Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

zwischen

TODO(ingo-legal-avv-customer-name): [Name des Kunden / der Kundin] TODO(ingo-legal-avv-customer-address): [Anschrift des Kunden / der Kundin]

— nachfolgend **„Verantwortlicher"** —

und

kenaro GmbH TODO(ingo-legal-address): Straße, Hausnummer, PLZ, Ort, Deutschland vertreten durch den Geschäftsführer Ingo Karstein E-Mail: privacy@clickprobe.ai

— nachfolgend **„Auftragsverarbeiter"** —

Präambel

Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen im Rahmen des ClickProbe-Dienstes (Software-as-a-Service zum explorativen, KI-gestützten Testen von Webanwendungen). Im Zuge dieser Leistungserbringung kann der Auftragsverarbeiter Zugang zu personenbezogenen Daten des Verantwortlichen erhalten. Die Parteien schließen daher diesen Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO.

---

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Nutzung des ClickProbe-Dienstes durch den Verantwortlichen gemäß dem zwischen den Parteien geschlossenen Hauptvertrag (Allgemeine Geschäftsbedingungen, abrufbar unter /de/legal/agb).

(2) Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags. Mit Beendigung des Hauptvertrags endet auch dieser Auftragsverarbeitungsvertrag, soweit nachfolgend nichts anderes bestimmt ist.

---

§ 2 Art und Zweck der Verarbeitung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zum Zweck der Erbringung des ClickProbe-Dienstes, das heißt insbesondere:

- Ausführung von KI-gestützten Explorationsläufen auf den vom Verantwortlichen angegebenen Web-Applikationen (URL-Targets),
- Speicherung und Verarbeitung von Screenshots, DOM-Snapshots und Session-Kontext-Daten, die während der Exploration anfallen,
- Bereitstellung der ClickProbe-Weboberfläche (Dashboard, Ergebnisanzeige, Konfiguration) für den Verantwortlichen und dessen autorisierte Nutzer,
- technischer Support und Betrieb der Infrastruktur.

(2) Eine Verarbeitung zu anderen Zwecken ist ohne ausdrückliche Weisung des Verantwortlichen unzulässig.

---

§ 3 Art der personenbezogenen Daten und Kategorien betroffener Personen

(1) Der Auftragsverarbeiter kann im Auftrag des Verantwortlichen folgende Datenkategorien verarbeiten:

Kategorie	Beschreibung	Betroffene
Nutzerkonto-Daten	Name, E-Mail-Adresse, Passwort-Hash des ClickProbe-Kontos	Mitarbeiter des Verantwortlichen
Exploration-Artefakte	Screenshots, DOM-Snapshots, URL-Listen, Session-Protokolle aus den getesteten Web-Apps	Endnutzer der getesteten App (sofern diese personenbezogene Daten enthält)
Rechnungsdaten	Name, E-Mail, Rechnungsadresse (keine Zahlungsdaten — diese liegen bei Stripe)	Rechnungsempfänger des Verantwortlichen
Telemetrie-Daten	Fehler-Stack-Traces, strukturierte Server-Logs, Alert-Payloads (zur Sicherstellung der Betriebsfähigkeit)	Mitarbeiter des Verantwortlichen (primär); Endnutzer (in Fehler-Traces enthalten)

(2) Welche personenbezogenen Daten durch die explorative Erkundung der Ziel-App tatsächlich verarbeitet werden, liegt im Verantwortungsbereich des Verantwortlichen. Der Verantwortliche sichert zu, dass er nur Applikationen testen lässt, für die er die erforderlichen Rechte und Erlaubnisse besitzt.

---

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen hin zu verarbeiten, es sei denn, eine Verarbeitung ist nach dem Unionsrecht oder dem nationalen Recht der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, vorgeschrieben.

(2) Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Der Auftragsverarbeiter ergreift alle erforderlichen Maßnahmen gemäß Art. 32 DSGVO (technisch-organisatorische Maßnahmen, nachfolgend „TOM"). Die TOM sind in Anlage 1 dieses Vertrags beschrieben.

(4) Der Auftragsverarbeiter hält die in Anlage 2 genannten Bedingungen für die Inanspruchnahme von Unterauftragsverarbeitern (Subprocessoren) ein.

(5) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und soweit möglich durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Pflicht des Verantwortlichen, Anträge auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person zu beantworten.

(6) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Art. 32–36 DSGVO genannten Pflichten (Datensicherheit, Meldung bei Datenverletzungen, Folgenabschätzung).

(7) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten dieses Artikels zur Verfügung und ermöglicht Überprüfungen, einschließlich Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu diesen bei. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Ansicht ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften der Union oder der Mitgliedstaaten verstößt.

---

§ 5 Pflichten des Verantwortlichen

(1) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten, die er dem Auftragsverarbeiter bereitstellt oder auf die der Auftragsverarbeiter im Rahmen des Dienstes zugreift, verantwortlich.

(2) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich und vollständig, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bezüglich

datenschutzrechtlicher Bestimmungen feststellt.

(3) Der Verantwortliche erteilt Weisungen ausschließlich in Textform (E-Mail an privacy@clickprobe.ai genügt).

---

§ 6 Unterauftragsverarbeiter

(1) Der Auftragsverarbeiter darf Unterauftragsverarbeiter (weitere Auftragsverarbeiter) nur gemäß den Vorgaben dieses Abschnitts einsetzen.

(2) Der Verantwortlichen erteilt hiermit seine allgemeine schriftliche Genehmigung zum Einsatz der nachfolgend aufgeführten Unterauftragsverarbeiter:

Unterauftragsverarbeiter	Sitz	Zweck
Anthropic PBC	USA (San Francisco, CA)	LLM-Inferenz für Exploration; Verarbeitungsgrundlage: Standardvertragsklauseln (SCCs) + EU Data Processing Addendum (Feb. 2025)
MailJet SAS	Frankreich (Paris)	Transaktions-E-Mail (Registrierung, Rechnungen)
Hetzner Online GmbH	Deutschland (Gunzenhausen)	Hosting der Cloud-Infrastruktur
Stripe Payments Europe Ltd.	Irland (Dublin)	Zahlungsabwicklung (Kreditkartendaten liegen ausschließlich bei Stripe)
Functional Software, Inc. — Sentry	Deutschland (Frankfurt, EU-Region)	Fehler-Monitoring / Error Tracking; Verarbeitung in EU-Datenresidenz; für die US-Muttergesellschaft kommen Standardvertragsklauseln zur Anwendung
Grafana Labs	Deutschland (Frankfurt, EU-Region)	Log-Aggregation (Loki) und On-Call-Alerting; Verarbeitung in EU-Rechenzentren; SCCs für US-Muttergesellschaft

(3) Der Auftragsverarbeiter ist verpflichtet, auch den Unterauftragsverarbeitern dieselben Datenschutzpflichten gemäß Art. 28 Abs. 3 DSGVO aufzuerlegen, die in diesem Vertrag festgelegt sind.

(4) Beabsichtigt der Auftragsverarbeiter, weitere Unterauftragsverarbeiter einzusetzen oder bestehende auszutauschen, informiert er den Verantwortlichen vorab per E-Mail. Der Verantwortliche kann dieser Änderung innerhalb von 14 Tagen widersprechen.

§ 7 Verarbeitung in Drittländern

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten grundsätzlich innerhalb der EU/des EWR oder in Ländern mit Angemessenheitsbeschluss (Art. 45 DSGVO).

(2) Soweit eine Verarbeitung in Drittländern ohne Angemessenheitsbeschluss erfolgt (derzeit: USA durch Unterauftragsverarbeiter Anthropic PBC), liegt eine geeignete Garantie gemäß Art. 46 Abs. 2 lit. c DSGVO in Form von Standardvertragsklauseln (EU-Kommissionsbeschluss 2021/914) vor, ergänzt durch ein Data Processing Addendum mit Supplementary Measures. Für die Unterauftragsverarbeiter Sentry (Functional Software, Inc.) und Grafana Labs findet die tatsächliche Verarbeitung in EU-Rechenzentren (Frankfurt) statt; Standardvertragsklauseln kommen ergänzend zur Anwendung, da die Muttergesellschaften in den USA ansässig sind.

---

§ 8 Technisch-organisatorische Maßnahmen (Anlage 1)

Der Auftragsverarbeiter hat folgende technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO implementiert:

Vertraulichkeit:

- Verschlüsselung aller Daten in Transit über TLS 1.2+ (HTTPS, WSS).
- Verschlüsselung von Daten at Rest (Hetzner-Speicher, AES-256 oder gleichwertig).
- Zugriffskontrolle: Rollenbasiertes Zugriffsmodell (RBAC); produktive Kundendaten nur durch autorisiertes Personal auf Need-to-Know-Basis.
- Trennung von Kunden-Datenbereichen durch logische Mandantenisolation (Tenant-ID-basiertes Datenbankschema).

Integrität:

- Alle Datenbank-Schreiboperationen laufen über versionierte API-Endpunkte; keine direkten DB-Zugriffe aus der Produktionsanwendung.
- Input-Validierung und Ausgabe-Encoding zur Verhinderung von Injection-Angriffen.

Verfügbarkeit:

- Automatisierte Backups (täglich, 30-Tage-Aufbewahrung) auf geographisch getrenntem Hetzner-Volume.
- Monitoring und Alerting über Uptime-Checks (< 5 min Reaktionszeit bei Ausfall).

Belastbarkeit:

- Blue-Green-Deployments zur Minimierung von Deployment-Ausfallzeiten.

- Incident-Response-Prozess mit definierten Eskalationsstufen.

Wiederherstellbarkeit:

- RTO (Recovery Time Objective): < 4 Stunden für vollständige Dienst-Wiederherstellung.
- RPO (Recovery Point Objective): < 24 Stunden (Backup-Intervall).

Überprüfungsverfahren:

- Jährliche interne Überprüfung der TOM.
- Penetrationstests auf Anfrage des Verantwortlichen (nach Vereinbarung).

---

§ 9 Meldepflichten bei Datenpannen

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von **72 Stunden** nach Bekanntwerden per E-Mail an die zuletzt bekannte E-Mail-Adresse des Verantwortlichen sowie an privacy@clickprobe.ai (zur Dokumentation).

(2) Die Meldung enthält mindestens:

- Art der Verletzung,
- Kategorien und ungefähre Anzahl betroffener Datensätze,
- wahrscheinliche Folgen,
- ergriffene oder vorgeschlagene Abhilfemaßnahmen.

---

§ 10 Löschung und Rückgabe nach Vertragsende

(1) Nach Beendigung des Auftrags löscht der Auftragsverarbeiter alle personenbezogenen Daten des Verantwortlichen, die ihm im Rahmen des Auftrags bekannt geworden sind, soweit der Verantwortliche nicht eine Rückgabe (Export) der Daten innerhalb von 30 Tagen nach Vertragsende beantragt.

(2) Exploration-Artefakte (Screenshots, DOM-Snapshots) werden spätestens 90 Tage nach Entstehung gelöscht, sofern kein expliziter Export durch den Verantwortlichen erfolgt.

(3) Steuerlich relevante Daten (Rechnungen, Buchungsdaten) werden für die gesetzlich vorgeschriebene Frist (10 Jahre gem. §§ 147 AO, 257 HGB) aufbewahrt und danach gelöscht. Diese Aufbewahrung erfolgt im Auftrag des Verantwortlichen und unterliegt ebenfalls diesem AVV.

(4) Der Auftragsverarbeiter stellt auf Verlangen den Nachweis der Löschung aus.

---

§ 11 Haftung

(1) Die Haftung der Parteien richtet sich nach den gesetzlichen Vorschriften, insbesondere Art. 82 DSGVO, sowie nach den Haftungsregelungen im Hauptvertrag (AGB § 8).

(2) Verstößt eine Partei gegen ihre Pflichten aus diesem Auftragsverarbeitungsvertrag, haftet sie für den dadurch entstehenden Schaden nach Maßgabe der jeweils einschlägigen gesetzlichen Regelungen.

---

§ 12 Schlussbestimmungen

(1) Dieser Auftragsverarbeitungsvertrag tritt mit Unterzeichnung durch beide Parteien in Kraft und gilt für die Dauer des Hauptvertrags.

(2) Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform (E-Mail genügt).

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

(4) Es gilt deutsches Recht. Gerichtsstand für Kaufleute ist Frankenthal (Pfalz) / Ludwigshafen am Rhein.

Unterschriften

Ort, Datum: _____

Verantwortlicher:

(Unterschrift, Name, Funktion)

Ort, Datum: _____

Auftragsverarbeiter: kenaro GmbH

(Ingo Karstein, Geschäftsführer)

Dieses Dokument ist ein ENTWURF (DRAFT). Es wurde von kenaro GmbH erstellt und ist vor Unterzeichnung von einem qualifizierten deutschen Rechtsanwalt zu prüfen. Stand: 2026-04-22.