

Auftragsverarbeitungsvertrag

nach Art. 28 DSGVO — modular mit produktspezifischen Anlagen
Stand: Mai 2026

Vertragsparteien

Auftraggeber (Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO):

Name/Firma: _____

Anschrift: _____

Vertretungsberechtigter: _____

E-Mail: _____

— nachstehend „Auftraggeber“ —

Auftragnehmer (Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO):

Daniel Wesseling, Die Netzhandwerker
Achtenbuhr 12, 48599 Gronau (Westfalen)
E-Mail: support@netzhandwerker.de

— nachstehend „Auftragnehmer“ —

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand dieses Vertrages sind die Verarbeitungstätigkeiten, die der Auftragnehmer im Auftrag des Auftraggebers durchführt. Die konkreten Verarbeitungstätigkeiten ergeben sich aus den angekreuzten produktspezifischen Anlagen (2A bis 2G) sowie aus dem zugrunde liegenden Hauptvertrag (z. B. Fernwartungs-, KI-Telefon-, Newsletter- oder Sensorik-Auftrag).

(2) Die Dauer dieses Vertrages richtet sich nach der Laufzeit des zugrunde liegenden Hauptvertrages. Der Vertrag endet automatisch mit Beendigung des Hauptvertrages, sofern nicht in den Anlagen abweichende Regelungen getroffen werden.

§ 2 Konkretisierung des Auftragsinhalts

(1) **Art und Zweck der Verarbeitung:** ergibt sich aus der jeweiligen Anlage und dem Hauptvertrag.

(2) **Art der personenbezogenen Daten und Kategorien betroffener Personen:** wird in der jeweiligen Anlage konkret benannt.

(3) **Verarbeitung erfolgt ausschließlich in Mitgliedsstaaten der Europäischen Union oder des EWR.** Drittlandtransfers erfolgen nur an die in der jeweiligen Anlage genannten Unterauftragnehmer auf den dort genannten Rechtsgrundlagen (DPF, Standardvertragsklauseln, ergänzende Schutzmaßnahmen).

§ 3 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Die im Hauptvertrag und in den Anlagen niedergelegten Verarbeitungstätigkeiten gelten als Weisung.

(2) Weisungen können in Textform (E-Mail genügt) erteilt werden. Wesentliche Änderungen müssen schriftlich bestätigt werden.

(3) Hält der Auftragnehmer eine Weisung für rechtswidrig, teilt er dies dem Auftraggeber unverzüglich mit (Art. 28 Abs. 3 S. 3 DSGVO).

§ 4 Pflichten des Auftragnehmers

(1) **Vertraulichkeit (Art. 28 Abs. 3 lit. b DSGVO):** Der Auftragnehmer verpflichtet alle zur Verarbeitung befugten Personen schriftlich auf die Vertraulichkeit. Diese Verpflichtung besteht auch nach Beendigung des Vertrages fort. In Berufsgeheimnisbereichen (Arztpraxen, Kanzleien, Therapeuten) erfolgt zusätzlich eine Verpflichtung nach § 203 Abs. 4 StGB.

(2) **Technische und organisatorische Maßnahmen (Art. 32 DSGVO):** Der Auftragnehmer trifft die in Anlage 1 (TOM) beschriebenen Maßnahmen.

(3) **Unterstützung des Auftraggebers (Art. 28 Abs. 3 lit. e + f DSGVO):** bei Anfragen Betroffener, Datenschutz-Folgenabschätzungen, Konsultation der Aufsichtsbehörde und Datenschutzverletzungen.

(4) **Meldung von Datenschutzverletzungen:** Der Auftragnehmer meldet dem Auftraggeber unverzüglich, spätestens jedoch **innerhalb von 24 Stunden** nach Bekanntwerden, jede Verletzung des Schutzes personenbezogener Daten.

(5) **Rückgabe/Löschung nach Vertragsende (Art. 28 Abs. 3 lit. g DSGVO):** Nach Abschluss der Verarbeitungstätigkeit hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, soweit nicht gesetzliche Aufbewahrungspflichten entgegenstehen.

(6) **Kontrollnachweise:** Der Auftragnehmer stellt dem Auftraggeber die erforderlichen Informationen zur Verfügung, um Einhaltung dieses Vertrages nachzuweisen.

§ 5 Unterauftragnehmer

(1) Der Auftraggeber genehmigt mit Vertragsschluss den Einsatz der in Anlage 3 genannten Unterauftragnehmer. Wesentliche Änderungen werden dem Auftraggeber mindestens 30 Tage vorab in Textform mitgeteilt. Der Auftraggeber kann der Änderung innerhalb dieser Frist aus wichtigem Grund widersprechen; in diesem Fall sind beide Parteien zur außerordentlichen Kündigung berechtigt.

(2) Der Auftragnehmer schließt mit allen Unterauftragnehmern vertragliche Regelungen, die mindestens die in diesem Vertrag genannten Pflichten enthalten (Art. 28 Abs. 4 DSGVO).

§ 6 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, die Einhaltung der Datenschutzpflichten und die getroffenen technischen und organisatorischen Maßnahmen zu kontrollieren. Die Kontrolle erfolgt nach Vorankündigung von mindestens 14 Tagen während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs.

(2) Statt einer Vor-Ort-Kontrolle kann der Auftragnehmer einen aktuellen Prüfbericht (z. B. SOC 2, ISO 27001) eines anerkannten Prüfers vorlegen.

§ 7 Haftung

Es gelten die Haftungsregelungen des Art. 82 DSGVO. Im Innenverhältnis haftet der Auftragnehmer dem Auftraggeber nur für Schäden, die durch eigene schuldhaftige Pflichtverletzung verursacht wurden. Im Übrigen gelten die Haftungsregelungen des Hauptvertrages.

§ 8 Schlussbestimmungen

(1) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Gronau (Westfalen), sofern der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

(2) Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform (Textform genügt, E-Mail ausreichend). Dies gilt auch für die Aufhebung dieses Schriftformerfordernisses.

(3) Sollte eine Bestimmung dieses Vertrages unwirksam sein, bleiben die übrigen Bestimmungen davon unberührt. Die unwirksame Bestimmung ist durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen am nächsten kommt.

Unterschriften

Ort, Datum

Ort, Datum

Auftraggeber (Stempel/Unterschrift)

Daniel Wesseling, Die Netzhandwerker

Vertragsbestandteile und angekreuzte Anlagen

Bestandteil dieses Vertrages sind der vorstehende Hauptvertrag sowie die nachfolgend angekreuzten Anlagen. Bitte kreuzen Sie die für Ihre Leistung relevanten Anlagen an:

☐ Anlage 1	Technische und organisatorische Maßnahmen (TOM)	verbindlich für alle Leistungen
☐ Anlage 2A	IT-Fernwartung und IT-Support	
☐ Anlage 2B	KI-Telefonassistent (Julia / White-Label)	
☐ Anlage 2C	KI-Chat-Assistent (FINN / White-Label)	
☐ Anlage 2D	Hosting / SaaS / Wartung von KI-Lösungen	
☐ Anlage 2E	Newsletter-Tool	
☐ Anlage 2F	Sensorik / Monitoring (spuerwerk©, linkx©, naturwerk©, fermentwerk©)	
☐ Anlage 2G	Sicherheits-Audit / Penetrationstest	
☐ Anlage 3	Unterauftragnehmer-Liste	verbindlich für alle Leistungen

Die vollständigen Texte der Anlagen 2A–2G sowie der Unterauftragnehmer-Liste (Anlage 3) sind im Folgenden enthalten und können auch jederzeit unter <https://netzhandwerker.de/av-vertrag> eingesehen werden.

Anlage 1 — Technische und organisatorische Maßnahmen (TOM)

gem. Art. 32 DSGVO

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

Zutrittskontrolle: Geschäftsräume Achtenbuhr 12, 48599 Gronau, mit Schließsystem und Alarmanlage; Server-Hosting bei All-Inkl (ISO/IEC 27001-zertifiziertes Rechenzentrum) und Hetzner Online GmbH (ISO/IEC 27001 + 9001 zertifiziert).

Zugangskontrolle: Zugang zu IT-Systemen ausschließlich für berechtigtes Personal über persönliche Benutzerkonten mit starken Passwörtern (mind. 14 Zeichen) und Multi-Faktor-Authentifizierung bei kritischen Systemen (E-Mail, Server-Admin, Auftragsverarbeiter-Konsolen, Banking).

Zugriffskontrolle: Berechtigungskonzept nach Need-to-Know-Prinzip; Logging aller administrativen Zugriffe.

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

Weitergabekontrolle: TLS 1.2+ für alle externen Verbindungen; verschlüsselte SSH-Verbindungen für Server-Administration; bei Mail-Versand DKIM + SPF + DMARC.

Eingabekontrolle: Audit-Logs für Server-Login und Änderungen kritischer Konfigurationen mit min. 30 Tagen Retention.

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

Verfügbarkeitskontrolle: Tägliche automatisierte Backups; Monitoring der kritischen Dienste; Notfall-Wiederherstellungsplan.

Schutz gegen Schadsoftware: aktuelle Betriebssysteme + Sicherheitsupdates auf allen Arbeitsplätzen; Web Application Firewall (Cloudflare) auf der Website.

4. Verfahren zur regelmäßigen Überprüfung

Datenschutz-Management: jährliche Überprüfung der TOM, Verarbeitungsverzeichnis (Art. 30 DSGVO) wird aktuell gehalten.

Auftragsverwaltung: AVV mit allen Auftragsverarbeitern abgeschlossen; siehe Anlage 3.

5. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

Pseudonymisierung: Newsletter-Engine speichert nach Abmeldung gehashte E-Mail-Adressen (SHA-256 mit Salt) zur Vermeidung versehentlicher Wieder-Anmeldung; FINN-Chat speichert nur gehashte IP-Ableitung.

Verschlüsselung at Rest: Server-Datenträger bei Hetzner und All-Inkl in physisch gesicherten Rechenzentren; bei besonders sensiblen Daten zusätzliche Anwendungs-Ebene-Verschlüsselung möglich.

6. Vorfälle und Wiederherstellung

Incident-Response: Verfahrensanweisung für Datenschutzverletzungen; Meldung an Auftraggeber innerhalb von 24 Stunden; Meldung an Aufsichtsbehörde durch den Verantwortlichen innerhalb von 72 Stunden (Art. 33 DSGVO).

7. Aktuelle TOM-Übersicht

Eine ausführliche und stets aktuelle TOM-Übersicht finden Sie unter <https://netzhandwerker.de/datenschutz/tom>. Diese Übersicht ist Bestandteil dieser Anlage.

Anlage 2A — IT-Fernwartung und IT-Support

Datenarten: Alle Daten, die auf dem fernzuwartenden System sichtbar werden (typisch: Geräte- und Konfigurationsdaten, Anwendungs-Inhalte, ggf. Kunden- oder Mitarbeiterdaten des Auftraggebers).

Kategorien betroffener Personen: Mitarbeiter, Kunden, Lieferanten des Auftraggebers (je nach System-Inhalt).

Eingesetzte Unterauftragnehmer: TeamViewer Germany GmbH (Göppingen, DE), AnyDesk Software GmbH (Karlsruhe, DE), Microsoft Ireland Operations Ltd. (Quick Assist), Google Ireland Ltd. (Chrome Remote Desktop), All-Inkl (Friedersdorf, DE).

Drittlandtransfer: Nur bei Chrome Remote Desktop oder Quick Assist möglich — Google und Microsoft sind beide DPF-zertifiziert (Active-Status), ergänzend EU-Standardvertragsklauseln.

Speicherdauer: Sitzungs-Logs werden nicht persistent gespeichert; Tickets max. 36 Monate nach Abschluss.

Anlage 2B — KI-Telefonassistent (Julia / White-Label)

Datenarten: Rufnummer (sofern übermittelt), Audio des Anrufs, Transkript, Anliegen-Text, gewünschter Rückrufzeitpunkt, Name. Bei Branchen-Use-Cases (Praxis, Kanzlei, Therapie) zusätzlich Branchen-Datenarten — diese werden technisch auf die für den Use-Case erforderlichen Felder begrenzt.

Kategorien betroffener Personen: Anrufer (potenzielle Patienten, Mandanten, Kunden des Auftraggebers).

Eingesetzte Unterauftragnehmer: Vapi Inc. (Dover/USA), Deepgram Inc. (West Hollywood/USA), ElevenLabs Inc. (New York/USA), Anthropic PBC (San Francisco/USA), easybell GmbH (Berlin/DE).

Drittlandtransfer: ElevenLabs ist EU-U.S. DPF-zertifiziert (Active). Vapi, Deepgram und Anthropic sind nicht DPF-zertifiziert — Übermittlung auf Grundlage EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) plus ergänzende Schutzmaßnahmen: Anthropic verfügt über ISO 27001:2022, ISO/IEC 42001:2023 und SOC 2 Type II; Vapi über SOC 2; Deepgram über SOC 2 und einen EU-Endpunkt (api.eu.deepgram.com).

Speicherdauer: Audio und Transkript bei den Auftragsverarbeitern max. 90 Tage; bei uns nur strukturierter Rückrufvorgang bis abgeschlossene Bearbeitung plus gesetzliche Aufbewahrungsfristen.

Besonderheiten: Schweigepflicht (§ 203 StGB): Bei Einsatz in Berufsgeheimnis-Branchen (Praxen, Kanzleien, Therapeuten) werden die Auftragsverarbeiter vertraglich nach § 203 Abs. 4 StGB verpflichtet. **EU**

AI Act: Anrufer werden zu Beginn jedes Gesprächs als mit einer KI sprechend identifiziert (Art. 50).

Anlage 2C — KI-Chat-Assistent (FINN / White-Label)

Datenarten: Chat-Inhalt, Zeitstempel, gehashte Ableitung der IP-Adresse (kein Rückschluss möglich). Bei Lead-Abschluss zusätzlich Name, E-Mail, Telefon, ggf. Unternehmen.

Kategorien betroffener Personen: Website-Besucher des Auftraggebers, ggf. Lead-Interessenten.

Eingesetzte Unterauftragnehmer: Anthropic PBC (San Francisco/USA), Hetzner Online GmbH (Falkenstein/Nürnberg, DE), Cloudflare Inc. (San Francisco/USA), All-Inkl (Friedersdorf, DE).

Drittlandtransfer: Anthropic: SCC + ergänzende Schutzmaßnahmen wie unter 2B. Cloudflare: DPF Active + SCC. Hetzner und All-Inkl: EU-Verarbeitung.

Speicherdauer: Unterhaltungsverläufe max. 90 Tage; Lead-Anfragen entsprechend Kontaktformular-Frist (12 Monate ohne Vertragsschluss, ansonsten gesetzliche Aufbewahrungsfristen).

Anlage 2D — Hosting / SaaS / Wartung

Datenarten: Produkt-abhängig; im Einzelfall in einer ergänzenden Verarbeitungsbeschreibung konkretisiert.

Kategorien betroffener Personen: Endnutzer des SaaS-Produkts des Auftraggebers; je nach Anwendungsfall Mitarbeiter, Kunden oder Mitglieder.

Eingesetzte Unterauftragnehmer: All-Inkl (Friedersdorf, DE), Hetzner Online GmbH (DE), Cloudflare Inc. (USA).

Drittlandtransfer: Cloudflare: DPF Active + SCC. Hosting selbst in Deutschland.

Speicherdauer: Mandantenfähigkeit: Logische Trennung pro Kunden-Instanz; getrennte API-Keys; kein gemeinsames Logging über Mandantengrenzen hinweg.

Anlage 2E — Newsletter-Tool

Datenarten: E-Mail-Adresse, Themenpräferenzen, Versandzeitplan, Layout, Tonalität, Länge, optionale Stichwörter, Zeitzone, IP/User-Agent/Zeitstempel der Anmeldung (Einwilligungsnachweis).

Kategorien betroffener Personen: Newsletter-Abonnenten des Auftraggebers.

Eingesetzte Unterauftragnehmer: Hetzner Online GmbH (DE — Engine), All-Inkl (DE — SMTP-Relay), Anthropic PBC (USA — KI für Inhaltserstellung, ohne Empfänger-Bezug).

Drittlandtransfer: Anthropic: SCC + ergänzende Schutzmaßnahmen wie unter 2B. Anthropic erhält ausschließlich abstrakte Auswahlparameter (Themenkategorien, Layout, Ton, Länge), keine E-Mail-Adressen oder personenbezogenen Daten.

Speicherdauer: Aktive Konfiguration für Dauer des Abonnements; nach Abmeldung Konfiguration max. 30 Tage; Einwilligungs-Protokoll max. 36 Monate.

Besonderheiten: Tracking: Kein Open-Tracking, keine personalisierten Tracking-Links, keine Zählpixel. Versand-Statistik nur aggregiert.

Anlage 2F — Sensorik / Monitoring (spuerwerk©, linkx©, naturwerk©, fermentwerk©)

Datenarten: Messwerte (Temperatur, Luftqualität, CO₂, Bewegung u.a.). Personenbezug nur, wenn die Messstelle räumlich oder zeitlich Personen zuordenbar ist.

Kategorien betroffener Personen: Personen in dem überwachten Raum (ggf. Mitarbeiter, Besucher, Schüler — abhängig vom Aufstellort).

Eingesetzte Unterauftragnehmer: Hetzner Online GmbH (DE — Daten-Backend), All-Inkl (DE — Frontend), Cloudflare Inc. (USA — CDN).

Drittlandtransfer: Cloudflare: DPF Active + SCC. Sonst EU.

Speicherdauer: Rohdaten pro Sensor max. 24 Monate (anpassbar); aggregierte Reports bis 5 Jahre; Lösch-/Export-Optionen jederzeit.

Anlage 2G — Sicherheits-Audit / Penetrationstest

Datenarten: Konfigurations- und Schwachstellendaten, ggf. extrahierte Test-Credentials (zerstörungsfrei), Logs.

Kategorien betroffener Personen: Mitarbeiter des Auftraggebers (bei Phishing-Simulationen); Endnutzer der zu testenden Anwendung (bei Web-Pentests).

Eingesetzte Unterauftragnehmer: In der Regel keine; bei vorab freigegebenen externen Scannern werden diese namentlich im Test-Protokoll genannt.

Drittlandtransfer: Keiner; alle Test-Aktivitäten erfolgen innerhalb der EU.

Speicherdauer: Rohdaten max. 30 Tage nach Test-Ende; Abschlussbericht beim Auftraggeber gemäß seiner Aufbewahrungsregeln.

Besonderheiten: Detailbedingungen: Siehe „Besondere Bedingungen für Sicherheits-Audits und Penetrationstests“ unter <https://netzhandwerker.de/agb-sicherheits-audit>.

Anlage 3 — Liste der Unterauftragnehmer

Eine stets aktuelle Liste der Unterauftragnehmer wird im Internet unter <https://netzhandwerker.de/datenschutz> (Abschnitt 9 Drittlandtransfer) gepflegt. Die folgende Übersicht ist Stand Mai 2026.

Anbieter	Sitz / Server	Zweck	Transfer-Grundlage
All-Inkl	DE	Web-Hosting, SMTP-Relay	EU
Hetzner Online GmbH	DE (Falkenstein/Nürnberg)	Server, Proxy, Engines	EU
Cloudflare Inc.	USA	CDN, DDoS-Schutz	DPF Active + SCC
TeamViewer Germany GmbH	DE	Fernwartung	EU
AnyDesk Software GmbH	DE	Fernwartung	EU
Microsoft Ireland Operations	IE / USA (Konzern)	Quick Assist	DPF Active + SCC
Google Ireland Ltd.	IE / USA (Konzern)	Chrome Remote Desktop, Analytics, Maps	DPF Active + SCC
Cal.com, Inc.	USA / EU-Datenregion	Terminbuchung	EU-Datenregion (kein Transfer)
Anthropic PBC	USA	LLM (Julia, FINN, Newsletter)	SCC + ISO 27001 + SOC 2
Vapi Inc.	USA	Voice-Plattform	SCC + SOC 2
Deepgram Inc.	USA (EU-Endpunkt verfügbar)	Spracherkennung	SCC + SOC 2
ElevenLabs Inc.	USA	Sprachsynthese	DPF Active + SCC
easybell GmbH	DE	SIP-Trunk Telefonie	EU
Stripe Payments Europe	IE	Zahlungsabwicklung (optional)	EU

Eine Aktualisierung dieser Liste wird in der Datenschutzerklärung (Abschnitt 9 Drittlandtransfer) gepflegt und ist verbindlich. Wesentliche Änderungen werden dem Auftraggeber mindestens 30 Tage vorab in Textform mitgeteilt; der Auftraggeber hat in diesem Fall die in § 5 dieses Vertrages genannten Widerspruchsrechte.