VERTRAGSFASSUNG · VERSION 2026-11-13

# 1. Parteien und Vertragsgegenstand

### Vertragsgrundlagen

Dieser Auftragsverarbeitungsvertrag einschließlich der Anlagen 1 bis 3 regelt die Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 DSGVO. Die im Vertrag beschriebenen Pflichten gelten unabhängig von den gewählten Produkteinstellungen. Der Datenschutzmodus in Audryo ersetzt weder die Rechtsgrundlage des Auftraggebers noch die vertraglichen Pflichten des Auftragnehmers.

### Auftragsverarbeiter

Dear Friend Digital GmbH, Emilienstraße 9, 90489 Nürnberg, Deutschland; Amtsgericht Nürnberg, HRB 26228. Kontakt für Weisungen und Datenschutzanliegen: hello@audryo.com. Im Folgenden: Auftragnehmer.

### Verantwortlicher

Firma / Organisation: _____
Anschrift: _____
Vertretungsberechtigte Person: _____
Datenschutz- und Weisungskontakt: _____
Betroffene Workspace-ID(s): _____
Im Folgenden: Auftraggeber.

### Gegenstand und Dauer

Der Auftragnehmer verarbeitet personenbezogene Daten zur Bereitstellung von Audryo: Verwaltung von Kontakten, Einwilligungen, Zielgruppen, Produkt-Events, E-Mail-Inhalten, Journeys, Kampagnen, Versand und Auswertungen nach dokumentierter Weisung des Auftraggebers. Die Einzelheiten stehen in Anlage 1. Die Verarbeitung beginnt mit dem vereinbarten Leistungsbeginn und dauert bis zur Beendigung des Hauptvertrags sowie zur vereinbarten Rückgabe oder Löschung.

### Rollen und Rangfolge

Der Auftraggeber entscheidet über Zwecke und zulässige Mittel der Kundendatenverarbeitung. Dieser Vertrag regelt die Auftragsverarbeitung nach Art. 28 DSGVO und geht bei Widersprüchen über den Schutz dieser Daten den allgemeinen Leistungsbedingungen vor. Eigenverantwortliche Verarbeitungen des Auftragnehmers, etwa gesetzlich erforderliche Vertrags- und Rechnungsdaten, richten sich nach den einschlägigen gesetzlichen Vorschriften und der Datenschutzerklärung.

### Vertragsschluss

Der Vertrag kann schriftlich oder elektronisch geschlossen werden. Auftraggeber ist die beim Vertragsschluss bezeichnete Organisation mit den zugeordneten Workspaces. Bei elektronischer Annahme werden Vertragsversion, Zeitpunkt und die annehmende berechtigte Person dokumentiert. Der bloße Download oder das Einschalten einer Produktoption stellt keine Vertragsannahme dar. Die Anlagen 1 bis 3 sind Bestandteil dieses Vertrags.

VERTRAGSFASSUNG · VERSION 2026-11-13

# 2. Weisungen, Vertraulichkeit und Sicherheit

### Dokumentierte Weisungen

Der Auftragnehmer verarbeitet Kundendaten ausschließlich auf dokumentierte Weisung des Auftraggebers, auch hinsichtlich einer Übermittlung in ein Drittland. Weisungen ergeben sich aus dem Hauptvertrag, diesem Vertrag und der durch berechtigte Personen veranlassten Nutzung von UI, API, MCP, Integrationen und Workspace-Einstellungen. Weitere Weisungen erfolgen in Textform an den vereinbarten Kontakt. Weisungen und Änderungen sind nachvollziehbar zu dokumentieren.

### Grenzen der Weisung

Ist der Auftragnehmer durch Unionsrecht oder das Recht eines Mitgliedstaats zu einer abweichenden Verarbeitung verpflichtet, informiert er den Auftraggeber vorab über diese Verpflichtung, soweit das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses untersagt. Hält er eine Weisung für datenschutzwidrig, informiert er den Auftraggeber unverzüglich und setzt die betroffene Verarbeitung bis zur Klärung aus, soweit rechtlich zulässig.

### Pflichten des Auftraggebers

Der Auftraggeber bleibt für die Rechtmäßigkeit der Datenerhebung, Rechtsgrundlagen, Datenschutzhinweise, Empfängerrechte und Versandentscheidungen verantwortlich. Er weist nur erforderliche Daten an und begrenzt Berechtigungen. Versand-Einwilligung und individuelle Tracking-Einwilligung sind getrennt zu beurteilen. Double-Opt-in ist ein Nachweisverfahren; es ersetzt keine vollständige, freiwillige und zweckbezogene Einwilligung.

### Verpflichtete Personen

Der Auftragnehmer gewährt nur befugten und zur Vertraulichkeit verpflichteten oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegenden Personen Zugang zu Kundendaten. Zugriffsrechte werden nach Aufgaben und Erforderlichkeit vergeben und bei Wegfall entzogen. Die Umsetzung und Verantwortlichkeiten werden nach Anlage 2 dokumentiert.

### Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft die nach Art. 32 DSGVO erforderlichen Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der Risiken für betroffene Personen. Die verbindliche Ausgangsbeschreibung ist Anlage 2. Maßnahmen dürfen weiterentwickelt werden, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber nachvollziehbar mitzuteilen.

### Verarbeitungsorte

Die Kernanwendung wird nach Betreiberangabe bei Hetzner in Nürnberg, Deutschland, gehostet. Das ist keine Zusage, dass sämtliche zusätzlichen Dienste ausschließlich dort verarbeiten. Für Dateiablage, E-Mail-Dienste, KI-Routing und Modellanbieter sind die tatsächlich eingesetzten Orte in Anlage 3 festzuhalten. Drittlandtransfers sind nur unter den Voraussetzungen der Art. 44 ff. DSGVO zulässig.

VERTRAGSFASSUNG · VERSION 2026-11-13

# 3. Unterstützung, Meldungen und Kontrolle

### Betroffenenrechte

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Pflichten zur Beantwortung von Anträgen nach Kapitel III DSGVO. Audryo bietet Kontakt-Export und Kontakt-Löschung. Weitergehende berechtigte Auskunfts-, Berichtigungs-, Einschränkungs- und Löschanweisungen werden über den vereinbarten Kontakt bearbeitet. Direkt eingehende Anträge zu Kundendaten leitet der Auftragnehmer unverzüglich an den Auftraggeber weiter und beantwortet sie nur auf dessen Weisung oder bei eigener gesetzlicher Pflicht.

### Datenschutzverletzungen

Der Auftragnehmer benachrichtigt den Auftraggeber unverzüglich nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten. Er übermittelt die ihm verfügbaren Informationen zu Art und Umfang, betroffenen Personen- und Datenkategorien, voraussichtlichen Folgen, ergriffenen oder vorgeschlagenen Maßnahmen sowie einem erreichbaren Kontakt. Noch fehlende Informationen werden ohne unangemessene Verzögerung nachgereicht. Er dokumentiert Vorfälle und unterstützt die Untersuchung, Eindämmung sowie die gesetzlichen Melde- und Benachrichtigungspflichten des Auftraggebers.

### Art. 32 bis 36 DSGVO

Unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen unterstützt der Auftragnehmer den Auftraggeber bei Sicherheit, Datenschutz-Folgenabschätzungen und erforderlichen vorherigen Konsultationen der Aufsichtsbehörde. Der Auftraggeber beurteilt insbesondere Risiken aus Profilbildung, Journey-Entscheidungen, sensiblen Daten und umfangreicher Verhaltensanalyse.

### Nachweise und Prüfungen

Der Auftragnehmer stellt alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO zur Verfügung und ermöglicht und unterstützt Überprüfungen einschließlich Inspektionen durch den Auftraggeber oder einen von ihm beauftragten Prüfer. Verhältnismäßige organisatorische Absprachen zu Termin, Sicherheit und Schutz anderer Kunden sind zulässig; sie dürfen das Prüfungsrecht nicht ausschließen. Bei einem konkreten Datenschutzvorfall oder behördlicher Anforderung ist eine zeitnahe Prüfung zu ermöglichen.

### Behörden und Zugriffsersuchen

Der Auftragnehmer informiert den Auftraggeber unverzüglich über behördliche Maßnahmen oder Zugriffsersuchen mit Bezug zu Kundendaten, soweit dies rechtlich zulässig ist. Er prüft die Rechtmäßigkeit und beschränkt eine erforderliche Offenlegung auf den gesetzlich notwendigen Umfang.

### Kontakt und Erreichbarkeit

Vertraglicher Kontakt des Auftragnehmers: hello@audryo.com. Der Auftraggeber hält seinen Datenschutz- und Weisungskontakt aktuell. Der Auftragnehmer dokumentiert seinen Sicherheits- und Vorfallsprozess einschließlich Vertretung und Erreichbarkeit nach Anlage 2.

VERTRAGSFASSUNG · VERSION 2026-11-13

# 4. Unteraufträge und Vertragsende

### Unterauftragsverarbeiter

Der Auftraggeber genehmigt den Einsatz der in Anlage 3 konkret benannten Unterauftragsverarbeiter für die dort bezeichneten Leistungen. Weitere oder ersetzende Unterauftragsverarbeiter werden mindestens 30 Tage vor Beauftragung unter Angabe von Identität, Leistung, Verarbeitungsorten und Transfergrundlagen mitgeteilt. Der Auftraggeber kann innerhalb von 14 Tagen aus begründeten Datenschutzgründen widersprechen. Bis zur Klärung wird der beanstandete Dienst nicht für die betroffenen Daten eingesetzt. Eine pauschale Genehmigung unbestimmter KI-Modellanbieter erfolgt nicht.

### Weitergabe der Pflichten

Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf im Wesentlichen dieselben Datenschutzpflichten, insbesondere ausreichende Garantien für geeignete Maßnahmen. Er bleibt dem Auftraggeber für die Erfüllung dieser Pflichten durch den Unterauftragsverarbeiter verantwortlich. Er hält die einschlägigen Nachweise verfügbar. Bei Drittländern sind Empfänger, Zugriffsmöglichkeiten und die einschlägige Transfergrundlage vorab zu prüfen und in Anlage 3 zu dokumentieren.

### Vom Kunden angebundene Dienste

Versandkonten, CRM-Integrationen, Webhook-Ziele, Zapier und externe Agenten können vom Auftraggeber selbst ausgewählt und beauftragt werden. Rollen, eigene Verträge und Transfergrundlagen sind anhand der tatsächlichen Einbindung zu bestimmen. Ein eigener API-Schlüssel allein entscheidet nicht über die datenschutzrechtliche Rolle. Die vom Auftragnehmer selbst eingesetzten Dienste gehören unabhängig davon in seine Unterauftragnehmerprüfung.

### Rückgabe und Löschung

Nach Ende der Leistung löscht der Auftragnehmer nach Wahl des Auftraggebers die personenbezogenen Daten oder gibt sie zurück und löscht vorhandene Kopien, sofern keine unions- oder mitgliedstaatliche gesetzliche Aufbewahrungspflicht besteht. Rückgabeformat und Ausführungsfrist sind bei Vertragsende dokumentiert abzustimmen. Gesetzlich aufzubewahrende Restdaten sind zu sperren, auf den erforderlichen Umfang zu begrenzen und nach Fristablauf zu löschen. Die Erledigung wird auf Verlangen bestätigt.

### Backups

Backups werden 14 Tage aufbewahrt. Gelöschte Daten dürfen darin nur bis zum Ablauf dieses Zyklus verbleiben, müssen dem normalen Zugriff entzogen sein und dürfen nur zur Wiederherstellung im Störungsfall genutzt werden. Nach einer Wiederherstellung sind zwischenzeitliche Lösch- und Sperranweisungen erneut anzuwenden. Der Auftragnehmer dokumentiert den Backup-Zyklus und das Verfahren zur Wiederanwendung dieser Anweisungen.

### Vertragsannahme

Ort / Datum: _____
Auftraggeber, Name / Funktion / Annahme: _____
Auftragnehmer, Name / Funktion / Annahme: _____
Vertragsversion: 2026-11-13; Anlagen 1 bis 3 sind einbezogen.
Bei elektronischem Vertragsschluss tritt der dokumentierte Annahmenachweis an die Stelle der Unterschriftsfelder.

VERTRAGSFASSUNG · VERSION 2026-11-13

# Anlage 1 - Verarbeitung und Datenarten

### Art und Zweck

Erheben auf Kundenanweisung, Importieren, Speichern, Ordnen, Anreichern nach Weisung, Segmentieren, Auslösen von Journeys, Personalisieren und Versenden freigegebener E-Mails, Zustellverarbeitung, Bearbeiten von Abmeldungen und Einwilligungen, Auswerten freigegebener Events, Exportieren und Löschen. Freiwillige zusätzliche Verarbeitung umfasst individuelle Öffnungs- und Klickanalyse, externe KI sowie die Weiterleitung an konfigurierte Dienste.

### Datenarten

Kontakt- und Identifikationsdaten (z.B. Name, E-Mail-Adresse, Kunden-ID, Sprache); vom Auftraggeber übergebene Profilfelder, Tags und Produkt-Events; Zielgruppenzugehörigkeiten; Einwilligungs- und Abmeldenachweise; E-Mail-Inhalte und Personalisierungswerte; Versand-, Fehler- und Zustellinformationen; bei gesonderter Freigabe Öffnungs- und Klickereignisse mit technischen Requestinformationen; Zugriffs-, Audit- und Weisungsprotokolle. Umfang und konkrete Felder bestimmt der Auftraggeber.

### Betroffene Personen

Kunden, Interessenten, Newsletter-Empfänger, Produktnutzer, Spender, Mitglieder und sonstige Kontakte des Auftraggebers sowie berechtigte Beschäftigte oder Beauftragte, soweit in den angewiesenen Daten enthalten. Minderjährige oder andere besonders schutzbedürftige Gruppen sind vom Auftraggeber gesondert zu beurteilen.

### Besondere Kategorien

Daten nach Art. 9 DSGVO oder über strafrechtliche Verurteilungen nach Art. 10 DSGVO sind nicht als allgemeiner Standardumfang vorgesehen. Die Verwendung erfordert eine vorherige ausdrückliche Abstimmung über Rechtsgrundlage, Erforderlichkeit, passende Maßnahmen und gegebenenfalls Datenschutz-Folgenabschätzung. Freitext, Eventnamen, Links und Segmentnamen können auch ohne besondere Feldbezeichnung sensible Informationen enthalten.

### Produktseitige Schutzfunktionen

Workspace-Schutzfunktionen lassen Öffnungs- und Klickstatistiken für E-Mails und Journeys eingeschaltet, verlangen für die Erfassung jedoch eine separate, belegte Einwilligung zum Zweck email_analytics. Auf einzelnen Kontaktprofilen werden Öffnungen, Klicks, Zeitpunkte und geklickte Ziele einschließlich der Timeline ausgeblendet und von der regulären Kontakt-API nicht ausgegeben. Die zugrunde liegende Erfassung bleibt personenbezogen; dies ist eine Anzeige- und Zugriffsbeschränkung, keine Anonymisierung. Externe KI, Remote-E-Mail-Schriften, ausgehende Webhooks und Audryo-Nutzungsanalyse sind zunächst aus. Für neue Marketing-Anmeldungen gilt Double-Opt-in, für Engagement-Daten eine voreingestellte Aufbewahrung von 90 Tagen; strengere vorhandene Fristen bleiben erhalten. Produkt-Events sind separat abschaltbar. Bestehende Einwilligungen und Daten werden nicht automatisch gelöscht oder erneuert.

### Grenzen und Aufbewahrung

Der Auftraggeber legt Erforderlichkeit, Zwecke und Fristen fest. Die automatische Produktfrist betrifft ausschließlich gespeicherte Öffnungs- und Klickereignisse. Sie ist kein allgemeines Löschkonzept für Profile, Produkt-Events, Einwilligungsnachweise, Audit-Logs, Zustelldaten, Auftragswarteschlangen oder Kopien bei Dritten. Diese Kategorien benötigen eigene dokumentierte Fristen und Verfahren. Sicherheits-, Sperr- und gesetzliche Aufbewahrungspflichten bleiben zu berücksichtigen.

VERTRAGSFASSUNG · VERSION 2026-11-13

# Anlage 2 - Technische und organisatorische Maßnahmen

### Technische Schutzmechanismen

Workspace-Zugriffsgrenzen; Rollen für Owner, Admin, Editor und Viewer; begrenzte API-/MCP-Scopes; Prüfung von Session-CSRF; gehashte Passwörter und Token; verschlüsselte Anbieter-Zugangsdaten im Anwendungsmodell; Audit-Ereignisse für Mutationen; Versandprüfung von Einwilligung und Sperren; signierte Empfängerlinks; Kontakt-Export und -Löschung. Bei S3-Objektablage werden private Buckets und serverseitige Verschlüsselung konfiguriert. Der Auftragnehmer prüft die wirksame Konfiguration der eingesetzten Mechanismen im Betrieb.

### Hosting und Datensicherung

Kernanwendung: Hetzner, Nürnberg, Deutschland. Backup-Aufbewahrung: 14 Tage. Die konkret verwendeten Rechenzentrumsleistungen, Verträge, Berechtigungen und Wiederherstellungsverfahren werden in der Betriebsdokumentation nachgewiesen.

### Organisatorische Sicherheitsmaßnahmen

Der Auftragnehmer dokumentiert und überprüft risikogerecht die Maßnahmen für TLS und Verschlüsselung im Betrieb, Schlüsselverwaltung und Rotation, administrative Zugriffe einschließlich Mehrfaktor-Authentifizierung, Vertraulichkeitsverpflichtungen und Schulung, Berechtigungsprüfungen bei Ein- und Austritt, Patch- und Schwachstellenmanagement, Mandantentrennung, Zugriffe auf Logs und Supportdaten, Incident-Response einschließlich Vertretung und Meldekontakten sowie Verfügbarkeit und getestete Wiederherstellungen. Verantwortlichkeiten und Nachweise werden aktuell gehalten. Die Maßnahmen werden nach Art. 32 Abs. 1 lit. d DSGVO regelmäßig überprüft und bewertet.

### Lösch- und Wiederherstellungsverfahren

Der Auftragnehmer dokumentiert kategorienbezogene Fristen für Kundendaten, Protokolle, Warteschlangen und externe Anbieter, die Behandlung von Exportdateien, die Löschung aus Primärsystem und Objektablage, Löschvermerke für Wiederherstellungen sowie die Sperrung gesetzlich aufzubewahrender Daten. Der 14-tägige Backup-Zyklus und die Wiederanwendung von Lösch- und Sperranweisungen nach einer Wiederherstellung werden nachgewiesen. Die Produktoption für Engagement-Aufbewahrung ist Teil dieses Verfahrens, ersetzt jedoch kein vollständiges Löschkonzept.

### Nachweise und Verantwortlichkeiten

Der Auftragnehmer führt ein aktuelles Verzeichnis der zuständigen Betriebs- und Sicherheitsverantwortlichen, der Prüfungen und der zugehörigen Nachweise. Der Auftraggeber erhält die für den Nachweis der Vertragserfüllung erforderlichen Informationen nach den Kontrollregelungen dieses Vertrags.

### Umfang der Zusagen

Eine ISO-Zertifizierung, die ausschließliche Verarbeitung sämtlicher optionaler Dienste innerhalb der EU, besondere Wiederherstellungsziele oder zusätzliche Reaktionsfristen werden durch diesen Vertrag nicht zugesichert. Gesondert vereinbarte Leistungen und die gesetzlichen Pflichten bleiben unberührt.

VERTRAGSFASSUNG · VERSION 2026-11-13

# Anlage 3 - Dienste und Unterauftragnehmer

### Hetzner Online GmbH - Hosting

Hetzner Online GmbH; Hosting der Kernanwendung in Nürnberg, Deutschland. Backup-Aufbewahrung: 14 Tage. Der Auftragnehmer dokumentiert den konkreten Leistungsumfang, die Auftragsverarbeitungsvereinbarung, Backup-Speicherorte und gegebenenfalls weitere Unteraufträge in seinen Vertrags- und Betriebsunterlagen.

### OpenRouter und ausführende Modellanbieter - optionale KI

OpenRouter wird als KI-Routingdienst für optionale KI-Funktionen eingesetzt. Die Anwendung nutzt unter anderem Google-Gemini-Modelle und teilweise Anthropic-Claude-Modelle als Fallback. Eine Modellbezeichnung bestimmt nicht den ausführenden Anbieter. Der Adapter fordert Zero Data Retention und untersagt Data-Collection; eine feste EU-Region ist nicht vorgegeben. Vor der Verarbeitung von Kundendaten über einen konkreten Anbieter stellt der Auftragnehmer dessen vollständige Vertragsgesellschaft, Leistung, Verarbeitungsorte, Vertrags- und Transfergrundlagen sowie Speicher- und Trainingsbedingungen nach dem Informations- und Genehmigungsverfahren dieses Vertrags bereit. Eine pauschale Genehmigung unbenannter Modell- oder Infrastruktur-Anbieter ist damit nicht verbunden. Website-Analyse und KI-Schreibassistenz sind getrennt steuerbar.

### Amazon S3 - optionale Objektablage

Die Anwendung unterstützt Amazon S3 für Datei- und Bildablage mit eu-central-1 als Regionsvorgabe und privatem Bucket. Soweit diese Ablage für Kundendaten eingesetzt wird, dokumentiert der Auftragnehmer die konkret beauftragte Vertragsgesellschaft, Verarbeitungsorte, Leistungen sowie Vertrags- und Transfergrundlagen und teilt sie nach dem vereinbarten Informations- und Genehmigungsverfahren mit. Eine Produktkonfiguration allein begründet keine Genehmigung einer unbestimmten Vertragsgesellschaft. Öffentlich abrufbare E-Mail-Bilder dürfen keine personenbezogenen Dokumente enthalten.

### E-Mail-Versanddienste

Audryo unterstützt Resend, Amazon SES, Mailgun und SMTP-Dienste. Vom Auftraggeber selbst beauftragte Versandkonten werden nach dessen Weisung angebunden; Verantwortlichkeiten und Vertragsketten richten sich nach der tatsächlichen Leistung. Soweit der Auftragnehmer einen Versanddienst für die Verarbeitung von Kundendaten selbst beauftragt, teilt er den konkreten Anbieter einschließlich Leistung, Verarbeitungsorten und Vertrags- und Transfergrundlagen nach dem vereinbarten Informations- und Genehmigungsverfahren mit. Anbieter-Tracking ist zusätzlich im Anbieter-Konto zu begrenzen; Audryo-Einstellungen allein steuern fremde Systeme nicht vollständig.

### Google und vom Kunden gewählte Dienste

Google Sign-In ist optional; Firebase/Google Analytics sind auf der Marketingseite mit Einwilligungssteuerung vorgesehen. Verarbeitung eigener Website- und Betreiberkontodaten ist gesondert von der Kundendaten-Auftragsverarbeitung zu beurteilen. Vom Kunden gewählte CRM-Systeme, Zapier-Ziele, Webhooks und Agenten sind anhand der Integration zuzuordnen; eine Auflistung der Funktionen ist noch keine Genehmigung ihrer Anbieter.

### Pflege des Unterauftragnehmerregisters

Der Auftragnehmer führt das Register der tatsächlich eingesetzten Unterauftragsverarbeiter mit vollständiger Vertragsgesellschaft und Anschrift, Leistung und Datenkategorien, Verarbeitungs- und Supportorten, Auftragsverarbeitungsvereinbarungen, Transfergrundlagen und Zusatzmaßnahmen, weiteren Unteraufträgen und Genehmigungsstand. Er stellt diese Informationen dem Auftraggeber nach den Informations- und Kontrollregelungen dieses Vertrags bereit und hält sie aktuell. Nicht konkret benannte Dienste gelten durch den Download oder die allgemeine Produktnutzung nicht als genehmigt.