

Vereinbarung zur Auftragsverarbeitung (AVV)

nach Art. 28 DSGVO · Version 1.0 · Stand: 18.07.2026 · scancompliance.de/avv

Diese Vereinbarung wird gemäß § 12 der Allgemeinen Geschäftsbedingungen mit Vertragsschluss Bestandteil des Vertrags zwischen dem Kunden — nachfolgend „**Verantwortlicher**“ — und

Neujeffski Software Development
Lars Neujeffski
Hanninghof 24, 48249 Dülmen, Deutschland
E-Mail: lars.neujeffski@neujeffski.com

— nachfolgend „**Auftragsverarbeiter**“ —, soweit der Kunde im Rahmen der Plattform scancompliance.de personenbezogene Daten im Auftrag verarbeiten lässt. Einer gesonderten Unterzeichnung bedarf es nicht (elektronisches Format, Art. 28 Abs. 9 DSGVO); auf Wunsch stellt der Auftragsverarbeiter eine unterzeichnete Fassung bereit.

§ 1 Gegenstand, Dauer und Abgrenzung

(1) Der Auftragsverarbeiter betreibt die Plattform scancompliance.de und erbringt für den Verantwortlichen Website-Compliance-Analysen (DSGVO/TDDDG/BFSG-Prüfungen) einschließlich Berichtserstellung, Beweissicherung und zugehöriger Nebenleistungen gemäß Hauptvertrag (AGB in der bei Vertragsschluss gültigen Fassung).

(2) Die Laufzeit dieser Vereinbarung folgt der Laufzeit des Hauptvertrags.

(3) **Abgrenzung:** Soweit der Auftragsverarbeiter eigene vertragliche Leistungen gegenüber dem Kunden erbringt (Kontoführung, Abrechnung, eigene Qualitätssicherung) oder der Kunde ausschließlich eigene Domains prüfen lässt, handelt der Anbieter als eigener Verantwortlicher; diese Verarbeitungen richten sich nach der Datenschutzerklärung. Auftragsverarbeitung liegt insbesondere vor, wenn der Kunde Domains Dritter (z. B. als Agentur oder Kanzlei für deren Mandanten bzw. Endkunden) scannen lässt oder Scan-Ergebnisse mit personenbezogenen Daten Dritter über die Plattform verwaltet.

§ 2 Art, Zweck und Ort der Verarbeitung

Zweck: Automatisierte Prüfung öffentlich erreichbarer Websites auf Rechtskonformität; Erstellung, Speicherung und Bereitstellung von Prüfberichten und Beweismaterial. **Art:** Erheben (Abruf öffentlicher Webinhalte), Speichern, Auswerten (einschließlich KI-gestützter Analyse), Bereitstellen, Löschen. **Ort:** Rechenzentren in Deutschland (Hetzner Online GmbH); KI-Analyse vorrangig auf eigener Infrastruktur des Auftragsverarbeiters in Deutschland. Ausnahmen: Anlage 2.

§ 3 Betroffene Personen und Datenarten

Betroffene: Besucher und Betreiber der gescannten Websites (z. B. im Impressum genannte Personen), Ansprechpartner des Verantwortlichen sowie ggf. dessen Endkunden. **Datenarten:** Inhalte öffentlich erreichbarer Webseiten (können personenbezogene Daten enthalten, z. B. Impressumsangaben); technische Scan-Artefakte

(Screenshots, HTTP-Logs, Cookies und Identifier der Zielseite); vom Verantwortlichen übermittelte Domain-Listen und Ansprechpartner-Daten. Besondere Kategorien (Art. 9 DSGVO) sind nicht Gegenstand der Beauftragung; sollten solche Daten auf gescannten Seiten öffentlich enthalten sein, werden sie ausschließlich als Bestandteil des Beweismaterials gespeichert.

§ 4 Weisungsrecht

(1) Verarbeitung ausschließlich auf dokumentierte Weisung des Verantwortlichen (Art. 28 Abs. 3 lit. a DSGVO); die Nutzung der Plattformfunktionen (Scan-Start, Löschung, Export) gilt als dokumentierte Weisung. (2) Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich und darf die Ausführung bis zur Klärung aussetzen.

§ 5 Vertraulichkeit

Alle zur Verarbeitung befugten Personen sind zur Vertraulichkeit verpflichtet (Art. 28 Abs. 3 lit. b DSGVO) oder unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht.

§ 6 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft die in Anlage 1 zusammengefassten Maßnahmen nach Art. 32 DSGVO und entwickelt sie fortlaufend weiter; das Schutzniveau darf nicht unterschritten werden. (2) Das vollständige TOM-Dokument wird auf Anfrage bereitgestellt; wesentliche Änderungen werden unter scancompliance.de/avv veröffentlicht.

§ 7 Unterauftragsverarbeiter

(1) Der Verantwortliche genehmigt allgemein den Einsatz der in Anlage 2 genannten Unterauftragsverarbeiter (Art. 28 Abs. 2 Satz 2 DSGVO). (2) Beabsichtigte Änderungen teilt der Auftragsverarbeiter mindestens 30 Tage vor Wirksamwerden in Textform mit (E-Mail an die Konto-Adresse); der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund widersprechen; bei Widerspruch besteht beidseitig ein Sonderkündigungsrecht des Hauptvertrags. (3) Mit jedem Unterauftragsverarbeiter werden Verträge geschlossen, die den Pflichten dieser Vereinbarung entsprechen; bei Drittlandtransfers werden geeignete Garantien nach Kapitel V DSGVO sichergestellt (Angemessenheitsbeschluss, insbesondere EU-US Data Privacy Framework, oder Standardvertragsklauseln), siehe Anlage 2.

§ 8 Unterstützungs- und Mitwirkungspflichten

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten Mitteln bei der Beantwortung von Betroffenenanfragen (Art. 12–23 DSGVO) sowie bei den Pflichten aus Art. 32–36 DSGVO (Art. 28 Abs. 3 lit. e, f DSGVO). (2) Direkt eingehende Anfragen betroffener Personen werden unverzüglich an den Verantwortlichen weitergeleitet.

§ 9 Meldung von Verletzungen

Verletzungen des Schutzes personenbezogener Daten meldet der Auftragsverarbeiter dem Verantwortlichen unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntniserlangung, an die im Kundenkonto hinterlegte

E-Mail-Adresse — mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit verfügbar; Nachmeldungen sind zulässig.

§ 10 Löschung und Rückgabe

(1) Nach Ende der Beauftragung werden alle im Auftrag verarbeiteten Daten gelöscht oder nach Wahl des Verantwortlichen zurückgegeben, soweit keine gesetzlichen Aufbewahrungspflichten bestehen (Art. 28 Abs. 3 lit. g DSGVO). (2) Plattformseitig gilt: Vom Kunden gelöschte Domains und Scans werden nach einer Karenzzeit von 14 Tagen endgültig und automatisiert gelöscht; Berichte und Beweis-Bundles kann der Kunde zuvor exportieren.

§ 11 Nachweise und Kontrollen

(1) Der Auftragsverarbeiter stellt alle zum Nachweis der Pflichten aus Art. 28 DSGVO erforderlichen Informationen zur Verfügung (Art. 28 Abs. 3 lit. h DSGVO), zuvorderst durch diese Vereinbarung, Anlage 1, Anlage 2 sowie Nachweise der Rechenzentrums-Betreiber (Hetzner: ISO-27001-zertifizierte Rechenzentren). (2) Vor-Ort-Kontrollen sind nach Terminabstimmung (14 Tage Vorlauf) während üblicher Geschäftszeiten zulässig, ohne konkreten Anlass höchstens einmal jährlich; Kosten trägt der Verantwortliche. Statt einer Vor-Ort-Kontrolle können aussagekräftige Selbstauskünfte oder Zertifikate beigebracht werden.

§ 12 Haftung, Schlussbestimmungen

(1) Die Haftung richtet sich nach Art. 82 DSGVO und den Regelungen des Hauptvertrags. (2) Änderungen dieser Vereinbarung bedürfen der Textform; es gilt deutsches Recht. (3) Bei Widersprüchen geht in datenschutzrechtlichen Fragen diese Vereinbarung dem Hauptvertrag vor.

Anlage 1 — Technische und organisatorische Maßnahmen (Zusammenfassung)

- **Zugangs-/Zugriffskontrolle:** SSH nur mit Public-Key + fail2ban; KI-Server ohne öffentliche Erreichbarkeit (privates VPN/WireGuard); Datenbank nicht öffentlich erreichbar; rollenbasierte Trennung Kunden-/Adminzugänge.
- **Mandantentrennung:** Logische Trennung aller Kundendaten auf Datenbankebene.
- **Transportverschlüsselung:** TLS für sämtliche externen Verbindungen (HTTPS, SMTP mit STARTTLS, SSH/VPN).
- **Integrität:** Versionierter Code mit Pflicht-Testpipeline vor jedem Deployment; Berichte mit SHA-256-Hash und RFC-3161-Zeitstempel; revisionsfähiges Guthaben-Ledger.
- **Verfügbarkeit:** Blue/Green-Deployment mit Health-Check; automatische Bereinigung hängender Verarbeitungen; tägliche Qualitäts-Regression mit Beweis-Audit.
- **Löschkonzept:** Automatisierte tägliche Löschroutinen (Retention, 14-Tage-Löschung, E-Mail-Scan-Bereinigung); dedizierter Auskunftsprozess.
- **Datensparsamkeit:** CookieLOSE eigene Reichweitenmessung; Scans ausschließlich öffentlich erreichbarer Inhalte.

Anlage 2 — Unterauftragsverarbeiter (Stand 18.07.2026)

Unterauftragsverarbeiter	Zweck	Ort	Drittland-Garantie
Hetzner Online GmbH, Gunzenhausen (DE)	Server-Hosting (Anwendung, Datenbank, Mailserver)	Deutschland	— (EU/EWR)
Google Ireland Ltd. / Google LLC (Gemini API)	KI-Textanalyse der Scan-Inhalte (nur öffentliche Webinhalte des Scan-Ziels)	EU / USA	EU-US Data Privacy Framework
Anthropic PBC (USA)	KI-Zweitprüfung einzelner Scans (Qualitätssicherung)	USA	EU-US Data Privacy Framework
Stripe Payments Europe Ltd. / Stripe Inc.	Zahlungsabwicklung	EU / USA	EU-US DPF / Standardvertragsklauseln
Cloudflare Inc. (Turnstile)	Bot-Schutz bei der Registrierung	EU / USA	EU-US Data Privacy Framework
Serper (serper.dev)	Suchmaschinen-Abfragen Wettbewerber- Recherche (keine Kundenkontodaten)	USA	Standardvertragsklauseln
freeTSA.org	RFC-3161-Zeitstempel für Beweis- Bundles (nur Hashwerte)	Deutschland	— (EU/EWR)