Flux); Änderungen sind nachvollziehbar und durchlaufen Review.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DSGVO)

3.1 Verfügbarkeitskontrolle

- **Hochverfügbare Datenbanken (CloudNativePG):** Betrieb mit mehreren Instanzen je Cluster, synchroner/asynchroner Replikation und Pod-Anti-Affinity zur Verteilung auf unterschiedliche Knoten.
- **Mehrere Availability Zones:** Verteilung der Knoten über mehrere AWS-AZs in der Region Frankfurt.
- Automatische Backups der Datenbanken (Barman Cloud) mit kontinuierlichem WAL-Archiving nach S3; planmäßige Sicherungen mit definierter Aufbewahrung (derzeit 15 Tage).
- **Selbstheilung und Autoscaling:** Kubernetes (EKS) startet ausgefallene Workloads automatisch neu; Karpenter skaliert die Knotenkapazität bedarfsgerecht.
- **Schutz vor Datenverlust im Nachrichtenbus:** replizierte Kafka-Topics; Verarbeitung mit „Commit nach erfolgreicher Veröffentlichung“ und Dead-Letter-Behandlung fehlerhafter Nachrichten.

3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c)

- Point-in-Time-Recovery der Datenbanken aus WAL-Archiven (RPO im Minutenbereich durch kontinuierliches WAL-Archiving).
- **Wiederherstellung per GitOps:** Cluster- und Anwendungszustand sind deklarativ in Git beschrieben und vollständig reproduzierbar neu aufbaubar.
- Skriptgestützte, weitgehend automatisierte Wiederherstellungsprozesse (Runbooks und Automatisierungs-Skripte) für Datenbank-Recovery; dadurch reproduzierbarer Ablauf mit minimalem manuellem Eingriff.
- Periodische Erprobung der Wiederherstellung (Restore-Drills).

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

4.1 Datenschutz- und Informationssicherheits-Management

- Regelmäßige Überprüfung und Fortschreibung dieser TOM.
- **Eigenanwendung der Sicherheitsanalyse:** Farion scannt seine eigene Codebasis im CI/CD (SAST/SCA) und betreibt damit kontinuierliche Schwachstellen-Erkennung in eigener Sache.
- **Abhängigkeits- und Image-Sicherheit:** Schwachstellen-Service auf Basis öffentlicher Feeds (NVD, OSV, CISA, EPSS); Container-Image-Scanning im Registry-Push.
- **Weitgehend automatisierte Betriebsprozesse:** Deployment, Sicherung, Wiederherstellung und Skalierung erfolgen skriptgestützt bzw. deklarativ über GitOps. Die Automatisierung reduziert manuelle Eingriffe und sorgt für reproduzierbare, nachvollziehbare Abläufe.

4.2 Auftrags-/Weisungskontrolle

- Verarbeitung personenbezogener Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen (geregelt im AVV).
- Unterauftragsverarbeiter ausschließlich gemäß AVV; jeder Unterauftragsverarbeiter ist vertraglich (DPA/SCC) gebunden.
- Mitarbeiter sind auf das Datengeheimnis verpflichtet und unterliegen Vertraulichkeitsvereinbarungen.

4.3 Incident-Response- und Datenpannen-Management

- Zentrales Monitoring und Alerting (Prometheus/Grafana) zur frühzeitigen Erkennung von Störungen und Auffälligkeiten.
- Telemetrie/Observability (Logs, Traces, Metriken) wird selbst gehostet in der eigenen AWS-Umgebung betrieben; es kommt kein externer Observability-Anbieter zum Einsatz.
- Prozess zur Erkennung, Bewertung und Meldung von Datenschutzverletzungen; Unterstützung des Verantwortlichen bei dessen Meldepflichten nach Art. 33/34 DSGVO. Meldung an den Verantwortlichen unverzüglich nach Bekanntwerden oder begründetem Verdacht, spätestens innerhalb von 48 Stunden (gemäß AVV).

4.4 Datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO – Privacy by Design/Default)

- **Datenminimierung:** KI-Eingaben werden auf den für die Sicherheitsanalyse erforderlichen Codekontext beschränkt; kein Training oder Fine-Tuning auf Kundendaten.
- Mandantentrennung und Least-Privilege als architektonische Grundvoreinstellung (siehe 1.3/1.4).
- Verschlüsselung als Standard für übertragene und ruhende Daten.
- Netzwerksegmentierung der Cluster-Workloads über Ingress- und Egress-Policies.

5. Umgang mit Kunden Quellcode und KI-Inferenz (produktspezifisch)

Für eine Sicherheits-Scanning-Plattform ist der Umgang mit bereitgestelltem Quellcode der zentrale Vertrauensanker. Daher gelten gesondert:

- **Verbleib in der AWS-Umgebung:** Quellcode, abgeleitete Property-Graphen und Scan-Ergebnisse werden ausschließlich innerhalb der AWS-Region Frankfurt verarbeitet und gespeichert.
- **Primäre KI-Inferenz:** Die KI-gestützte Bewertung erfolgt primär über ein von Farion selbst betriebenes Inferenz-Backend auf von Farion kontrollierten Kubernetes-Clustern. Kundendaten, Quellcode, Scan-Kontexte und Analyseergebnisse werden nicht zum Training oder Fine-Tuning von KI-Modellen verwendet.

- **Ergänzende KI-Inferenz:** Farion behält sich vor, in bestimmten Fällen ergänzend auf Amazon Bedrock in der AWS-Region Frankfurt (eu-central-1) zurückzugreifen. Es werden keine öffentlichen, separat angebundenen LLM-APIs Dritter für Kundendaten verwendet. Keine Cross-Region-Inference für Kundendaten.
- Verschlüsselte Übermittlung und Speicherung des Quellcodes (TLS in transit, SSE-KMS at rest).
- **Löschung nach Zweckerreichung:** Quellcode-Archive werden nach Abschluss der Analyse gelöscht. Nach Beendigung der zugrunde liegenden Beauftragung bzw. Nutzung werden personenbezogene Kundendaten gemäß AVV gelöscht oder zurückgegeben. Ein durchgängiger Lösch-Workflow inklusive Workspace-Löschung ist umgesetzt.

6. Schlussbestimmungen

- Diese TOM werden bei wesentlichen Änderungen der Verarbeitung oder der technischen Infrastruktur aktualisiert.
- Im Zweifel gehen die Regelungen des AVV vor.