

KONTRIB – Informationen für den Datenschutzbeauftragten

Datenfluss, Datenkategorien, Einwilligung, Speicherung, technische und organisatorische Maßnahmen, Unterauftragsverarbeiter und Betroffenenrechte. Stand 17. Oktober 2026, Version 1.3. Herausgeber: KAIH UG (haftungsbeschränkt), Jagenberg 13, 42659 Solingen, Datenschutzkontakt datenschutz@kaih.io.

1. Zweck dieses Dokuments und Rollen

Dieses Dokument beschreibt, welche Daten die Attributionsplattform KONTRIB verarbeitet, auf welchem Weg sie fließen, wo sie gespeichert werden und wie Einwilligungen wirken. Es ergänzt den Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO und dient dem Datenschutzbeauftragten des Kunden als Grundlage für das Verzeichnis der Verarbeitungstätigkeiten, die Datenschutzerklärung der Website und die Einwilligungstexte des Consent-Tools.

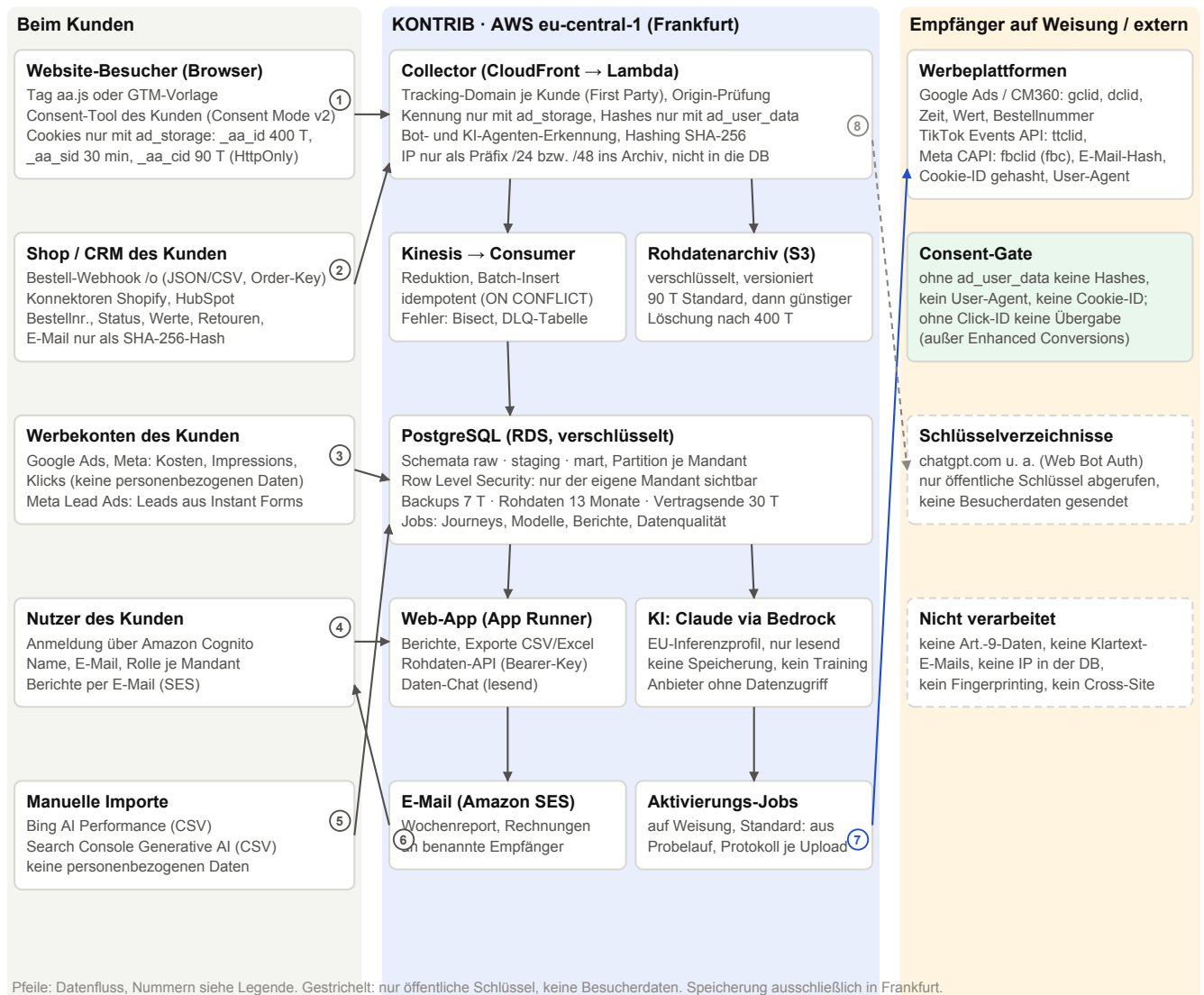
- Verantwortlicher ist der Kunde für die Daten seiner Website-Besucher, Bestellungen und Nutzerkonten. Auftragsverarbeiter ist die KAIH UG (haftungsbeschränkt) ausschließlich zur Bereitstellung von KONTRIB (Tracking, Attribution, Aktivierung, Berichte). Setzt eine Agentur KONTRIB für ihre Kunden ein, bleibt der jeweilige Kunde Verantwortlicher; die Agentur handelt in seinem Auftrag.
- Rechtsgrundlage auf der Website: Das Setzen der First-Party-Kennung und das Auslesen von Click-IDs erfordern eine Einwilligung (§ 25 TDDDG, Art. 6 Abs. 1 lit. a DSGVO), die der Kunde über sein Consent-Tool einholt. KONTRIB liest den Einwilligungsstatus über Google Consent Mode v2 (vier Flags) und verhält sich entsprechend. Ohne Einwilligung werden nur aggregierte Zählwerte ohne Kennung erfasst.
- Weisungen: Die Konfiguration in der Plattform (Kanalregeln, Ziele, Aktivierungskonten, Exporte) gilt als dokumentierte Weisung des Kunden (AVV § 4).

2. Verarbeitungstätigkeiten im Überblick

- Erfassung von Seitenaufrufen, Events und Bestellungen über ein First-Party-Tag (eigene Tracking-Subdomain des Kunden, z. B. `kunde.track.kontrib.io` oder eine Subdomain der Kundendomain) und einen Bestell-Webhook bzw. Konnektoren zu Shop und CRM.
- Bildung von Customer Journeys und Bewertung der Marketingkanäle (Regelmodelle, Markov, Shapley, Grenzkosten), Datenqualitätskennzahlen, Wochenreport.
- Import von Kosten- und Plattformdaten aus den Werbekonten des Kunden (keine personenbezogenen Daten).
- Auf Weisung des Kunden: Rückspielung attribuerter Conversions an Werbeplattformen (Aktivierung); standardmäßig deaktiviert, zunächst im Probelauf.
- Berichte, Exporte, KI-gestützte Auswertungen (Claude über Amazon Bedrock in der EU, nur lesend) und Nutzerverwaltung.

3. Datenflussdiagramm

Alle Komponenten von KONTRIB laufen in der AWS-Region eu-central-1 (Frankfurt). CloudFront liefert das Tag und den Collector-Endpunkt über Edge-Standorte aus; gespeichert wird ausschließlich in Frankfurt.



Legende · 1 Seitenaufrufe, Events, Click-IDs und Consent-Status (Tag → Collector) · 2 Bestellungen über Webhook oder Konnektor (E-Mail nur als Hash) · 3 Kosten- und Plattformdaten, Leads aus Meta Lead Ads · 4 Anmeldung der Nutzer des Kunden · 5 manuelle CSV-Importe ohne personenbezogene Daten · 6 Wochenreport und Rechnungen per E-Mail · 7 Aktivierung auf Weisung: Click-ID, Zeitpunkt, Wert, Bestellnummer, bei Meta zusätzlich E-Mail-Hash und gehashte Cookie-ID nur mit ad_user_data · 8 Abruf öffentlicher Schlüssel signierender KI-Agenten (keine Besucherdaten). Senkrechte Pfeile: Verarbeitung innerhalb von Frankfurt.

4. Datenflüsse im Einzelnen

Nr.	Fluss	Daten und Schutzmaßnahmen	Speicherort
1	Website → Collector	Seitenaufrufe, Events, Referrer, UTM-Parameter, Click-IDs (gclid, gbraid, wbraid, dclid, fbclid, ttclid, msclkid, li_fat_id), Consent-Status, Land und Region (CloudFront-Header), Geräteklasse und Browserfamilie aus dem User-Agent; Cookie-ID nur mit ad_storage; SHA-256-Hash von E-Mail oder Telefon nur mit ad_user_data (Hashing im Collector, kein Klartext); Klartext-User-Agent nur bei Conversion-Events mit ad_user_data (für Meta CAPI). IP-Adresse nur als gekürztes Netzpräfix (/24 bzw. /48) im Rohdatenarchiv, nicht in der Datenbank.	Datenbank und Rohdatenarchiv, Frankfurt
2	Shop/CRM → Bestell-Webhook (/o)	Bestellnummer, Status (erstellt, bezahlt, versandt, storniert, retourniert), Werte, Retouren, Kundensegment, Neu-/Bestandskunde, Lead-ID; E-Mail nur als Hash. Authentifizierung mit Order-Key des Mandanten.	Datenbank, Frankfurt
3	Konnektoren (Abruf)	Shopify, HubSpot: Bestellungen und Leads wie Fluss 2. Google Ads, Meta: Kosten, Impressions, Klicks. Meta Lead Ads: Leads aus Instant Forms des Kunden (Name, E-Mail, Telefon) in das CRM des Kunden innerhalb von KONTRIB. Zugangsdaten des Kunden liegen verschlüsselt in AWS Secrets Manager.	Datenbank, Frankfurt
4	Verarbeitung	Kinesis-Stream → Consumer → PostgreSQL (Schemata raw, staging, mart; Partition je Mandant; Row Level Security). Rohdatenarchiv in S3 über Firehose. Nächtliche Jobs bilden Journeys, Modelle und Berichte.	Frankfurt
5	Nutzung durch den Kunden	Web-App mit Anmeldung über Amazon Cognito (Name, E-Mail, Rolle), Exporte CSV/Excel, Rohdaten-API mit Bearer-Key (nur pseudonyme Daten), Wochenreport und Rechnungen per E-Mail (Amazon SES) an vom Kunden benannte Empfänger.	Frankfurt; E-Mail an Empfänger des Kunden
6	KI-Funktionen	Daten-Chat, Tracking-Assistent, Wochenreport-Texte: Claude über Amazon Bedrock im EU-Inferenzprofil. Prompts und Antworten werden von AWS nicht gespeichert und nicht zum Training verwendet; Anthropic erhält keine Kundendaten. Die KI liest nur den jeweiligen Mandanten.	EU (AWS)
7	Aktivierung (auf Weisung)	Google Ads und Campaign Manager 360: Click-ID, Conversion-Zeitpunkt, Wert, Bestellnummer; Enhanced Conversions (gehashte E-Mail) nur als Fallback ohne Click-ID und nur mit ad_user_data. Meta Conversions API: fbclid als fbc, E-Mail-Hash, gehashte Cookie-ID, User-Agent, Event-ID zur Deduplizierung gegen das Pixel – alles nur mit ad_user_data. TikTok Events API: ttclid, E-Mail-Hash, gehashte Cookie-ID, User-Agent, Event-ID – ebenfalls nur mit ad_user_data. Jede Aktivierung ist standardmäßig aus und protokolliert jeden Upload.	Plattformen (eigene Verantwortung des Kunden gegenüber der Plattform)
8	Externe Abrufe ohne Besucherdaten	Zur Erkennung signierender KI-Agenten (Web Bot Auth, RFC 9421) ruft der Collector das öffentliche Schlüsselverzeichnis des Agenten ab (z. B. chatgpt.com). Dabei werden keine Besucherdaten übermittelt.	–
9	Manuelle Importe	Bing AI Performance und Search-Console-Bericht „Generative AI“ als CSV (Zitate bzw. Impressionen je Tag und Seite, keine personenbezogenen Daten).	Datenbank, Frankfurt

5. Einwilligung (Google Consent Mode v2)

Das Tag liest die vier Consent-Mode-Flags des Consent-Tools (Cookiebot, Usercentrics, Borlabs, OneTrust und andere; alternativ direkt per aa('consent', ...)). Änderungen wirken sofort; ein Widerruf ruft zusätzlich den Endpunkt /revoke auf, der alle Collector-Cookies löscht und kein Event speichert.

Flag	Wirkung in KONTRIB
ad_storage	Persistente First-Party-Kennung (Cookie _aa_id) und Click-ID-Cookie werden gesetzt; Journeys über mehrere Sitzungen möglich. Ohne: keine Kennung, nur Session-ID (30 Minuten), nur aggregierte Zählwerte.
ad_user_data	Gehashte E-Mail/Telefon aus Pixel oder Bestellung werden gespeichert (Identity-Stitching, Enhanced Conversions, Meta CAPI); Klartext-User-Agent bei Conversion-Events. Ohne: keine Hashes, keine Weitergabe von Identifikatoren an Plattformen.

Flag	Wirkung in KONTRIB
ad_personalization	Wird erfasst und mit dem Event gespeichert; KONTRIB nutzt das Flag nicht für eigene Verarbeitung, es steht den Plattformen (Consent Mode) zur Verfügung.
analytics_storage	Wird erfasst und mit dem Event gespeichert; Statistik-Auswertungen in KONTRIB arbeiten ohne eigene Kennung, wenn ad_storage fehlt.

6. Cookies und Browser-Speicher

Name	Zweck	Laufzeit	Eigenschaften
_aa_id	Pseudonyme Besuchererkennung (Zufallswert) für Journeys über mehrere Sitzungen	400 Tage	HttpOnly, Secure, First Party auf der Tracking-Domain des Kunden; nur mit ad_storage
_aa_sid	Sitzungskennung	30 Minuten	HttpOnly, Secure
_aa_cid	Zuletzt gesehene Click-IDs (gclid, fbclid ...) mit Zeitstempel für die Aktivierung	90 Tage	HttpOnly, Secure; nur mit ad_storage
sessionStorage _aa_eng	Engagement der Sitzung (Seitenzahl, aktive Sekunden, letzte Pfade) für Soft Conversions	Sitzung	keine Kennung, nur im Browser

Die Cookies werden vom Collector gesetzt (nicht per JavaScript lesbar), bleiben auf der Tracking-Domain des jeweiligen Kunden und werden nicht domainübergreifend verwendet. Es gibt kein Fingerprinting. Optionale „probabilistische Brücke“ (standardmäßig aus): Auf ausdrückliche Weisung des Kunden und nur nach Freigabe durch dessen Datenschutzbeauftragten kann KONTRIB eine Sitzung im In-App-Browser (WebView einer Social-App) mit einer kurz darauf folgenden Direct-Sitzung im System-Browser desselben Geräts verbinden. Dafür bildet der Collector bei Sitzungsstarts mit Einwilligung ad_storage einen Sitzungsschlüssel als SHA-256 über gekürztes IP-Präfix (/24 bzw. /48), Geräteklasse und Land mit einem geheimen Salt; der Schlüssel ist ohne den Salt nicht auf das Präfix zurückrechenbar, wird nach drei Tagen gelöscht und verbindet nur Sitzungen innerhalb eines Zeitfensters (Standard sechs Stunden) mit genau einem oder zwei Kandidaten (Konfidenz 0,8 bzw. 0,5). Die Verknüpfungen werden mit Konfidenz gespeichert, Journeys und Datenqualität weisen sie als Schätzung aus. Ist die Funktion aus, entsteht kein Schlüssel.

7. Speicherung, Aufbewahrung und Löschung

Ort	Inhalt	Schutz	Aufbewahrung
PostgreSQL (Amazon RDS), Frankfurt	Rohereignisse, Bestellungen, Journeys, Modelle, Berichte, Konfiguration; Sitzungsschlüssel der optionalen Brücke nur drei Tage	Verschlüsselung at rest (KMS), TLS, Row Level Security, Partition je Mandant, Löschschutz	Rohdaten nach vereinbarter Frist (Standard 13 Monate); automatische Backups 7 Tage
Rohdatenarchiv (Amazon S3), Frankfurt	Kopie aller Collector-Datensätze (inkl. gekürztem IP-Präfix)	Verschlüsselung, Versionierung, kein öffentlicher Zugriff	90 Tage Standardklasse, danach günstigere Klasse, Löschung nach 400 Tagen
Protokolle (CloudWatch)	Technische Laufzeitprotokolle ohne Nutzdaten	Zugriff nur Betrieb	14 Tage
Secrets Manager	Zugangsdaten zu Werbekonten, Shop und CRM des Kunden	KMS-verschlüsselt, Zugriff nur für die jeweilige Funktion	Laufzeit des Vertrags
Vertragsende	Alle Daten des Mandanten	Export (CSV, Excel, JSON, Rohdatenarchiv) auf Anforderung	Löschung innerhalb von 30 Tagen, Bestätigung in Textform

8. Technische und organisatorische Maßnahmen

Bereich	Maßnahme
Standort	Ausschließlich AWS eu-central-1 (Frankfurt). Auslieferung des Tags über CloudFront mit Edge-Standorten, Speicherung nur in Frankfurt.
Einwilligung	Consent Mode v2 mit vier Flags. Ohne Einwilligung keine Kennung, nur aggregierte Zählwerte. Änderungen der Einwilligung werden sofort wirksam.
Pseudonymisierung	E-Mail und Telefon werden im Collector gehasht (SHA-256, normalisiert). IP-Adressen werden nicht in der Datenbank gespeichert; im Archiv nur als Netzpräfix.

Bereich	Maßnahme
Zugriffskontrolle am Collector	Treffer werden nur von den Site-Domains des Kunden angenommen (Origin-Prüfung); Bestell- und Serverschnittstellen mit mandantenspezifischem Schlüssel; Bot- und KI-Crawler-Erkennung.
Mandantentrennung	Partitionierung je Mandant und Row Level Security in PostgreSQL; die Anwendung sieht nur den Mandanten des angemeldeten Nutzers.
Verschlüsselung	TLS 1.2+ auf allen Strecken, Verschlüsselung at rest für Datenbank, Rohdatenarchiv und Secrets (AWS KMS).
Zugriff	Anmeldung über Amazon Cognito, Rollen agency_admin, agency_planner, client_admin, client_viewer; administrative Zugriffe werden protokolliert.
KI	Claude über Amazon Bedrock im EU-Inferenzprofil, nur lesender Zugriff auf den jeweiligen Mandanten; keine Speicherung, kein Training.
Betrieb	Infrastruktur als Code (Terraform), Deployments nachvollziehbar, Datenbank mit Löschschutz; Zwischenfälle werden dokumentiert.

9. Unterauftragsverarbeiter und Empfänger

Unternehmen	Zweck	Standort	Garantie
Amazon Web Services EMEA SARL, Luxemburg	Hosting, Datenbank, Streaming, Speicher, E-Mail-Versand, KI-Inferenz (Amazon Bedrock)	EU, Frankfurt	AVV mit EU-Standardvertragsklauseln, EU-US Data Privacy Framework
Anthropic (Modell Claude, ausschließlich über Amazon Bedrock)	Bereitstellung des Sprachmodells	Ausführung in der EU durch AWS	Kein Datenzugriff, keine Speicherung, kein Training
DocuSign, Inc.	Nur elektronische Unterzeichnung der Verträge (Name, E-Mail des Unterzeichners, Bankdaten des SEPA-Mandats)	EU-Rechenzentrum	Standardvertragsklauseln; keine Verarbeitung von Plattformdaten

Empfänger auf Weisung des Kunden (keine Unterauftragsverarbeiter, sondern eigene Verantwortliche): Google Ads, Campaign Manager 360, Meta, TikTok und die Affiliate-Netzwerke Awin, ADCELL, Tradedoubler und Webgains erhalten bei aktivierter Aktivierung die in Fluss 7 genannten Daten. KI-Connector (MCP): Schaltet der Kunde den Connector frei und verbindet ein KI-Werkzeug (z. B. Claude) mit seinem API-Schlüssel, übermittelt er Berichtsdaten (Kanalkennzahlen, Journeys ohne Cookie-IDs und Hashes, Datenqualität) an den KI-Anbieter seiner Wahl; das geschieht auf seine Weisung und außerhalb der Auftragsverarbeitung durch KAIH. Weitere Unterauftragsverarbeiter setzt KAIH nur nach vorheriger Information in Textform ein; der Kunde kann innerhalb von 14 Tagen aus wichtigem Grund widersprechen.

10. Betroffenenrechte und Unterstützung

- **Widerruf:** Das Consent-Tool des Kunden setzt die Flags zurück; KONTRIB stoppt weitere Events und löscht über /revoke alle Collector-Cookies.
- **Auskunft und Löschung:** Gespeichert sind pseudonyme Kennungen. Ein Betroffener kann über seine Cookie-ID (im Browser nicht auslesbar, aber vom Kunden über ein Hilfsskript ermittelbar) oder über den Hash seiner E-Mail-Adresse zugeordnet werden; KAIH stellt auf Weisung des Kunden Auskunft bereit und löscht die zugehörigen Datensätze in Datenbank und Archiv. Anfragen, die bei KAIH eingehen, werden innerhalb von 48 Stunden an den Kunden weitergeleitet.
- **Datenübertragbarkeit und Export:** Rohdaten-API (JSON, Cursor-Paginierung, nur pseudonyme Felder) und Exporte CSV/Excel in der App.
- **Datenschutzverletzungen:** Meldung an den Kunden unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, mit Art, betroffenen Kategorien und Personen, Folgen und Maßnahmen.
- **Kontrollrechte:** Prüfung nach Abstimmung einmal jährlich; KAIH kann die Prüfung durch aktuelle Nachweise erfüllen (AVV § 10).

11. Besucherklassen: Bots und KI-Agenten

Der Collector erkennt Crawler und Suchmaschinen (darunter die KI-Crawler GPTBot, ClaudeBot, PerplexityBot, Google-Extended) am User-Agent und schließt sie aus den Auswertungen aus. KI-Agenten, die im Auftrag eines Menschen handeln (ChatGPT agent, Claude, Perplexity), werden als eigene Besucherklasse geführt: Erkennung am User-Agent-Marker

des Anbieters oder an der signierten Kennung nach Web Bot Auth (RFC 9421). Zur Signaturprüfung ruft der Collector nur das öffentliche Schlüsselverzeichnis des Anbieters ab; Besucherdaten verlassen die Plattform dabei nicht. Die Klasse dient der Datenqualität und wird in Datenqualität, Traffic und Journeys ausgewiesen.

12. Was nicht verarbeitet wird

- Keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO); der Kunde stellt sicher, dass solche Daten nicht übermittelt werden.
- Keine Klartext-E-Mail-Adressen oder Telefonnummern von Website-Besuchern; keine IP-Adressen in der Datenbank.
- Kein Fingerprinting, kein domainübergreifendes Tracking, keine Weitergabe an Dritte außerhalb der in Abschnitt 9 genannten Empfänger auf Weisung.
- Keine Nutzung von Kundendaten zum Training von KI-Modellen.

13. Änderungsstand

Version	Datum	Änderung
1.0	17. Oktober 2026	Erstfassung; berücksichtigt Meta Conversions API als Aktivierungsplattform, Identity-Stitching über E-Mail-Hash, Origin-Prüfung am Collector, Besucherklasse KI-Agent und den Search-Console-Import.
1.3	17. Oktober 2026	Empfänger auf Weisung um die Affiliate-Netzwerke (Awin, ADCELL, Tradedoubler, Webgains) und den KI-Connector (MCP, Berichtsdaten an den vom Kunden gewählten KI-Anbieter) ergänzt.
1.2	17. Oktober 2026	Korrektur: Microsoft Advertising ist keine Aktivierungsplattform (msclid wird nur als Click-ID erfasst); TikTok Events API als Empfänger auf Weisung ergänzt.
1.1	17. Oktober 2026	Optionale probabilistische Brücke beschrieben (Abschnitt 6): standardmäßig aus, nur nach Freigabe des Datenschutzbeauftragten, gesalzener Sitzungsschlüssel aus IP-Präfix, Geräteklasse und Land, Löschung nach drei Tagen, Konfidenz je Verknüpfung.

Dieses Dokument beschreibt den technischen Stand der Plattform; es ersetzt weder den AVV noch eine rechtliche Prüfung der Einwilligungstexte und Datenschutzerklärung des Kunden. Fragen: datenschutz@kaih.io.