

Auftragsverarbeitungsvertrag (AVV)

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

- **Verantwortlicher:** [...]
- **Anschrift:** [...]
- **Vertretung Verantwortlicher:** [...]
- **Auftragsverarbeiter:** Nexode Consulting GmbH („Farion“, „Auftragsverarbeiter“)
- **Anschrift:** Oberwallstraße 6, 10117 Berlin · AG Charlottenburg HRB 234987 B · USt-IdNr. DE347774883
- **Vertreten durch:** Christoph Ebeling (Geschäftsführer)
- **Gegenstand:** Sicherheitsanalyse von Software über die Farion-Plattform (Farion ASPM)
- **Laufzeit:** für die Dauer der zugrunde liegenden Beauftragung bzw. Nutzung der Farion-Plattform
- **Stand / Version:** Stand: 22.06.2026, Version 1.2

Präambel: Der Verantwortliche beauftragt den Auftragsverarbeiter mit der Durchführung von Sicherheitsanalysen über die Plattform Farion. Dabei kann der Auftragsverarbeiter im Auftrag und nach Weisung des Verantwortlichen personenbezogene Daten verarbeiten. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien nach Art. 28 DSGVO für die Dauer der zugrunde liegenden Beauftragung bzw. Nutzung der Farion-Plattform.

§ 1 Gegenstand und Dauer

- Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Verantwortlichen im Zusammenhang mit dem Betrieb der Farion-Plattform zur Sicherheitsanalyse von Software (Application Security Posture Management).

- Die nähere Beschreibung von Art, Umfang, Zweck der Verarbeitung, der Art der Daten und der Kategorien betroffener Personen ergibt sich aus Anlage 1.
- Die Dauer dieses Vertrags entspricht der Laufzeit der zugrunde liegenden Beauftragung bzw. Nutzung der Farion-Plattform. Pflichten zur Löschung und zur Verschwiegenheit bestehen über das Vertragsende hinaus fort.

§ 2 Art und Zweck der Verarbeitung

- Der Auftragsverarbeiter verarbeitet die vom Verantwortlichen bereitgestellten oder angebundenen technischen Daten ausschließlich zur Durchführung der vereinbarten Sicherheitsanalysen, insbesondere zur Analyse von Quellcode, Abhängigkeiten, Softwarekomponenten, Sicherheitsrisiken, Schwachstellen, Reachability, Exploitability, Dataflows und Security Findings.
- Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters findet nicht statt. Kundendaten werden nicht zum Training von KI-Modellen verwendet.
- Die Verarbeitung erfolgt ausschließlich innerhalb der Europäischen Union (AWS-Region Frankfurt, eu-central-1). Einzelheiten regelt Anlage 1.

§ 3 Weisungsrecht des Verantwortlichen

- Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Verantwortlichen, es sei denn, er ist gesetzlich zu einer Verarbeitung verpflichtet.
- Weisungen werden in der Regel über die Funktionen der Plattform sowie in Textform erteilt. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.
- Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies dem Verantwortlichen unverzüglich mit. Er ist berechtigt, die Durchführung der betreffenden Weisung auszusetzen, bis sie bestätigt oder geändert wird.

§ 4 Pflichten des Auftragsverarbeiters

- **Vertraulichkeit:** Der Auftragsverarbeiter verpflichtet die mit der Verarbeitung befassten Personen auf Vertraulichkeit (Art. 28 Abs. 3 lit. b, Art. 29 DSGVO), soweit sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
- **Technische und organisatorische Maßnahmen:** Der Auftragsverarbeiter setzt die in Anlage 2 (TOM) beschriebenen Maßnahmen nach Art. 32 DSGVO um und hält sie während der Vertragslaufzeit aufrecht.
- **Zugriff nach Need-to-know:** Ein Zugriff des Auftragsverarbeiters auf Kundendaten erfolgt nur, soweit dies für Betrieb, Sicherheit, Fehleranalyse oder Support erforderlich ist. Inhaltliche Zugriffe auf Kundendaten erfolgen grundsätzlich nur auf Anfrage oder mit Zustimmung des Verantwortlichen und nach dem Need-to-know-Prinzip.
- **Unterstützung:** Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des Zumutbaren bei der Wahrung der Betroffenenrechte (Art. 12–23 DSGVO) sowie bei den Pflichten aus Art. 32–36 DSGVO.
- **Mitteilung:** Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich nach Bekanntwerden oder bei begründetem Verdacht einer Verletzung des Schutzes personenbezogener Daten.

§ 5 Technische und organisatorische Maßnahmen

- Die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sind in Anlage 2, dem gesondert beigefügten Dokument „Technische und organisatorische Maßnahmen (TOM)“, dokumentiert und Bestandteil dieses Vertrags.
- Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter ist berechtigt, alternative, gleichwertige Maßnahmen umzusetzen, sofern das Schutzniveau nicht unterschritten wird.

§ 6 Unterauftragsverarbeiter

- Der Verantwortliche stimmt dem Einsatz der in Anlage 3 genannten Unterauftragsverarbeiter zu. Für diese bereits benannten Unterauftragsverarbeiter gilt die Zustimmung mit Abschluss dieses Vertrags als erteilt.

- Beabsichtigt der Auftragsverarbeiter einen Wechsel oder die Hinzunahme eines weiteren Unterauftragsverarbeiters, informiert er den Verantwortlichen vorab in Textform. Der Verantwortliche kann einem Wechsel aus wichtigem datenschutzrechtlichem Grund innerhalb von 30 Tagen widersprechen. Bei Unterauftragsverarbeitern, die für die Erbringung der Plattform zwingend erforderlich sind, kann ein berechtigter Widerspruch dazu führen, dass die Leistung gegenüber dem Verantwortlichen nicht oder nicht weiter erbracht werden kann. In diesem Fall steht den Parteien ein Sonderkündigungsrecht zu.
- Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf ein Datenschutzniveau, das den Anforderungen dieses Vertrags entspricht (Art. 28 Abs. 4 DSGVO).

§ 7 Betroffenenrechte

- Wendet sich eine betroffene Person mit Ansprüchen auf Auskunft, Berichtigung, Löschung oder Einschränkung unmittelbar an den Auftragsverarbeiter, leitet dieser das Ersuchen unverzüglich an den Verantwortlichen weiter.
- Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen der technischen Möglichkeiten und unter Berücksichtigung der Art der Verarbeitung bei der Erfüllung der Betroffenenrechte (Art. 15–22 DSGVO). Soweit eine direkte Berichtigung oder Löschung in abgeleiteten technischen Artefakten, Audit-Logs oder Backups nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, erfolgt die Umsetzung durch Löschung des zugrunde liegenden Datensatzes, Sperrung, Überschreibung im regulären Löschyklus oder andere angemessene technische Maßnahmen.

§ 8 Nachweise und Kontrollen

- Der Auftragsverarbeiter weist dem Verantwortlichen die Einhaltung seiner Pflichten auf Anforderung in geeigneter Weise nach: durch die Dokumentation der Maßnahmen in den TOM, durch ein ausgefülltes Selbstauskunfts-/Sicherheitsfragebogen, durch vorhandene eigene Prüfberichte (z. B. Penetrationstests zu Farion) sowie durch Zertifizierungen und Nachweise der eingesetzten Cloud-Infrastruktur (u. a. AWS ISO 27001/C5, SOC 2). Die AWS-Nachweise decken die Infrastrukturebene; seine eigene Organisations- und Anwendungsebene weist der Auftragsverarbeiter gesondert nach.

- Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO erforderlich sind, und ermöglicht sowie unterstützt Prüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten unabhängigen Prüfer. Prüfungen erfolgen grundsätzlich zunächst dokumentenbasiert oder remote, mit angemessener Vorankündigung, während üblicher Geschäftszeiten und unter Wahrung der Vertraulichkeit, der Sicherheit der Plattform sowie der Rechte anderer Kunden. Ein Zugriff auf Daten anderer Mandanten, Quellcode des Auftragsverarbeiters, interne Bewertungslogiken, Modelle, Scoring-Logiken oder sonstige Geschäftsgeheimnisse findet nicht statt, soweit dies für den Nachweis der datenschutzrechtlichen Pflichten nicht zwingend erforderlich ist.

§ 9 Meldung von Datenschutzverletzungen

- Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden oder bei begründetem Verdacht durch eine zuständige Stelle des Auftragsverarbeiters, spätestens innerhalb von 48 Stunden, und stellt die zur Erfüllung der Pflichten aus Art. 33/34 DSGVO erforderlichen Informationen bereit. Eine Erstmeldung erfolgt auch bei noch unvollständigem Sachverhalt; ergänzende Informationen werden unverzüglich nachgereicht. Die Meldung stellt kein Anerkenntnis einer Rechtspflichtverletzung dar.

§ 10 Löschung und Rückgabe

- Personenbezogene Kundendaten werden so lange gespeichert, wie der Verantwortliche diese in der Plattform vorhält oder die Speicherung für Betrieb, Nachvollziehbarkeit, Sicherheit oder die vereinbarte Sicherheitsanalyse erforderlich ist.
- Nach Beendigung der zugrunde liegenden Beauftragung bzw. Nutzung löscht der Auftragsverarbeiter personenbezogene Kundendaten oder gibt vom Verantwortlichen in die Plattform eingebrachte personenbezogene Daten, soweit technisch verfügbar, in einem angemessenen Standardformat zurück. Die Löschung bzw. Rückgabe erfolgt innerhalb von 14 Tagen nach Beendigung oder auf dokumentierte Weisung des Verantwortlichen, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Der Auftragsverarbeiter

bestätigt die Löschung auf Verlangen in Textform unter Angabe des Datums.

- Der AVV begründet keinen Anspruch auf Herausgabe interner Analyseartefakte, Property Graphs, Dataflows, Modelle, Prompts, Heuristiken, Scoring-/Bewertungslogiken oder sonstiger Geschäftsgeheimnisse des Auftragsverarbeiters.
- Daten in rollierenden Sicherungskopien (Backups) werden mit dem regulären Sicherungszyklus überschrieben (derzeit: WAL-Archive bis 15 Tage, Nachrichtenbus bis 7 Tage); sie werden bis dahin nicht aktiv genutzt, die Vertraulichkeitspflichten bestehen fort. Serverlogs sowie Tracking-/Cookie-bezogene Daten werden mit einer Retention von je 30 Tagen gespeichert.

§ 11 Schlussbestimmungen

- Bei Widersprüchen gehen die Regelungen dieses Vertrags den Regelungen des Hauptvertrags in Bezug auf den Datenschutz vor. Anlage 1 (Beschreibung der Verarbeitung), Anlage 2 (Technische und organisatorische Maßnahmen) und Anlage 3 (Unterauftragsverarbeiter) sind Bestandteil dieses Vertrags.
- Änderungen und Ergänzungen bedürfen der Textform; dies gilt auch für die Änderung dieses Textformerfordernisses.
- Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit zulässig, Berlin.
- Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anlage 1 – Beschreibung der Verarbeitung

Gegenstand / Zweck: Durchführung von Sicherheitsanalysen (Quellcode, Abhängigkeiten, Softwarekomponenten, Sicherheitsrisiken, Schwachstellen, Reachability, Exploitability, Dataflows, Security Findings) über die Farion-Plattform.

Art der Daten: Der Auftragsverarbeiter verarbeitet primär technische Daten, insbesondere Quellcode, Code-Ausschnitte, Repository-Metadaten, Dependency-Daten, SBOMs, Konfigurationsdaten, Scan-Konfigurationen, SCM-/OAuth-Token und sonstige verschlüsselt gespeicherte Zugangsdaten zu Quellcode-Verwaltungssystemen, optionale DAST-Login-Daten, DAST-Requests/-Responses, technische Scan-Logs, Scan-Ergebnisse, Security

Findings, CVE-/CWE-Zuordnungen sowie daraus abgeleitete Risiko- und Analyseinformationen. Zusätzlich werden Nutzerkonten, Rollen, E-Mail-Adressen, IP-Adressen, Audit-Logs und technische Zugriffsdaten verarbeitet, soweit dies für Betrieb, Sicherheit, Authentifizierung, Nachvollziehbarkeit und Support erforderlich ist.

Kategorien betroffener Personen: Nutzerinnen und Nutzer der Plattform auf Seiten des Verantwortlichen (Mitarbeitende, technische Ansprechpartner); mittelbar Personen, deren personenbezogene Daten unbeabsichtigt in bereitgestellten Repositories oder Artefakten enthalten sein können.

Hinweis zu personenbezogenen Daten im Quellcode: Farion ist nicht darauf ausgelegt, personenbezogene Daten im Quellcode oder in technischen Artefakten zu verarbeiten. Das Vorhandensein personenbezogener Daten in vom Verantwortlichen bereitgestellten Repositories, Konfigurationsdateien, Kommentaren, Testdaten oder Logs kann jedoch nicht ausgeschlossen werden. Der Verantwortliche ist dafür verantwortlich, keine personenbezogenen Daten oder sonstigen nicht erforderlichen sensiblen Inhalte in die Plattform einzubringen, soweit dies für den vereinbarten Zweck nicht erforderlich ist.

Ort der Verarbeitung: EU — AWS-Region Frankfurt (eu-central-1). Keine Cross-Region-Inference für Kundendaten.

Mandantentrennung: Die Mandantentrennung erfolgt im Standardbetrieb logisch auf Anwendungsebene. Für Enterprise-Kunden kann ab einer gesondert zu vereinbarenden Nutzerzahl ein separates Deployment bereitgestellt werden, sofern dies vertraglich vereinbart ist.

Anlage 2 — Technische und organisatorische Maßnahmen

Es gelten die technischen und organisatorischen Maßnahmen gemäß dem gesondert beigelegten Dokument „Technische und organisatorische Maßnahmen (TOM)“ (Stand 22.06.2026). Diese TOM bilden Anlage 2 dieses Vertrags.

Anlage 3 – Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung	Rechtsgrundlage / Transfer
Amazon Web Services EMEA SARL	Hosting (Compute, Speicher, Datenbanken, Objektspeicher, Backups)	EU — Frankfurt (eu-central-1)	AWS-DPA, EU-Standardvertragsklauseln
Amazon Bedrock (Teil von AWS)	Ergänzende KI-Inferenz zur Schwachstellenbewertung, soweit eingesetzt	EU — Frankfurt (eu-central-1)	AWS-DPA; keine Trainingsnutzung der Eingaben
Amazon SES (Teil von AWS)	Versand von Konto- und Benachrichtigungs-E-Mails	EU — Frankfurt (eu-central-1)	AWS-DPA, EU-Standardvertragsklauseln