

AUFTRAGSVERARBEITUNGSVERTRAG

Nach Art. 28 Abs. 3 DSGVO

Version 1.2 | Stand: März 2026

VERTRAGSPARTEIEN

Auftraggeber (Verantwortlicher):

[AUFTRAGGEBER NAME]

[AUFTRAGGEBER ADRESSE]

[AUFTRAGGEBER PLZ ORT]

— im Folgenden „Auftraggeber“ —

Auftragnehmer (Auftragsverarbeiter):

k3i GmbH

Kolonnenstr. 8

10827 Berlin

Vertreten durch die Geschäftsführer:

Joe-Philipp Kohnert, Martin Lohmann, Martin Klepsch

— im Folgenden „Auftragnehmer“ —

PRÄAMBEL

Der Auftragnehmer erbringt für den Auftraggeber Dienstleistungen im Bereich **KI-Implementierung und Beratung für Energieunternehmen**, insbesondere die Entwicklung von **Voice-Assistenten für den Kundenservice**.

Bei der Erbringung dieser Leistungen verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers.

Dieser Vertrag regelt die Auftragsverarbeitung nach Art. 28 DSGVO und stellt sicher, dass die Verarbeitung personenbezogener Daten datenschutzkonform erfolgt.

§ 1 — ANWENDUNGSBEREICH UND GEGENSTAND

(1) Vertragsgegenstand

Dieser Vertrag regelt die Rechte und Pflichten der Vertragsparteien bei der Verarbeitung personenbezogener Daten im Rahmen der Auftragsverarbeitung gemäß Art. 28 DSGVO.

(2) Hauptvertrag

Die Auftragsverarbeitung erfolgt im Rahmen des zwischen den Parteien geschlossenen Hauptvertrags vom _____ über [PROJEKTBEZEICHNUNG].

(3) Geltungsbereich

Dieser Vertrag gilt für alle Tätigkeiten, bei denen Mitarbeiter, Freelancer oder sonstige Beauftragte des Auftragnehmers personenbezogene Daten des Auftraggebers verarbeiten.

§ 2 — ART UND ZWECK DER DATENVERARBEITUNG

(1) Art der Datenverarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich zur Erfüllung des Hauptvertrags. Dies umfasst insbesondere:

- Entwicklung und Implementierung von KI-gestützten Kundenservice-Lösungen
- Konfiguration und Testing von Voice-Assistenten
- Analyse und Optimierung von Kundenservice-Prozessen
- Dokumentation und Support

Konkrete Verarbeitungstätigkeiten:

- Speicherung und Analyse von Kundenstammdaten
- Verarbeitung von Kommunikationsdaten
- Auswertung von Verbrauchsdaten (falls projektrelevant)
- Testing mit anonymisierten oder pseudonymisierten Kundendaten

(2) Zweck der Verarbeitung

Der Zweck der Datenverarbeitung ist die **Bereitstellung KI-gestützter Kundenservice-Lösungen** für den Auftraggeber.

(3) Kategorien betroffener Personen

- Endkunden des Auftraggebers (B2B2C-Beziehung)
- Ansprechpartner beim Auftraggeber (bei Bedarf)

(4) Kategorien personenbezogener Daten

Je nach Projekt können folgende Datenkategorien verarbeitet werden:

- **Kundenstammdaten:** Name, Vorname, Adresse, Kundennummer
- **Kommunikationsdaten:** E-Mail-Adressen, Telefonnummern, Kommunikationsverlauf
- **Verbrauchsdaten:** Energieverbrauch, Zählerdaten (standardmäßig anonymisiert)
- **Vertragsdaten:** Vertragsbeziehungen, Tarifdetails

Besondere Kategorien gem. Art. 9 DSGVO: [] JA [X] NEIN

(5) Dauer der Verarbeitung

Die Dauer der Auftragsverarbeitung entspricht der Laufzeit des Hauptvertrags.

§ 3 — WEISUNGEN UND WEISUNGSBEFUGNIS

(1) Weisungsgebundenheit

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich nach dokumentierten Weisungen des Auftraggebers.

(2) Form der Weisungen

Weisungen werden in folgenden Formen erteilt:

- Schriftlich (E-Mail oder Briefform)
- Mündlich (mit nachträglicher schriftlicher Bestätigung innerhalb von 48 Stunden)

(3) Initialweisung

Die Initialweisung zur Datenverarbeitung erfolgt durch diesen Vertrag und dessen Anlagen.

(4) Änderung von Weisungen

Änderungen oder Ergänzungen von Weisungen bedürfen der Schriftform.

(5) Unmöglichkeit der Weisung

Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er den Auftraggeber unverzüglich. Der Auftragnehmer ist berechtigt, die Durchführung der Weisung bis zur Bestätigung oder Änderung durch den Auftraggeber auszusetzen.

§ 4 — PFLICHTEN DES AUFTRAGNEHMERS

(1) Datenschutz-Compliance

Der Auftragnehmer verpflichtet sich zur Einhaltung der DSGVO, des BDSG und aller sonstigen anwendbaren Datenschutzvorschriften.

(2) Vertraulichkeit

Der Auftragnehmer stellt sicher, dass alle zur Verarbeitung personenbezogener Daten befugten Personen:

- Zur Vertraulichkeit verpflichtet wurden (§ 53 BDSG) oder
- Einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen

Diese Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

(3) Dokumentation

Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und stellt dies dem Auftraggeber auf Anfrage zur Verfügung.

(4) Unterstützungspflichten

Der Auftragnehmer unterstützt den Auftraggeber bei:

- Betroffenenanfragen (Auskunft, Berichtigung, Löschung, etc.)
- Datenschutz-Folgenabschätzungen (Art. 35 DSGVO)
- Meldung von Datenpannen (Art. 33, 34 DSGVO)
- Anfragen von Aufsichtsbehörden

§ 5 — TECHNISCH-ORGANISATORISCHE MASSNAHMEN (TOM)

(1) Umsetzung

Der Auftragnehmer verpflichtet sich, geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO umzusetzen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Dokumentation

Die aktuellen TOM sind in **Anlage 1** dokumentiert und werden bei wesentlichen Änderungen aktualisiert.

(3) Anpassung

Der Auftragnehmer ist berechtigt, die TOM anzupassen, sofern das Schutzniveau nicht unterschritten wird. Der Auftraggeber wird über wesentliche Änderungen informiert.

§ 6 — SUB-AUFTRAGSVERARBEITER

(1) Genehmigung

Der Auftraggeber erteilt dem Auftragnehmer die **allgemeine Genehmigung** zur Beauftragung von Sub-Auftragsverarbeitern nach Art. 28 Abs. 2 DSGVO.

(2) Aktuelle Sub-Auftragsverarbeiter

Eine Liste der aktuell eingesetzten Sub-Auftragsverarbeiter findet sich in **Anlage 2**.

(3) Hinzufügen neuer Sub-Auftragsverarbeiter

Bei der Hinzuziehung neuer Sub-Auftragsverarbeiter:

- Informiert der Auftragnehmer den Auftraggeber **mindestens 30 Tage im Voraus**
- Kann der Auftraggeber innerhalb dieser Frist **schriftlich Widerspruch** einlegen
- Erfolgt kein Widerspruch, gilt die Beauftragung als genehmigt

(4) Vertragliche Absicherung

Der Auftragnehmer stellt sicher, dass Sub-Auftragsverarbeiter die gleichen Datenschutzverpflichtungen eingehen wie der Auftragnehmer gegenüber dem Auftraggeber.

§ 7 — RECHTE DES AUFTRAGGEBERS

(1) Kontrollrechte

- Kontrollen vor Ort durchzuführen
- Einsicht in Dokumentationen zu nehmen
- Audits durchzuführen

(2) Durchführung von Kontrollen

- Kontrollen sind mit **14 Tagen Vorlauf** anzukündigen
- Kontrollen finden während der üblichen Geschäftszeiten statt
- Der Auftragnehmer stellt notwendige Informationen und Zugang bereit

(3) Kosten

Kosten für Kontrollen trägt der Auftraggeber, es sei denn, die Kontrolle ergibt einen Verstoß des Auftragnehmers gegen diesen Vertrag.

§ 8 — DATENPANNEN UND SICHERHEITSVORFÄLLE

(1) Meldepflicht

Der Auftragnehmer meldet Datenschutzverletzungen gemäß Art. 33 DSGVO **unverzüglich, spätestens innerhalb von 24 Stunden** nach Kenntnisnahme an den Auftraggeber.

(2) Inhalt der Meldung

Die Meldung enthält mindestens:

- Art der Verletzung des Schutzes personenbezogener Daten
- Kategorien und Anzahl betroffener Personen
- Kategorien und Anzahl betroffener Datensätze
- Mögliche Folgen der Verletzung
- Ergriffene oder vorgeschlagene Maßnahmen

(3) Dokumentation

Der Auftragnehmer dokumentiert alle Datenschutzverletzungen nach Art. 33 Abs. 5 DSGVO.

§ 9 – LÖSCHUNG UND RÜCKGABE VON DATEN

(1) Nach Vertragsende

Nach Beendigung des Hauptvertrags löscht der Auftragnehmer alle personenbezogenen Daten innerhalb von **30 Tagen**, sofern keine gesetzlichen Aufbewahrungspflichten bestehen.

(2) Wahlrecht des Auftraggebers

- **Löschung** aller Daten
- **Rückgabe** aller Daten in einem gängigen Format (z.B. CSV, JSON)

(3) Ausnahmen

Ausgenommen von der Löschung sind Daten, für die gesetzliche Aufbewahrungspflichten bestehen (z.B. § 147 AO, § 257 HGB).

(4) Löschnachweis

Der Auftragnehmer stellt auf Wunsch einen Nachweis über die ordnungsgemäße Löschung aus.

§ 10 – HAFTUNG

(1) Gesetzliche Haftung

Die Haftung der Vertragsparteien richtet sich nach Art. 82 DSGVO sowie nach den gesetzlichen Bestimmungen.

(2) Haftungsbegrenzung – Datenschutzverstöße

Für Schäden aus Datenschutzverstößen haftet der Auftragnehmer im Rahmen der Versicherungssumme der bestehenden Berufshaftpflichtversicherung (Hiscox Net IT).

Versicherungsdeckung (volle Limits):

- **Vermögensschadenhaftpflicht:** bis zu 1.000.000 EUR je Versicherungsfall
- **Datenschutzverletzungen (Vertragsstrafen):** bis zu 125.000 EUR je Versicherungsfall
- **Betriebshaftpflicht (Personen-/Sachschäden):** bis zu 3.000.000 EUR je Versicherungsfall

Die Haftung des Auftragnehmers für Schäden aufgrund **leichter Fahrlässigkeit** bei Datenschutzverstößen ist begrenzt auf die vorstehenden Versicherungssummen.

(3) Versicherungsnachweis

Der Auftragnehmer stellt dem Auftraggeber auf Anfrage einen Nachweis über die bestehende Versicherungsdeckung zur Verfügung.

(4) Ausnahmen von der Haftungsbegrenzung

- Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit
- Vorsatz und grobe Fahrlässigkeit
- Garantien
- Zwingend gesetzliche Haftungstatbestände (z.B. Produkthaftungsgesetz)

(5) Haftung für nicht-datenschutzrechtliche Schäden

Für Schäden, die nicht auf Datenschutzverstößen beruhen, gelten die allgemeinen gesetzlichen Haftungsregelungen.

(6) Freistellung

Der Auftragnehmer stellt den Auftraggeber von Ansprüchen Dritter frei, die auf einem vom Auftragnehmer zu vertretenden Verstoß gegen Datenschutzvorschriften beruhen, soweit diese Ansprüche im Rahmen der vorstehenden Haftungsgrenzen liegen.

§ 11 — BESONDERE BESTIMMUNGEN FÜR MESSDATENVERARBEITUNG

(1) Anwendungsbereich

Diese Bestimmungen gelten zusätzlich, wenn der Auftragnehmer im Rahmen der Auftragsverarbeitung **Messdaten** im Sinne des Messstellenbetriebsgesetzes (MsbG) oder des Energiewirtschaftsgesetzes (EnWG) verarbeitet.

(2) Verbrauchsdaten-Verarbeitung

a) Zweckbindung

Verbrauchsdaten werden ausschließlich für die folgenden Zwecke verarbeitet:

- Entwicklung und Testing von KI-gestützten Kundenservice-Lösungen
- Optimierung von Kundenservice-Prozessen
- Qualitätssicherung und Fehleranalyse

Eine Verarbeitung zu anderen Zwecken ist nur nach ausdrücklicher schriftlicher Weisung des Auftraggebers zulässig.

b) Anonymisierung und Pseudonymisierung

- **Testing und Entwicklung:** erfolgt ausschließlich mit anonymisierten oder pseudonymisierten Verbrauchsdaten
- **Produktivbetrieb:** Verbrauchsdaten werden nur im technisch erforderlichen Umfang in nicht-anonymisierter Form verarbeitet
- Der Auftragnehmer dokumentiert die eingesetzten Anonymisierungs- und Pseudonymisierungsverfahren

c) Smart-Meter-Daten

- Die technischen Richtlinien des BSI (BSI TR-03109)
- Besondere Sicherheitsanforderungen für intelligente Messsysteme
- Erhöhte Anforderungen an Datensicherheit und Verschlüsselung

(3) Löschfristen für Messdaten

Datenart	Löschfrist	Rechtsgrundlage
Smart-Meter-Verbrauchsdaten	2 Jahre nach Erhebung	§ 49 Abs. 3 MsbG
Konventionelle Verbrauchsdaten	3 Jahre nach Vertragsende	§ 47 Abs. 2 EnWG
Anonymisierte Testdaten	Keine Frist	Kein Personenbezug

(4) Technische Sicherheitsmaßnahmen

- **Verschlüsselung:** Transportverschlüsselung (TLS 1.3+) und Verschlüsselung im Ruhezustand
- **Zugriffskontrolle:** Rollenbasierter Zugriff, Protokollierung aller Zugriffe auf Messdaten
- **Datentrennung:** Strikte Trennung von Produktiv- und Testdaten
- **Regelmäßige Prüfung:** Vierteljährliche Überprüfung der Sicherheitsmaßnahmen

(5) Meldepflichten bei Messstellenbetreibern

- An die zuständige Regulierungsbehörde (Bundesnetzagentur), sofern vom Auftraggeber angewiesen
- Innerhalb der gesetzlichen Fristen nach § 49 Abs. 5 MsbG

§ 12 — KI-SPEZIFISCHE ANFORDERUNGEN (EU AI ACT)

(1) Anwendungsbereich

Diese Bestimmungen gelten zusätzlich, wenn die im Rahmen der Auftragsverarbeitung entwickelten oder eingesetzten KI-Systeme als **Hochrisiko-System** nach Art. 6 der KI-Verordnung (EU) 2024/1689 (EU AI Act) einzustufen sind.

(2) Hochrisiko-Einstufung

- Zur **kritischen Infrastruktur** nach Anhang III Ziffer 2 AI Act
- **Sicherheitsrelevante Entscheidungen** im Energieversorgungsbereich
- Vom Auftraggeber ausdrücklich als Hochrisiko-System eingestuft

(3) Risikomanagementsystem

a) Risikoanalyse

- Durchführung einer initialen Risikoanalyse vor Inbetriebnahme
- Identifizierung möglicher Risiken für Gesundheit, Sicherheit und Grundrechte
- Dokumentation der Risikoanalyse nach Art. 9 AI Act
- Regelmäßige Aktualisierung bei wesentlichen Änderungen

b) Risikominimierung

- Implementierung geeigneter Maßnahmen zur Risikominimierung
- Testing und Validierung des KI-Systems vor Produktivbetrieb
- Kontinuierliche Überwachung im Betrieb

(4) Datenqualität und Governance

a) Trainings-, Validierungs- und Testdaten:

- Relevanz, Repräsentativität und Fehlerfreiheit der Datensätze
- Berücksichtigung des spezifischen Umfelds
- Dokumentation der Datenquellen und -herkunft

b) Datenschutz-Governance:

- Geeignete Maßnahmen zur Erkennung und Behebung von Verzerrungen (Bias)
- Einhaltung datenschutzrechtlicher Vorgaben (Art. 10 Abs. 5 AI Act)
- Lückfüllung und Aktualisierung von Datensätzen

(5) Technische Dokumentation

- Allgemeine Beschreibung des KI-Systems (Zweck, Funktionsweise)
- Entwicklungsprozess-Dokumentation (Methoden, Algorithmen, Datenquellen)
- Risikomanagement-Dokumentation (Analysen, Maßnahmen, Tests)
- Änderungshistorie und Versionierung

(6) Menschliche Aufsicht (Human Oversight)

a) Aufsichtsmaßnahmen:

- Menschliche Prüfung kritischer Entscheidungen vor Umsetzung
- Möglichkeit zur Intervention, Überschreibung oder Abschaltung
- Angemessene Schulung des Aufsichtspersonals

b) Transparenz gegenüber Nutzern:

- Kenntlichmachung, dass ein KI-System verwendet wird
- Klare Kommunikation der Systemgrenzen und -fähigkeiten
- Informationen über menschliche Aufsicht und Eskalationswege

(7) Protokollierung und Transparenz

- Automatische Protokollierung relevanter Ereignisse
- Rückverfolgbarkeit von Entscheidungen und eingesetzten Datengrundlagen
- Aufbewahrung der Protokolle für mindestens 6 Monate (Art. 12 Abs. 1 AI Act)

(8) Genauigkeit, Robustheit und Cybersicherheit

- **Genauigkeit:** Angemessenes Niveau in Bezug auf den vorgesehenen Zweck
- **Robustheit:** Widerstandsfähigkeit gegenüber Fehlern, Inkonsistenzen, Adversarial Attacks
- **Cybersicherheit:** Schutz gegen unbefugten Zugriff, Manipulation und Angriffe

(9) Konformitätsbewertung

a) Unterstützung bei Konformitätsbewertung:

- Bereitstellung der technischen Dokumentation
- Zugang zu Datenquellen und Testumgebungen
- Unterstützung bei Audits durch benannte Stellen

b) EU-Konformitätserklärung:

Sofern der Auftragnehmer das KI-System als Produkt bereitstellt, erstellt er die EU-Konformitätserklärung nach Art. 47 AI Act.

(10) Informationspflichten

- Bei Hinweisen auf Nichtkonformität des KI-Systems mit dem AI Act
- Bei schwerwiegenden Zwischenfällen (Art. 73 AI Act)
- Bei behördlichen Anfragen bezüglich des KI-Systems
- Bei geplanten wesentlichen Änderungen am KI-System

(11) Nicht-Hochrisiko-Systeme

- Kenntlichmachung der KI-Nutzung für Endnutzer
- Erklärbarkeit von KI-generierten Outputs auf Anfrage
- Keine Täuschung über die Natur der Interaktion (Mensch vs. KI)

§ 13 – VERTRAGSLAUFZEIT UND KÜNDIGUNG

(1) Laufzeit

Dieser Vertrag tritt mit Unterzeichnung in Kraft und läuft für die Dauer des Hauptvertrags.

(2) Ordentliche Kündigung

Dieser Vertrag kann mit einer Frist von **einem Monat** zum Monatsende gekündigt werden. Die Kündigung bedarf der Schriftform.

(3) Außerordentliche Kündigung

- Schwerwiegenden Verstößen gegen Datenschutzvorschriften
- Zahlungsverzug des Auftraggebers von mehr als 60 Tagen
- Insolvenz einer Vertragspartei

§ 14 – SCHLUSSBESTIMMUNGEN

(1) Änderungen und Ergänzungen

Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform.

(2) Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht.

(3) Anwendbares Recht

Für diesen Vertrag gilt das Recht der Bundesrepublik Deutschland.

(4) Gerichtsstand

Gerichtsstand ist der Sitz des Auftraggebers.

UNTERSCHRIFTEN

Auftraggeber:

Ort, Datum

Name, Funktion, Unterschrift

Auftragnehmer (k3i GmbH):

Ort, Datum

Name, Funktion, Unterschrift

ANLAGEN

- **Anlage 1:** Technisch-organisatorische Maßnahmen (TOM)
- **Anlage 2:** Sub-Auftragsverarbeiter

ANLAGE 1: TECHNISCH-ORGANISATORISCHE MASSNAHMEN (TOM)

k3i GmbH | Stand: März 2026

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

1.1 Zutrittskontrolle

Ziel: Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren

Maßnahme	Beschreibung	Status
Sichere Büroräume	Arbeitsräume mit Schloss gesichert	Ja
Clean-Desk-Policy	Keine sensiblen Unterlagen offen liegen lassen	Ja
Mobile Geräte	Verschlüsselte Firmenlaptops (APFS/FileVault)	Ja

1.2 Zugangskontrolle

Ziel: Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden

Maßnahme	Beschreibung	Status
Benutzerverwaltung	Individuelle Benutzerkonten für alle Mitarbeiter/Freelancer	Ja
Passwort-Management	OnePassword (Team Plan), mind. 16 Zeichen	Ja
2-Faktor-Authentifizierung	Aktiviert für: Microsoft 365, Notion, Anthropic, Cloudflare	Ja
Automatische Bildschirmsperre	Nach Inaktivität aktiviert	Ja
Regelmäßige Passwortänderung	Bei Verdacht auf Kompromittierung	Ja

1.3 Zugriffskontrolle

Maßnahme	Beschreibung	Status
Rollenbasierter Zugriff	Notion: Projektbezogene Zugriffsrechte für Freelancer	Ja
Minimalprinzip	Zugriff nur auf notwendige Datenbestände	Ja
Rechtevergabe dokumentiert	Dokumentation in internem System	Ja

1.4 Trennungskontrolle

Maßnahme	Beschreibung	Status
Projektspezifische Datenablage	Separate Notion-Seiten und Ordnerstrukturen pro Kunde	Ja
Mandantenfähige Systeme	Klare Trennung in Microsoft 365 und Notion	Ja

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

Maßnahme	Beschreibung	Status
Testing mit anonymisierten Daten	Standard bei KI-Voice-Assistant-Testing	Ja
MSB-Projekte	Verbrauchsdaten standardmäßig anonymisiert	Ja

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

2.1 Weitergabekontrolle

Maßnahme	Beschreibung	Status
E-Mail-Verschlüsselung	TLS für E-Mail-Transport	Ja
Verschlüsselte Übertragung	HTTPS für alle Web-Anwendungen	Ja
Kontrolle von Datenträgern	USB-Sticks nur verschlüsselt nutzen	Ja
Cloud-Dienste mit AVV	Nur Tools mit gültigem Auftragsverarbeitungsvertrag	Ja

2.2 Eingabekontrolle

Maßnahme	Beschreibung	Status
Logging in Cloud-Systemen	Notion, Microsoft 365 mit Versionierung	Ja
Änderungshistorie	Aktiviert in Notion und Microsoft 365	Ja
Protokollierung von Zugriffen	Wo technisch möglich aktiviert	Ja

3. VERFÜGBARKEIT UND BELASTBARKEIT (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Verfügbarkeitskontrolle

Maßnahme	Beschreibung	Status
Backups	Automatische Cloud-Backups (Microsoft 365, Notion)	Ja
Redundante Datenhaltung	Cloud-Anbieter mit SLA-Garantien	Ja
USV/Notstrom	Bei Cloud-Anbietern gewährleistet	Ja

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

Maßnahme	Beschreibung	Status
Notfallplan	Dokumentierter Wiederherstellungsprozess	Ja
Backup-Wiederherstellung	Regelmäßig getestet (jährlich)	Ja

4. VERFAHREN ZUR ÜBERPRÜFUNG (Art. 32 Abs. 1 lit. d DSGVO)

4.1 Datenschutz-Management

Maßnahme	Beschreibung	Status
Datenschutz-Koordinator	Joe Kohnert	Ja
Schulungen	Jährliche Datenschutz-Schulung für alle GF	Ja
Dokumentation	Verzeichnis der Verarbeitungstätigkeiten (VVT)	Ja
Datenpannen-Prozess	Meldeverfahren definiert	Ja

4.2 Incident Response Management

Maßnahme	Beschreibung	Status
Meldeprozess	Datenpannen binnen 24h an Verantwortlichen	Ja
Kontaktdaten	Datenschutz-Koordinator erreichbar	Ja

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Maßnahme	Beschreibung	Status
KI-Tool-Konfiguration	Training-Opt-out bei allen KI-Plattformen	Ja
Minimaldatenerhebung	Nur notwendige Daten verarbeiten	Ja

4.4 Auftragskontrolle

Maßnahme	Beschreibung	Status
AVV mit Sub-Verarbeitern	Microsoft, Notion, n8n, Anthropic, Cloudflare	Ja
Vertraulichkeitserklärungen	Für alle Freelancer verpflichtend	Ja

Maßnahme	Beschreibung	Status
NDA	Für alle Freelancer verpflichtend	Ja

5. ZUSÄTZLICHE TECHNISCHE MASSNAHMEN

5.1 Verschlüsselung

System	Verschlüsselung	Details
Laptops	APFS/FileVault	Vollständige Festplattenverschlüsselung
E-Mail	TLS 1.2+	Transport-Verschlüsselung
Cloud-Speicher	Provider-seitig	Microsoft 365, Notion

5.2 Firewall und Virenschutz

Maßnahme	Details
OS-Firewall	Aktiviert auf allen Geräten
Antivirus	macOS-integrierter Schutz + regelmäßige Updates
Updates	Automatische Sicherheitsupdates aktiviert

6. ORGANISATORISCHE MASSNAHMEN

6.1 Datenschutz-Schulungen

- **Häufigkeit:** Jährlich
- **Zielgruppe:** Alle Geschäftsführer
- **Inhalte:** DSGVO-Basics, interne Policies, KI-Nutzungsrichtlinie, Betroffenenrechte

6.2 Löschkonzept

Datenkategorie	Löschfrist
Kundenprojekte (ohne personenbez. Endkundendaten)	Nach Projektende + 3 Monate
Buchhaltung/Verträge	10 Jahre (§ 147 AO)
E-Mail-Korrespondenz	6 Jahre
Leads/Interessenten	2 Jahre nach letztem Kontakt
Messdaten (Smart Meter)	2 Jahre nach Erhebung
Messdaten (konventionell)	3 Jahre nach Vertragsende

6.3 Regelmäßige Überprüfung

- **Quartalsweise:** Löschprüfung
- **Jährlich:** Überprüfung der TOM
- **Bei Bedarf:** Anpassung bei neuen Tools oder Prozessen

Verantwortlich für TOM:

Joe Kohnert, Datenschutz-Koordinator

Letzte Überprüfung: März 2026

Nächste Überprüfung: März 2027

ANLAGE 2: SUB-AUFTRAGSVERARBEITER

k3i GmbH | Stand: März 2026

Der Auftragnehmer setzt für die Erbringung der vertraglich vereinbarten Leistungen folgende Sub-Auftragsverarbeiter ein:

1. MICROSOFT CORPORATION

Anbieter	Microsoft Corporation
Adresse	One Microsoft Way, Redmond, WA 98052-6399, USA
Leistung	Cloud-Dienste (Microsoft 365: Outlook, Teams, SharePoint, OneDrive)
Verarbeitete Daten	Rechnungen, Verträge, E-Mail-Korrespondenz, interne Dokumente
Hosting-Region	EU (EU Data Boundary)
AVV/DPA	Ja — Microsoft Online Services Terms (OST) mit Data Protection Addendum
Standardvertragsklauseln	Ja — Modul 2: Controller to Processor
Training-Opt-out	Ja — Copilot nicht aktiviert
Website	https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

2. NOTION LABS, INC.

Anbieter	Notion Labs, Inc.
Adresse	2300 Harrison Street, San Francisco, CA 94110, USA
Leistung	Projektmanagement, CRM, interne Dokumentation
Verarbeitete Daten	Projekte, Kontakte (CRM), interne Dokumentation, Gesprächsnotizen
Hosting-Region	USA
AVV/DPA	Ja — Data Processing Addendum verfügbar
Standardvertragsklauseln	Ja
Training-Opt-out	Ja — Notion AI: Training deaktiviert
Website	https://www.notion.so/help/notion-and-data-protection

3. N8N GMBH

Anbieter	n8n GmbH
Adresse	Borsigstraße 27, 10115 Berlin, Deutschland
Leistung	Workflow-Automatisierung (Cloud)
Verarbeitete Daten	Alle Arten von Daten je nach Workflow-Konfiguration
Hosting-Region	EU
AVV/DPA	Ja — Data Processing Agreement verfügbar
Standardvertragsklauseln	n/a (EU-Hosting)
Training-Opt-out	n/a (keine KI-Funktion)

Website	https://n8n.io/legal/data-processing-agreement
----------------	---

4. ANTHROPIC, PBC

Anbieter	Anthropic, PBC
Adresse	548 Market St, San Francisco, CA 94104, USA
Leistung	KI-Modelle (Claude) für Textverarbeitung und Assistenz
Verarbeitete Daten	Anfrage-Texte, Konversationsdaten (je nach Projekt)
Hosting-Region	USA
AVV/DPA	Ja — Data Processing Addendum verfügbar
Standardvertragsklauseln	Ja
Training-Opt-out	Ja — Training mit Kundendaten deaktiviert
Website	https://www.anthropic.com/policies/privacy

5. CLOUDFLARE, INC.

Anbieter	Cloudflare, Inc.
Adresse	101 Townsend St, San Francisco, CA 94107, USA
Leistung	Website-Hosting, CDN, DNS, DDoS-Schutz
Verarbeitete Daten	HTTP-Requests, IP-Adressen, Website-Traffic
Hosting-Region	EU
AVV/DPA	Ja — Data Processing Addendum verfügbar
Standardvertragsklauseln	n/a (EU-Hosting)
Training-Opt-out	n/a (keine KI-Funktion)
Website	https://www.cloudflare.com/trust-hub/gdpr/

HINWEISE

Änderungen der Liste

Diese Liste wird bei Änderungen aktualisiert. Der Auftraggeber wird über die Hinzuziehung neuer Sub-Auftragsverarbeiter mindestens 30 Tage im Voraus informiert und kann gemäß § 6 des Hauptvertrags Widerspruch einlegen.

Eigene Sub-Auftragsverarbeiter

Die genannten Anbieter können ihrerseits weitere Sub-Auftragsverarbeiter einsetzen:

- **Microsoft:** <https://learn.microsoft.com/en-us/compliance/regulatory/offering-home>
- **Notion:** <https://www.notion.so/help/notion-and-data-protection>
- **Anthropic:** <https://www.anthropic.com/policies/privacy>
- **Cloudflare:** <https://www.cloudflare.com/trust-hub/gdpr/>

Letzte Aktualisierung: März 2026

ENDE DES VERTRAGS