VERTRAGSVORLAGE · STAND 07/2026

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO · Vorlage für Kunden von Audit Strike

Hinweis zur Verwendung
Diese Vorlage bildet die Standardregelungen ab, die wir mit Kunden von Audit Strike vereinbaren. Bitte ergänzen Sie die Angaben zu Ihrem Unternehmen und senden Sie uns das Dokument unterzeichnet zurück. Branchenspezifische Anforderungen (z. B. § 203 StGB, KRITIS, BAIT/VAIT) stimmen wir auf Anfrage individuell mit Ihnen ab. Stand 07/2026, Änderungen vorbehalten.

Parteien

Verantwortlicher (im Folgenden „Auftraggeber“):

[Firma des Auftraggebers, Anschrift, Registergericht/Registernummer, USt-IdNr., vertretungsberechtigte Person]

Auftragsverarbeiter (im Folgenden „Auftragsverarbeiter“ oder „Audit Strike“):

Infosec Technologie GmbH, Frankfurterstraße 229, 63263 Neu-Isenburg, Deutschland — Amtsgericht Offenbach am Main, HRB 58513, USt-IdNr. DE459387705, vertreten durch die Geschäftsführung. Telefon 069 66 3 666 30, E-Mail mbazra@infosectec.de.

Audit Strike ist ein Angebot der Infosec Technologie GmbH.

Präambel

Der Auftraggeber nutzt die Compliance-Plattform „Audit Strike“ zur Verwaltung seines Informationssicherheits-Managementsystems (ISMS). Im Rahmen dieser Nutzung verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Sinne von Art. 28 DSGVO.

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand der Verarbeitung ist die Bereitstellung der SaaS-Plattform Audit Strike zur Verwaltung von Compliance-Anforderungen (ISO 27001, TISAX, BSI Grundschutz, BSI C5, DSGVO, NIS-2 u.a.), Evidenzen, Richtlinien, Audits und KI-gestützten Vorschlägen.

(2) Die Verarbeitung erfolgt für die Dauer des zwischen den Parteien geschlossenen Hauptvertrags und endet automatisch mit dessen Beendigung.

(3) Nach Vertragsende werden die Daten gemäß § 8 dieses Vertrags gelöscht oder zurückgegeben.

§ 2 Art und Zweck der Verarbeitung

(1) Verarbeitungszweck: Bereitstellung der vertraglich geschuldeten SaaS-Funktionalität (Speicherung, Strukturierung, Zuordnung, Versionierung, Export von Compliance-Daten und Nachweisen).

(2) Art der Verarbeitung: Erheben, Erfassen, Organisation, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung im Rahmen der Plattform, Abgleich, Verknüpfung, Einschränken, Löschen.

(3) Soweit der Auftraggeber die KI-gestützte Analyse nutzt, werden Titel und Textinhalt hochgeladener Dokumente an den vom Auftragsverarbeiter eingesetzten Anbieter des Sprachmodells übermittelt (siehe Anlage 2).

§ 3 Art der Daten und Kategorien betroffener Personen

(1) Folgende Datenkategorien werden verarbeitet:

- Stammdaten der Nutzer des Auftraggebers (Name, E-Mail-Adresse, Rolle, Abteilung)
- Authentifizierungsdaten (gehashte Passwörter, Refresh-Tokens, Session-Daten)
- Audit- und Aktivitätsprotokolle (wer hat wann was im System gemacht)
- Inhalte hochgeladener Dokumente (Policies, Verträge, Nachweise) — diese können personenbezogene Daten Dritter enthalten, deren Verarbeitung in der Verantwortung des Auftraggebers liegt
- Konfigurations- und Nutzungsdaten der Plattform

(2) Kategorien betroffener Personen:

- Mitarbeiter und Beauftragte des Auftraggebers
- ggf. dritte Personen, deren Daten in vom Auftraggeber hochgeladenen Dokumenten enthalten sind (z.B. in Mitarbeiterrichtlinien, Lieferantenverträgen, Auditprotokollen)

§ 4 Pflichten des Auftragsverarbeiters

Audit Strike verpflichtet sich:

- die Daten ausschließlich im Rahmen des Vertrags und nach dokumentierten Weisungen des Auftraggebers zu verarbeiten;
- die Vertraulichkeit aller mit der Datenverarbeitung beauftragten Personen sicherzustellen (Verpflichtung auf das Datengeheimnis);
- die in § 5 genannten technischen und organisatorischen Maßnahmen einzuhalten;
- den Auftraggeber unverzüglich zu informieren, wenn eine Weisung gegen Datenschutzvorschriften verstößt;
- den Auftraggeber bei der Erfüllung von Betroffenenrechten (Art. 15–21 DSGVO) angemessen zu unterstützen — insbesondere durch die im Tool bereitgestellten Datenexport- und Löschfunktionen;
- den Auftraggeber unverzüglich (spätestens 24 Stunden nach Kenntnis) über Datenschutzverletzungen zu informieren (Art. 33 DSGVO);
- an Datenschutz-Folgenabschätzungen mitzuwirken (Art. 35–36 DSGVO);
- einen Datenschutzbeauftragten zu benennen, sofern gesetzlich erforderlich;
- auf Verlangen einen Nachweis über die Einhaltung der Pflichten nach Art. 28 DSGVO zu erbringen.

§ 5 Technische und organisatorische Maßnahmen

Audit Strike trifft die in Anlage 1 zu diesem Vertrag beschriebenen technischen und organisatorischen Maßnahmen (TOM) gemäß Art. 32 DSGVO.

§ 6 Unterauftragsverarbeiter

(1) Der Auftraggeber stimmt der Beauftragung der in Anlage 2 aufgeführten Unterauftragsverarbeiter zu.

(2) Audit Strike informiert den Auftraggeber mindestens 30 Tage im Voraus über beabsichtigte Änderungen der Unterauftragsverarbeiter und gewährt ihm ein Widerspruchsrecht aus berechtigtem Grund.

(3) Audit Strike schließt mit jedem Unterauftragsverarbeiter einen Vertrag mit Datenschutzpflichten ab, die denen dieses AVV mindestens gleichwertig sind.

§ 7 Datenübermittlung in Drittländer

(1) Eine Verarbeitung personenbezogener Daten außerhalb der EU/des EWR findet nur statt, soweit dies in Anlage 2 ausdrücklich aufgeführt ist.

(2) Soweit eine Übermittlung in Drittländer erfolgt, geschieht dies ausschließlich auf Grundlage geeigneter Garantien gemäß Art. 46 DSGVO (insbesondere EU-Standardvertragsklauseln in der jeweils aktuellen Fassung).

§ 8 Löschung und Rückgabe von Daten

(1) Nach Beendigung des Hauptvertrags löscht Audit Strike sämtliche im Auftrag verarbeiteten Daten innerhalb von 30 Tagen, sofern keine gesetzliche Aufbewahrungspflicht besteht.

(2) Auf Verlangen des Auftraggebers stellt Audit Strike vor der Löschung einen vollständigen Datenexport im JSON-Format zur Verfügung (vgl. die Funktion „DSGVO-Export“ in der Anwendung).

(3) Die endgültige Löschung wird auf Anforderung dokumentiert.

§ 9 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, sich von der Einhaltung der Pflichten dieses Vertrags zu überzeugen — insbesondere durch Einholung von Auskünften, Einsicht in Zertifikate und vorhandene Audit-Berichte (z.B. ISO 27001, SOC 2 wenn vorhanden) sowie durch Vor-Ort-Kontrollen nach angemessener Vorankündigung.

(2) Audit Strike stellt dem Auftraggeber auf Anfrage die in der Anwendung verfügbaren Audit-Logs zur Verfügung (Funktion „Datenschutz“ !’ „Audit-Log“).

(3) Vor-Ort-Kontrollen finden in der Regel nicht häufiger als einmal pro Jahr statt und werden mindestens 30 Tage im Voraus angekündigt. Sie dürfen den Geschäftsbetrieb nicht unangemessen stören.

§ 10 Haftung und Schadensersatz

Es gelten die Regelungen des Hauptvertrags. Im Übrigen haften die Parteien gegenüber Betroffenen nach Maßgabe des Art. 82 DSGVO.

§ 11 Schlussbestimmungen

(1) Bei Widerspruch gehen die Regelungen dieses AVV den Regelungen des Hauptvertrags vor, soweit es um Datenschutzfragen geht.

(2) Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(3) Änderungen und Ergänzungen bedürfen der Schriftform (auch elektronisch in qualifizierter Form gemäß eIDAS).

(4) Anwendbares Recht: deutsches Recht. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragsverarbeiters (63263 Neu-Isenburg).

Ort, Datum: _____

_____

Auftraggeber (Verantwortlicher)

_____

Auftragsverarbeiter — Infosec Technologie GmbH

ANLAGE 1

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO

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

Zutrittskontrolle:

- Hosting in zertifizierten Rechenzentren (Hetzner: ISO 27001, ISO 9001, ISO 14001; AWS-Regionen wenn genutzt: ISO 27001/27017/27018, SOC 1/2/3, C5)
- Physischer Zugang nur für berechtigtes Rechenzentrumspersonal

Zugangskontrolle:

- Authentifizierung über JWT mit Refresh-Token-Rotation
- Mindestpasswortlänge und -komplexität gemäß BSI-Empfehlung
- Schutz gegen automatisiertes Ausprobieren von Passwörtern durch Begrenzung der Anmeldeversuche

Zugriffskontrolle:

- Rollenbasiertes Berechtigungssystem (RBAC): tenant_admin, isms_manager, auditor, control_owner, reviewer, viewer
- Mandantentrennung auf Datenbank- und Storage-Ebene (jedes Objekt enthält die Tenant-ID; Storage-Schlüssel sind tenant-präfixiert)
- Defense-in-Depth-Prüfung beim Lesen von Dateien

Pseudonymisierung / Verschlüsselung:

- Verschlüsselung aller Verbindungen mit TLS 1.2+ (HTTPS)
- Verschlüsselung der Daten im Ruhezustand auf Storage- und Datenbank-Ebene
- Passwörter ausschließlich als bcrypt-Hashes gespeichert
- Keine Speicherung von API-Keys im Klartext

2. Integrität

- Eingabevalidierung an allen API-Endpoints (class-validator)
- Datei-Hashes (SHA-256) für Evidenz-Uploads
- Vollständiges Audit-Log für alle datenmodifizierenden Aktionen
- Versionsverlauf für Controls, Evidenzen und Policies

3. Verfügbarkeit und Belastbarkeit

- Automatisierte Sicherungen der Datenbank; dokumentiertes Wiederherstellungsverfahren
- Redundante Speicherung der Object-Storage-Daten beim Storage-Anbieter
- Überwachung der Anwendung (Fehler- und Leistungsüberwachung, Health-Checks)
- Entkoppelte Hintergrundverarbeitung über Job-Warteschlangen

4. Verfahren zur regelmäßigen Überprüfung

- Interne Sicherheits-Reviews im Rahmen des Entwicklungsprozesses; externe Penetrationstests sind vorgesehen
- Automatisierte Testsuite in der Bereitstellungskette (CI/CD)
- Regelmäßige Aktualisierung der eingesetzten Softwarebibliotheken
- Dokumentierte Verfahren für Sicherung, Wiederherstellung und Rücknahme von Releases

ANLAGE 2

Liste der Unterauftragsverarbeiter (Stand 07/2026)

Anbieter	Standort / Region	Zweck
Hetzner Online GmbH	Deutschland (EU)	Object-Storage für hochgeladene Dokumente und Nachweise
Railway Corp.	EU-Region; Anbietersitz USA	Betrieb der Anwendungsschnittstelle, der Datenbank und der Warteschlange
Vercel Inc.	USA, mit Auslieferungsknoten in der EU	Betrieb der Weboberfläche
OpenAI Ireland Ltd.	Irland (EU); Verarbeitung auch in den USA	KI-gestützte Dokumentenanalyse — siehe Hinweis unten
Stripe Payments Europe, Ltd.	Irland (EU); Konzernverarbeitung auch in den USA	Abwicklung von Abonnements und Zahlungen
Sentry (Functional Software, Inc.)	USA; EU-Region wählbar	Fehler- und Leistungsüberwachung ohne personenbezogene Inhalte
Mailserver des Hosting-Anbieters	EU	Versand transaktionaler E-Mails (Anmeldung, Einladungen, Erinnerungen)

Hinweis zur KI-gestützten Dokumentenanalyse

Die KI-gestützte Analyse erfolgt derzeit über OpenAI; Vertragspartner für den Europäischen Wirtschaftsraum ist OpenAI Ireland Ltd. Übermittelt werden der Titel und der ausgelesene Textinhalt der hochgeladenen Dokumente sowie die Bezeichnungen der Anforderungen, denen sie zugeordnet werden sollen. Nach Angaben des Anbieters werden Inhalte, die über seine Programmierschnittstelle übermittelt werden, nicht zum Training seiner Modelle verwendet.

Ein Wechsel des Anbieters wird dem Auftraggeber gemäß § 6 Abs. 2 dieses Vertrags mindestens 30 Tage im Voraus angekündigt. Auf Wunsch kann die Analyse über einen anderen Anbieter oder einen vom Auftraggeber betriebenen Dienst erfolgen oder für den Auftraggeber entfallen.

Für Verarbeitungen außerhalb der EU/des EWR gelten die EU-Standardvertragsklauseln in der Fassung des Beschlusses (EU) 2021/914.