

# Verzeichnis von Verarbeitungstätigkeiten

## Record of Processing Activities (Art. 30 GDPR)

### CIATA DeepResearch — Controller Record

**Version:** 1.11 **Date:** 2026-10-08 **Status:** Draft — not yet reviewed by external legal counsel **Next review due:** On any material change to processing; mandatory annual review **Prepared by:** Prof. Dr. Tim Landgraf, Managing Director, CIATA GmbH

**Note on mandatory update duty.** This record must be updated whenever the processing activities described herein change in any material respect — including changes to purposes, data categories, sub-processors, retention periods, or technical measures. A supervisory authority (in this case the Berliner Beauftragte für Datenschutz und Informationsfreiheit, BlnBDI) will request this document first in any inspection or enforcement proceeding. An out-of-date ROPA is itself a violation of Art. 30(4) GDPR.

**Note on status.** This record has not been reviewed by external legal counsel. It reflects the technical state of the system as at 2026-08-11, cross-checked against source code and the following internal documents: LAW\_FIRM\_BRIEFING.md v1.2, ZDR\_STATEMENT.md v2.1, DPIA.md v1.2, and LIA.md v1.2 (all dated 2026-08-11). Where source documents and code disagree, this record follows the code.

## 1. Controller Information

| Field                          | Value                                                                                                                                                                                                                                                                           |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Controller</b>              | CIATA GmbH                                                                                                                                                                                                                                                                      |
| <b>Address</b>                 | Arnimallee 7, 14195 Berlin, Germany                                                                                                                                                                                                                                             |
| <b>Commercial Register</b>     | HRB 266084 B, Amtsgericht Charlottenburg                                                                                                                                                                                                                                        |
| <b>Managing Director</b>       | Prof. Dr. Tim Landgraf                                                                                                                                                                                                                                                          |
| <b>Data Protection Contact</b> | privacy@ciata.io                                                                                                                                                                                                                                                                |
| <b>Data Protection Officer</b> | Not designated. <a href="#">⚠ Open item:</a> § 38(1) sentence 2 BDSG provides that a DPO is mandatory, regardless of headcount, where processing is subject to a mandatory DPIA under Art. 35 GDPR. The DPIA (DPIA-DR-2026-01, §1.1) concludes that a DPIA is required for this |

| Field | Value                                                                                                                                                                        |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | processing. If that conclusion is correct, a DPO appointment is likely mandatory. This must be assessed and resolved before this record is considered complete. See DPIA §7. |

## 2. Processor-Status Note

CIATA GmbH acts as **controller** for all activities described in this record. The record covers controller-side obligations under Art. 30(1) GDPR.

Where CIATA engages external processors, those processors are listed under each activity. **As of 2026-08-11, no Art. 28 GDPR Data Processing Agreement has been executed with any sub-processor.** The required DPAs are identified as outstanding for each recipient where applicable. Until DPAs are executed, any statement in supporting documents that a processor applies particular safeguards (zero retention, no training use) reflects an intended contractual basis only, not a confirmed one.

## 3. General Description of Technical and Organisational Security Measures (Art. 30(1)(g))

The following measures apply across all processing activities unless a specific activity states otherwise. They are described in detail in DPIA §4 and LAW\_FIRM\_BRIEFING §6.

### 3.1 Technical Measures

| Measure                      | Implementation                                                                                                                                                                                                                                 |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Encryption in transit        | HTTPS/TLS via Caddy reverse proxy (automatic certificate provisioning, Let's Encrypt)                                                                                                                                                          |
| Password hashing             | bcrypt with salt (bcrypt library); hashed values only stored, never plaintext                                                                                                                                                                  |
| Authentication               | JWT access tokens (60-minute TTL) and refresh tokens (7-day TTL); per-user API keys (bcrypt-hashed, dr_* prefix)                                                                                                                               |
| Server-side token revocation | token_version counter in users table (schema v12); password change/reset increments counter, invalidating all outstanding tokens immediately, irrespective of TTL                                                                              |
| Authorisation                | Per-endpoint ownership verification on all data-returning endpoints; no administrative override that allows one user's data to be read by another user via the API                                                                             |
| Rate limiting                | 30 requests per 60 seconds per API key (configurable)                                                                                                                                                                                          |
| PII filter                   | Regex-based scrubbing applied to all web page content before LLM submission and before storage; covers emails, phone numbers, IBANs, credit card numbers (Luhn-validated), DE Steuerliche Identifikationsnummer, DE Sozialversicherungsnummer, |

| Measure                     | Implementation                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             | Swiss AHV/AVS, IPv4 addresses, German postal address patterns; does NOT cover personal names or non-DACH national identifiers                                                                                                                                                                                                                                                                            |
| Content truncation          | Maximum 16,000 characters per source page in production                                                                                                                                                                                                                                                                                                                                                  |
| Automated retention cleanup | Background timer runs every 24 hours; deletes run directories older than DATA_RETENTION_DAYS (default 30 days)                                                                                                                                                                                                                                                                                           |
| User-initiated deletion     | DELETE /v1/research/{job_id} (immediate); DELETE /v1/auth/me (requires password; soft-deletes account and queues run deletion)                                                                                                                                                                                                                                                                           |
| In-flight erasure           | Worker re-checks account is_active before job start and at each research iteration; deleted account's queued or in-progress jobs are aborted                                                                                                                                                                                                                                                             |
| Encryption at rest          | <b>Not enabled.</b> Production Hetzner Cloud volumes (Docker ./runs and ./data) are not encrypted at rest (confirmed 2026-07-15, accepted gap). Compensating controls: bcrypt hashing, TLS in transit, per-user access isolation, 30-day retention, encrypted off-site backups. Enabling volume-level LUKS/dm-crypt before hot-production cutover remains a recommended hardening step (DPIA action A1). |
| Off-site backups            | Encrypted backups stored geo-redundantly within the EU (Hetzner Frankfurt → Helsinki)                                                                                                                                                                                                                                                                                                                    |
| Container security          | Non-root Docker container (UID 1000)                                                                                                                                                                                                                                                                                                                                                                     |
| Request IDs                 | Every request assigned a unique ID for audit trail correlation                                                                                                                                                                                                                                                                                                                                           |
| robots.txt compliance       | Checked before every direct page fetch by CIATA; per-domain in-memory cache (1-hour TTL); graceful-allow fallback if robots.txt is unreachable. Not applied to pages Staan retrieves server-side.                                                                                                                                                                                                        |
| Web-crawling rate limiting  | Minimum 1 second between direct fetches to the same domain                                                                                                                                                                                                                                                                                                                                               |
| Honest bot identification   | User-Agent: CIATA-DeepResearch/1.0 (+https://research.ciata.io; bot; contact: privacy@ciata.io)                                                                                                                                                                                                                                                                                                          |
| Input sanitisation          | Research questions stripped of VSRMark variation selectors and zero-width characters at API ingestion                                                                                                                                                                                                                                                                                                    |
| AI content disclosure       | VSRMark invisible Unicode variation-selector watermark and visible "AI-generated" label embedded in every report (EU AI Act Art. 50(2))                                                                                                                                                                                                                                                                  |

## 3.2 Organisational Measures

| Measure                        | Status                                                        |
|--------------------------------|---------------------------------------------------------------|
| DPIA                           | Completed — DPIA-DR-2026-01 v1.2, 2026-08-11                  |
| Legitimate Interest Assessment | Completed — LIA-DR-2026-01 v1.2, 2026-08-11                   |
| Privacy policy                 | Published at research.ciata.io/privacy.html (bilingual DE/EN) |

| Measure                              | Status                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data protection contact              | privacy@ciata.io                                                                                                                                                                                                                                                                                                                       |
| Data subject rights                  | Art. 15–22 exercisable via privacy@ciata.io; 30-day response per Art. 12(3); Art. 17 self-service deletion implemented                                                                                                                                                                                                                 |
| Art. 21 objection mechanism          | privacy@ciata.io                                                                                                                                                                                                                                                                                                                       |
| Annual DPIA review                   | Scheduled; next due 2027-06-18                                                                                                                                                                                                                                                                                                         |
| Sub-processor DPAs                   | ⚠ Required; none yet executed (see each activity below)                                                                                                                                                                                                                                                                                |
| Incident-response / breach procedure | Documented in INCIDENT_RESPONSE.md (v1.0, 2026-08-11): 72-hour workflow, severity triage, notification templates and Art. 33(5) breach-register specification. ⚠ Not yet externally reviewed or rehearsed; the breach-register file itself does not yet exist, and every incident role currently rests on the Managing Director alone. |
| Standalone Art. 32 TOM document      | Produced — TOM.md v1.0 (2026-08-11), structured to the standard German AVV Anlage categories and suitable as a customer-DPA schedule. ⚠ Not yet externally reviewed.                                                                                                                                                                   |
| DPO designation                      | ⚠ See §1 above                                                                                                                                                                                                                                                                                                                         |

## 4. Processing Activities

### Activity 1 — User Account Management and Authentication

| Field                              | Content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reference</b>                   | ROPA-DR-01                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Purpose</b>                     | Registration of user accounts; authentication and session management; email address verification; password reset; account lifecycle management (deactivation, soft-deletion); credit balance tracking; API key management                                                                                                                                                                                                                                                                              |
| <b>Legal basis</b>                 | Art. 6(1)(b) GDPR — performance of contract (provision of the DeepResearch service requires an authenticated account)                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Categories of data subjects</b> | Registered users (B2B account holders and individual users)                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Categories of personal data</b> | Email address; name (optional, may be empty); bcrypt-hashed password; email verification token (temporary, up to 72 h); password reset token (temporary, up to 1 h); is_business self-declaration (Boolean: consumer/B2B, set at first purchase); credit balance and credit transaction history; account creation timestamp; token_version counter (session generation for server-side JWT revocation); SHA-256 hash of deleted-account email (retained after deletion for re-registration prevention) |
| <b>Authentication artefacts</b>    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Field                              | Content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                    | JWT access tokens (60-minute TTL; stored client-side in browser localStorage, not on server); JWT refresh tokens (7-day TTL; validated against token_version); per-user API keys (bcrypt-hashed hash stored; raw key shown once only, prefix dr_*)                                                                                                                                                                                                                                                                                            |
| <b>Categories of recipients</b>    | Hetzner Online GmbH (cloud infrastructure hosting, Germany) — <a href="#">Art. 28 DPA</a> required, not yet executed; Scaleway SAS (transactional email for email verification, password reset, purchase confirmation, and report-ready notification — see Activity 5)                                                                                                                                                                                                                                                                        |
| <b>Third-country transfers</b>     | None. All processing within the EEA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Envisaged erasure deadlines</b> | Account data: cleared on account deletion (soft-delete replaces email, name, and password hash with placeholder values; SHA-256 email hash retained indefinitely for re-registration prevention); unverified accounts auto-deleted after 72 hours if email verification not completed; JWT refresh tokens: 7 days; API keys: until revoked or on account deletion; usage logs (usage_log table) and credit transaction history (credit_transactions table): <a href="#">Art. 17(1) GDPR</a> retention period not yet defined — see Open Items |

## Activity 2 — Research Job Execution (Core Product)

| Field                              | Content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reference</b>                   | ROPA-DR-02                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Purpose</b>                     | Processing user-submitted research questions through the autonomous AI research pipeline; generating, storing, and delivering research reports; operating the credit system; providing real-time progress updates via Server-Sent Events                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Legal basis</b>                 | Art. 6(1)(b) GDPR — performance of contract                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Categories of data subjects</b> | Registered users who submit research jobs; incidentally, individuals whose personal data may appear in research questions submitted by users (CIATA cannot screen incoming questions for personal data content)                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Categories of personal data</b> | Research question text (user-submitted, up to 4,000 characters); LLM-generated sub-questions; coverage scores and iteration metadata; extracted findings (PII-filtered fact text with source URLs); generated research report (Markdown text with citations and methodology); VSRMark watermark payload (producer id, version, ai_generated: true, job_id, UTC timestamp — embedded in report text); AI provenance HTML comment (embedded in report); synthesis_route flag (records which writer produced the report); job credit deduction record. Run provenance metadata (schema_version, code_revision, agent_models, config_digest) is operational metadata and is not personal data. |
| <b>LLM processing via AKI.io</b>   | Research question and derived content (sub-questions, queries, PII-filtered page text, findings) are sent to AKI.io GmbH for LLM inference. Models in use: gpt-oss-120b (reasoning agents: Decomposer, Re-decomposer, Query Generator, Evaluator, Entity Extractor, Scope Analyzer, Intent Classifier, Outliner, Glossary, Relevance Gate; Figure Sheet disabled by default), qwen3.8-72b (Synthesizer, Section Writer, Table Repair, Paragraph Checker, Consistency Checker, Report Patcher), gemma4-chat-26b (Extractor and Language Guard, reasoning disabled). Zero retention at AKI.io is the intended contractual basis; <a href="#">Art. 28 DPA</a> AKI.io DPA not yet executed.    |

| Field                              | Content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Search processing via Staan</b> | Derived search queries (not the original research question) are sent to Staan / European Perspective SAS. Staan keeps them for 25 months (Staan DPA, Appendix 1, on file) and treats them as not personal data (DPA §2). Staan's FAQ says an unnamed US fallback can supplement results, so some queries may leave the EU; the DPA does not list it. CIATA has asked Staan to switch it off for its account (issue #194).                                                                                                                                                                                                                                                                                   |
| <b>Categories of recipients</b>    | AKI.io GmbH (LLM inference, Frankfurt DE) — <a href="#">△</a> Art. 28 DPA required, not yet executed; DPA must explicitly cover all three model IDs currently in use (gpt-oss-120b, qwen3.8-27b, gemma4-chat-26b) and past processing on qwen3.6-chat-35b (in use until 2026-09-27); Staan / European Perspective SAS (web search, EU) — <a href="#">△</a> Art. 28 DPA required, not yet executed; Hetzner Online GmbH (infrastructure hosting, Germany) — <a href="#">△</a> Art. 28 DPA required, not yet executed; Scaleway SAS (receives report title and short summary for the report-ready notification email, Paris FR — <a href="#">△</a> Art. 28 DPA pending acceptance and filing; see Activity 5) |
| <b>Third-country transfers</b>     | None in default production configuration (all sub-processors within EEA). Conditional on SEARCH_BACKEND=staan being active in production — <a href="#">△</a> not yet confirmed; see Open Items.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Envisaged erasure deadlines</b> | Research state (state.json) and report (report.md): deleted automatically 30 days after job creation by background cleanup timer (DATA_RETENTION_DAYS); user-initiated early deletion available at any time via DELETE /v1/research/{job_id}; all research jobs deleted on account deletion.                                                                                                                                                                                                                                                                                                                                                                                                                |

### Activity 3 — Web Retrieval and Page-Content Processing

| Field                              | Content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reference</b>                   | ROPA-DR-03                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Purpose</b>                     | Programmatic reading of publicly accessible web pages to extract factual information for AI-generated research reports; diagnostic retention of PII-filtered extractor input per source to enable analysis of zero-yield sources                                                                                                                                                                                                                                                                                         |
| <b>Legal basis</b>                 | Art. 6(1)(f) GDPR — Legitimate Interest. Cross-reference: LIA-DR-2026-01, Activity A (version 1.2, 2026-08-11). The legitimate interests of CIATA and its users in providing and using AI research capabilities outweigh the residual impact on data subjects, given the safeguards applied (PII filter, 30-day TTL, access restriction, and AKI.io's no-training commitment — the DPA giving that commitment contractual effect is not yet executed).                                                                   |
| <b>Categories of data subjects</b> | Third-party individuals whose personal data appears incidentally in publicly accessible web pages retrieved during research jobs. These individuals have no direct relationship with CIATA.                                                                                                                                                                                                                                                                                                                              |
| <b>Categories of personal data</b> | PII-filtered web page text (raw unfiltered text is never stored; the PII filter runs before any text is written to disk): structured personal identifiers covered by the PII filter are replaced with placeholder tags before storage or LLM submission; the stored copy may still contain personal names and non-DACH national identifiers (filter limitation — see DPIA §2.2 and LIA §A.2). PII-filtered extractor input is capped at 16,000 characters per source and retained in state.json for diagnostic purposes. |
| <b>Categories of recipients</b>    | Staan / European Perspective SAS (server-side full_content page fetch — in production-default configuration, Staan fetches result pages on CIATA's behalf before CIATA's PII filter is applied; <a href="#">△</a> Staan DPA must explicitly cover this full_content flow; not yet                                                                                                                                                                                                                                        |

| Field                                         | Content                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                               | executed); AKI.io GmbH (receives PII-filtered page text for fact extraction, Frankfurt DE — <a href="#">Art. 28 DPA</a> required, not yet executed); Hetzner Online GmbH (storage of PII-filtered extractor input, Germany — <a href="#">Art. 28 DPA</a> required, not yet executed)                               |
| <b>Third-country transfers</b>                | None in default production configuration. Conditional on SEARCH_BACKEND=staan; see Open Items.                                                                                                                                                                                                                     |
| <b>Access restriction on stored page text</b> | The stored PII-filtered extractor input (page_text field in state.json) is accessible via GET /v1/admin/reports/{job_id}/sources/{i}/text only to a caller who simultaneously holds the admin role AND owns the specific run. No CIATA staff member can use this endpoint to read another user's stored page text. |
| <b>Envisaged erasure deadlines</b>            | 30 days from job creation (deleted with the run state); user-initiated early deletion via DELETE /v1/research/{job_id}.                                                                                                                                                                                            |

## Activity 4 — Billing, Payments, and Invoicing

| Field                              | Content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reference</b>                   | ROPA-DR-04                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Purpose</b>                     | Processing credit pack purchases (including payment session creation, webhook handling, and credit granting); generating VAT-compliant invoices; maintaining payment records in compliance with § 147 AO (German commercial law, 10-year retention obligation)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Legal basis</b>                 | Art. 6(1)(b) GDPR — performance of contract (credit purchase and service access); Art. 6(1)(c) GDPR — legal obligation (§ 147 AO invoice retention; § 14 / § 14a UStG invoicing duty)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Categories of data subjects</b> | Registered users who purchase credit packs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Categories of personal data</b> | At CIATA: Mollie payment ID, credit pack metadata (pack_id, credits, locale), CIATA-internal user_id, purchase timestamp (processed_payments table); Qonto invoice ID (cross-reference in processed_payments.qonto_invoice_id). B2B billing profile (company_profiles table, schema v8): organization_name, given_name, family_name, email, street_and_number, postal_code, city, country, VAT number (USt-IdNr.), Handelsregister registration number; collected only from users who elect B2B/invoice payment. is_business self-declaration flag (users table). Card details are processed exclusively by Mollie and never transmitted to or stored by CIATA.                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Categories of recipients</b>    | Mollie B.V. (payment processing, Amsterdam NL) — receives payment amount, currency, CIATA-internal user_id, pack_id, credits, locale; receives billing address for Billie-method purchases; <a href="#">Art. 28 DPA</a> required, not yet executed. Billie GmbH (B2B BNPL embedded in Mollie checkout, Berlin DE) — receives given name, family name, organization name, street, postal code, city, country, VAT number, Handelsregister number for credit underwriting; <b>treated as independent controller</b> (BNPL credit decision reached via Mollie's checkout, not a direct CIATA integration) — no Art. 28 DPA required on this basis; Art. 13/14 disclosure provided in privacy policy §6; <a href="#">Art. 28 DPA</a> classification to be confirmed with counsel. Qonto (invoicing, Paris FR) — receives buyer name, email, full billing address, VAT number, and Mollie payment reference for every completed purchase; <b>treated as independent controller</b> (licensed payment institution acting in its own name) — no Art. 28 DPA required |

| Field                              | Content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                    | on this basis; Art. 13/14 disclosure provided in privacy policy §6; <a href="#">△</a> classification to be confirmed with counsel. Hetzner Online GmbH (CIATA's own payment record storage, Germany) — <a href="#">△</a> Art. 28 DPA required, not yet executed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Third-country transfers</b>     | None. All recipients within the EEA (NL, DE, FR).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Envisaged erasure deadlines</b> | CIATA's payment records (processed_payments table): 10 years (§ 147 AO). B2B billing profile (company_profiles table): retained while the account exists; on account deletion it is marked and deleted 90 days later by the hourly cleanup (#193). The invoices issued from it are kept by Qonto for the statutory retention period, which is where the § 147 AO obligation is met; counsel to confirm (DPIA action A8, OI-08). Billing data held by Mollie: governed by Mollie's regulatory obligations; CIATA account deletion does not erase Mollie records. Invoicing data held by Qonto: governed by Qonto's regulatory obligations (French commercial law minimum 10 years). BNPL underwriting data held by Billie: governed by Billie's regulatory obligations. |

## Activity 5 — Transactional Email

| Field                              | Content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reference</b>                   | ROPA-DR-05                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Purpose</b>                     | Sending transactional emails necessary for contract performance: email address verification; password reset; purchase confirmation; report-ready notification (sent to the account owner when an AI research report is complete)                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Legal basis</b>                 | Art. 6(1)(b) GDPR — performance of contract                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Categories of data subjects</b> | Registered users                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Categories of personal data</b> | Recipient email address; name (if given); email verification link or password reset link (containing a temporary token, single-use, time-limited); purchase confirmation content (credits purchased, pack label, price, new credit balance, Mollie payment reference, purchase date); report-ready notification content: report title, a short summary of the report (first paragraph of its executive summary, up to approximately 500 characters), link to the report, the report's deletion date. The report-ready notification is on by default; users can turn it off in account settings (Notifications).                                                                   |
| <b>Categories of recipients</b>    | Scaleway SAS (Scaleway Transactional Email, fr-par region, Paris FR) — current provider from 2026-09-26; <a href="#">△</a> Art. 28 DPA: Scaleway publishes a standard DPA (version June 2024, <a href="https://www-uploads.scaleway.com/DPA_2024_ENG_b0abb5cc26.pdf">https://www-uploads.scaleway.com/DPA_2024_ENG_b0abb5cc26.pdf</a> ); pending acceptance and filing by CIATA, not yet on file. Former provider: Brevo SAS (Paris FR), used until 2026-09-26; Art. 28 DPA was never executed. Wind-down: close Brevo account and request deletion of sending logs and contacts once the switch has run stably; record the deletion confirmation ( <a href="#">△</a> see OI-05). |
| <b>Third-country transfers</b>     | None identified. Scaleway TEM operates exclusively in the fr-par (Paris, France) region; Scaleway's documentation states that all data is hosted and processed within the European Union. No EU data-residency configuration step is required. Scaleway's sub-processor list names US-headquartered data-centre colocation operators with EU locations only;                                                                                                                                                                                                                                                                                                                      |

| Field                              | Content                                                                                                                                                                                                                                                                                   |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                    | whether that creates a residual transfer risk is a question for counsel (DPA register, Entry 4). For mails Brevo delivered until the switch, EU residency was never confirmed (DPA register, OI-6).                                                                                       |
| <b>Envisaged erasure deadlines</b> | CIATA holds no separate copy of email content after delivery. Scaleway retains email sending logs (recipient, subject, status) for service operation; retention period governed by Scaleway's DPA and documentation. <a href="#">△</a> TO CONFIRM: retention period of Scaleway TEM logs. |

## Activity 6 — Withdrawal-Consent Records

| Field                              | Content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reference</b>                   | ROPA-DR-06                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Purpose</b>                     | Documentary evidence that a consumer expressly requested immediate performance of the digital service and acknowledged that the statutory right of withdrawal lapses on performance (§ 356(5) / § 312f BGB); evidence for defence of legal claims                                                                                                                                                                                                                                                                          |
| <b>Legal basis</b>                 | Art. 6(1)(b) GDPR — performance of contract (documentary evidence of the consumer's own contractual consent); Art. 6(1)(f) GDPR — legitimate interest in the ability to defend legal claims                                                                                                                                                                                                                                                                                                                                |
| <b>Categories of data subjects</b> | Consumer users (i.e. users who are not B2B buyers) who purchase credit packs and submit research jobs; the <code>is_business</code> flag determines at runtime whether the withdrawal-consent UI is shown                                                                                                                                                                                                                                                                                                                  |
| <b>Categories of personal data</b> | <code>job_id</code> (opaque identifier linking the consent record to the specific research run); <code>user_id</code> (links the consent to the user account); <code>consent_version</code> (version string of the consent text presented); <code>locale</code> (language locale of the consent text presented, enabling reconstruction of the exact wording); <code>consented_at</code> (UTC ISO timestamp of consent). Stored in the <code>withdrawal_consents</code> table in SQLite (Hetzner Cloud DE).                |
| <b>Categories of recipients</b>    | Hetzner Online GmbH (infrastructure hosting, Germany) — <a href="#">△</a> Art. 28 DPA required, not yet executed                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Third-country transfers</b>     | None.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Envisaged erasure deadlines</b> | <a href="#">△</a> To be determined — see Open Items. These records are NOT deleted with the 30-day run TTL (the filesystem cleanup does not touch SQLite rows). They are NOT deleted on account soft-deletion ( <code>soft_delete_user</code> does not delete consent rows). The minimum retention period must be confirmed by counsel, having regard to the statutory limitation periods under §§ 195/199 BGB (DPIA action A7). Until that determination is made, these records must be treated as indefinitely retained. |

## Activity 7 — Technical and Access Logs

| Field            | Content    |
|------------------|------------|
| <b>Reference</b> | ROPA-DR-07 |
| <b>Purpose</b>   |            |

| Field                              | Content                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                    | Security monitoring; detection and investigation of unauthorised access, credential-stuffing, DDoS, and abuse; rate-limit enforcement; error diagnosis; performance monitoring; compliance with potential legal obligations to disclose breach details                                                                                                                                                                                                            |
| <b>Legal basis</b>                 | Art. 6(1)(f) GDPR — Legitimate Interest. Cross-reference: LIA-DR-2026-01, Activity B (version 1.2, 2026-08-11). The legitimate security and operational interest is clearly established; access log data is not used for any purpose other than security and operations.                                                                                                                                                                                          |
| <b>Categories of data subjects</b> | Registered users and visitors to research.ciata.io                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Categories of personal data</b> | Source IP address; HTTP method; endpoint path; HTTP response status code; timestamp; User-Agent string; request ID (internal correlation identifier)                                                                                                                                                                                                                                                                                                              |
| <b>Categories of recipients</b>    | Hetzner Online GmbH (infrastructure hosting; logs reside in the Docker container log and, after a deploy, in compressed archives on the same server, Hetzner Cloud, Germany) — <a href="#">Art. 28 DPA</a> required, not yet executed                                                                                                                                                                                                                             |
| <b>Third-country transfers</b>     | None.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Envisaged erasure deadlines</b> | At most 90 days: the running container's log until the container is replaced at the next deploy; scripts/save_container_log.sh then keeps it as a compressed, root-only file in /var/log/deepresearch/ on the same server and deletes it 90 days after the container started (issue #161). No Docker log rotation is configured. A container that ran longer than 90 days without a deploy would hold older lines in its live log; deploys happen far more often. |

## Activity 8 — Internal Staff Access to Operate and Secure the Service

| Field                              | Content                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reference</b>                   | ROPA-DR-08                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Purpose</b>                     | Enabling authorised CIATA staff and (where applicable) authorised sub-processor personnel acting under instruction to access operational systems — including the SQLite database, research state files, access logs, and infrastructure components — as necessary to deliver, monitor, troubleshoot, and secure the service; and to fulfil data subject rights requests under Art. 15–22 GDPR |
| <b>Legal basis</b>                 | Art. 6(1)(f) GDPR — Legitimate Interest. Cross-reference: LIA-DR-2026-01, Activity C (version 1.2, 2026-08-11). Operational necessity is clear; access is controlled and authenticated.                                                                                                                                                                                                       |
| <b>Categories of data subjects</b> | Registered users whose account data, research jobs, payment records, and consent records may be accessed during operational work                                                                                                                                                                                                                                                              |
| <b>Categories of personal data</b> | All data categories held in the SQLite database (users, api_keys, credit_transactions, company_profiles, withdrawal_consent, processed_payments tables) and the ./runs/ filesystem (research state, reports, PII-filtered page text). Access is limited to the minimum necessary for the operational task. Note: stored PII-filtered page text in                                             |

| Field                              | Content                                                                                                                                                                                                                                                                                  |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                    | state.json is accessible via the admin report inspector endpoint only when the accessing user simultaneously holds the admin role AND owns the run; there is no administrative override.                                                                                                 |
| <b>Categories of recipients</b>    | No external recipients for this activity (data remains on CIATA's Hetzner Cloud infrastructure). Sub-processors receive access only to the data necessary for their contracted function under their respective agreements — <a href="#">△</a> none of those agreements are yet executed. |
| <b>Third-country transfers</b>     | None.                                                                                                                                                                                                                                                                                    |
| <b>Envisaged erasure deadlines</b> | Staff access is transient (task duration only); actions are captured in access logs (Activity 7, approximately 90-day retention).                                                                                                                                                        |

## Activity 9 — Website Analytics (Self-Hosted Plausible)

| Field                              | Content                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reference</b>                   | ROPA-DR-09                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Purpose</b>                     | Aggregate product and conversion analytics: page-view counts, referrer statistics, and click-level conversion events (event name and page URL only). No individual user tracking.                                                                                                                                                                                                                                                       |
| <b>Legal basis</b>                 | Art. 6(1)(f) GDPR — Legitimate Interest in aggregate product and conversion analytics. No personal data is processed; a legal basis is formally not required for this activity but is stated for completeness.                                                                                                                                                                                                                          |
| <b>Categories of data subjects</b> | None — Plausible is cookie-free, processes no personal data, and stores no IP addresses.                                                                                                                                                                                                                                                                                                                                                |
| <b>Categories of personal data</b> | None. Event names and page URLs are not personal data. No device fingerprints, no user identifiers, no form field values.                                                                                                                                                                                                                                                                                                               |
| <b>Categories of recipients</b>    | None — Plausible runs on CIATA-controlled infrastructure at trc.ciata.io (Hetzner Cloud DE). It is NOT a third-party sub-processor; no personal data is transferred to any external party for this activity.                                                                                                                                                                                                                            |
| <b>Third-country transfers</b>     | None.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Envisaged erasure deadlines</b> | Aggregate statistical data; no personal data to erase.                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Notes</b>                       | Eleven conversion events are configured (ten in frontend/index.html, one via the Plausible JS API in frontend/js/app.js). Ten are confirmed: Home+Get+Started, Home+Pricing+CTA, Home+Final+CTA, View+Create+Account, Account+Created, and the report-view events (issue #189) Report+Shared, Report+Downloaded+Markdown, Report+Downloaded+PDF, Report+Copied+Button, Report Text Copied (the last fired via the Plausible JS API from |

| Field | Content                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | frontend/js/app.js; it sends only the event name, never the copied text). One (Start+Research) uses a non-standard attribute and is not confirmed to fire — recorded here for completeness, not as an assertion that it is currently collected (ZDR §5.8). <a href="#">△</a> ePrivacy / TDDDG position for cookie-free, identifier-free event tracking via a self-hosted analytics instance should be confirmed with counsel. |

## Activity 10 — Product and Performance Telemetry (Planned — Not Yet Live)

| Field                                                  | Content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reference</b>                                       | ROPA-DR-10                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Status</b>                                          | <b>PLANNED — NOT CURRENTLY ENABLED.</b> The telemetry code exists in <code>src/perf.py</code> ( <code>@time_it</code> decorator and <code>track_metric()</code> function), but the OpenObserve export is disabled by default. It transmits only when <code>OPENOBSERVE_API_KEY</code> , <code>OPENOBSERVE_ORG</code> and <code>OPENOBSERVE_STREAM</code> are all set; if any is absent the exporter is inert. As of 2026-08-11 they are not set and this processing is not occurring. This activity is recorded in advance so that the ROPA is ready when the feature is enabled. The ROPA must be updated and reviewed before activation. |
| <b>Purpose (planned)</b>                               | Exporting per-function execution time metrics and custom job-level metrics (token counts, finding counts, agent call durations) to an OpenObserve metrics instance (hosting model undecided — see recipients below) for operational performance monitoring and debugging                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Legal basis (to be confirmed before activation)</b> | Art. 6(1)(b) GDPR (contract performance — operational monitoring necessary to deliver the service) or Art. 6(1)(f) GDPR (legitimate interest in service reliability); to be confirmed before activation                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Categories of data subjects (when enabled)</b>      | Registered users, to the extent that <code>job_id</code> can be linked to a user account                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Categories of personal data (when enabled)</b>      | Function name; execution duration in milliseconds; success/failure status; error message string (if any); custom metric name and value; <code>job_id</code> (opaque identifier; constitutes personal data to the extent it can be linked to a user account); arbitrary context labels passed by the caller. All other fields are technical metadata.                                                                                                                                                                                                                                                                                       |
| <b>Categories of recipients (when enabled)</b>         | An OpenObserve instance. <a href="#">△</a> The hosting model is <b>undecided and determines the classification</b> : self-hosted on CIATA infrastructure would make it no third-party recipient at all (the Plausible position, Activity 9); a managed OpenObserve service would make it an Art. 28 processor requiring an executed DPA and, depending on region, a transfer assessment. See ZDR §5.9.                                                                                                                                                                                                                                     |
| <b>Third-country transfers</b>                         | None anticipated, but this follows from the hosting decision and cannot be asserted until it is made.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Envisaged erasure deadlines</b>                     | <a href="#">△</a> To be determined before activation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Pre-activation requirements</b>                     | Before this activity is enabled in production: (1) this ROPA entry must be updated with confirmed hosting location, retention period, and legal basis; (2) a DPA must be executed with the infrastructure provider if not already covered; (3) if the                                                                                                                                                                                                                                                                                                                                                                                      |

| Field | Content                                                                                                       |
|-------|---------------------------------------------------------------------------------------------------------------|
|       | OpenObserve instance is hosted on infrastructure other than Hetzner Cloud DE, data flows must be re-assessed. |

## 5. Sub-Processor Summary

| Sub-Processor                    | Role                                                                                                 | Location                        | DPA Status                                                                                                                                        | Third-Country Transfer                                 |
|----------------------------------|------------------------------------------------------------------------------------------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| AKI.io GmbH                      | LLM inference (gpt-oss-120b, qwen3.8-27b, gemma4-chat-26b)                                           | Frankfurt, Germany              | ⚠ Required — not yet executed                                                                                                                     | None                                                   |
| European Perspective SAS (Staan) | Web search and (in default config) server-side full_content page fetch                               | EU                              | ⚠ Required — not yet executed; must cover full_content flow                                                                                       | None                                                   |
| Hetzner Online GmbH              | Cloud infrastructure hosting (Hetzner Cloud, shared virtualised)                                     | Germany                         | ⚠ Required — not yet executed                                                                                                                     | None                                                   |
| Mollie B.V.                      | Card payment processing                                                                              | Amsterdam, NL                   | ⚠ Required — not yet executed                                                                                                                     | None                                                   |
| Scaleway SAS                     | Transactional email (verification, password reset, purchase confirmation, report-ready notification) | Paris, France (fr-par, EU-only) | ⚠ Required — Scaleway standard DPA (version June 2024) pending acceptance and filing by CIATA; not yet on file                                    | None (Scaleway TEM operates exclusively within the EU) |
| Billie GmbH                      | B2B BNPL (via Mollie checkout; independent controller — BNPL credit decision)                        | Berlin, Germany                 | Independent controller — no Art. 28 DPA required on this basis; Art. 13/14 disclosure in privacy policy; ⚠ classification to confirm with counsel | None                                                   |
| Qonto                            | Invoice generation (independent controller — licensed payment institution)                           | Paris, France                   | Independent controller — no Art. 28 DPA required on this basis; Art. 13/14 disclosure in privacy policy; ⚠ classification to confirm with counsel | None                                                   |

**Note on former email processor:** Brevo SAS (Paris, France) was the transactional email provider until 2026-09-26. After the switch, no personal data is sent to Brevo. Art. 28 DPA with Brevo was never executed. Wind-down open item: close the Brevo account and request deletion of sending logs and contacts; record confirmation on receipt (OI-05).

**Note on Plausible Analytics:** The self-hosted Plausible instance at trc.ciata.io runs on CIATA-controlled infrastructure. It is not a third-party sub-processor and is not listed above. No personal data is transferred to or processed by Plausible's own servers.

---

## 6. Third-Country Transfers

No personal data transfers to third countries (outside the EEA) take place in the default production configuration. This is conditional on:

1. `SEARCH_BACKEND=staan` being the active production configuration ([△](#) not yet confirmed — see Open Items)

The condition on Brevo EU data residency (OI-13) no longer applies to current processing: the transactional email provider is now Scaleway SAS, whose Transactional Email product operates exclusively in the fr-par (Paris, France) region, and Scaleway's documentation states that all data is hosted and processed within the European Union. It still applies to the mails Brevo delivered until the switch, for which EU residency was never confirmed (DPA register, OI-6).

Alternative search backends (DuckDuckGo, US-based; Google Custom Search, US-based) exist in source code (`src/searcher.py`) and can be enabled via configuration. If either is enabled, search queries constitute an EEA-to-US transfer and require a documented Art. 46 transfer mechanism (Standard Contractual Clauses or equivalent) before activation.

---

## 7. Open Items

The following gaps and unresolved questions were identified in drafting this record. Each is an outstanding compliance obligation.

| #     | Item                                                                                                                                                                                                                     | Source                                | Priority              |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|-----------------------|
| OI-01 | No Art. 28 DPA executed with AKI.io GmbH. DPA must explicitly cover the three model IDs currently in use (gpt-oss-120b, qwen3.8-27b, gemma4-chat-26b) and past processing on qwen3.6-chat-35b (in use until 2026-09-27). | ZDR §5.1;<br>LAW_FIRM_BRIEFING §5     | Critical — pre-launch |
| OI-02 | No Art. 28 DPA executed with Staan / European Perspective SAS. DPA must explicitly cover the <code>full_content</code> server-side page-fetch flow, not only the basic search index query.                               | ZDR §5.2; LIA Activity A, §A.2 item 9 | Critical — pre-launch |
| OI-03 | No Art. 28 DPA executed with Hetzner Online GmbH.                                                                                                                                                                        | ZDR §5.3;<br>LAW_FIRM_BRIEFING §5     | Critical — pre-launch |
| OI-04 | No Art. 28 DPA executed with Mollie B.V.                                                                                                                                                                                 | ZDR §5.4;<br>LAW_FIRM_BRIEFING §5     | Critical — pre-launch |

| #     | Item                                                                                                                                                                                                                                                                                                                                                                                                               | Source                                                  | Priority              |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|-----------------------|
| OI-05 | Scaleway SAS (email provider from 2026-09-26): Art. 28 DPA not yet accepted and filed. Scaleway publishes a standard DPA (version June 2024); pending CIATA acceptance and filing. Former provider Brevo SAS: Art. 28 DPA was never executed; wind-down required: close the Brevo account and request deletion of sending logs and contacts; record confirmation on receipt.                                       | This record, Activity 5; ZDR §5.7; LAW_FIRM_BRIEFING §5 | Critical – pre-launch |
| OI-06 | DPO not designated. § 38(1) sentence 2 BDSG likely requires a DPO because this processing is assessed as requiring a mandatory DPIA. The privacy contact (privacy@ciata.io) is the Managing Director, who faces a structural conflict of interest under Art. 38(3) GDPR and EDPB WP243 rev.01. An external DPO is the recommended route. Must be resolved before this ROPA can be considered Art. 35(2)-compliant. | DPIA §7; LAW_FIRM_BRIEFING §12.1 note                   | Critical – pre-launch |
| OI-07 | Retention period for withdrawal-consent records (withdrawal_consent table) not determined. Records are currently retained indefinitely. Minimum retention period must be confirmed by counsel having regard to §§ 195/199 BGB limitation periods. Records must NOT be deleted on account erasure or 30-day job TTL cleanup until the minimum period is confirmed.                                                  | DPIA action A7; LAW_FIRM_BRIEFING §12.1(3b)             | High                  |
| OI-08 | Interaction between the § 147 AO 10-year minimum retention obligation and the GDPR Art. 17 erasure right for B2B billing profiles (company_profiles table). Fields that fed into invoices may need to be retained in restricted form after account deletion, not erased. Redaction vs. deletion approach to be confirmed with counsel.                                                                             | DPIA action A8; LAW_FIRM_BRIEFING §12.1(3b)             | High                  |
| OI-09 | Retention periods for usage logs (usage_log table) and credit transaction history (credit_transactions table) not defined in this record. Define and document.                                                                                                                                                                                                                                                     | This record, Activity 1                                 | High                  |
| OI-10 | Production SEARCH_BACKEND setting not confirmed as staan. If a non-EU backend (DuckDuckGo, Google CSE) is active in production, an EEA-to-US transfer is occurring without a documented Art. 46 transfer mechanism, and the "no third-country transfers" statement in this record is incorrect. Verify and document.                                                                                               | DPIA action A2; ZDR §6; LIA transfer assessment         | High                  |
| OI-11 | Billie GmbH independent-controller classification must be confirmed with external counsel. If Billie is determined to act as a processor for any part of its data handling, an Art. 28 DPA is required.                                                                                                                                                                                                            | ZDR §5.5; DPIA §6                                       | Medium                |
| OI-12 | Qonto independent-controller classification must be confirmed with external counsel (optionally via dpo@qonto.com).                                                                                                                                                                                                                                                                                                | ZDR §5.6; DPIA §6                                       | Medium                |

| #     | Item                                                                                                                                                                                                                                                                                                                                                                 | Source                                               | Priority                        |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|---------------------------------|
| OI-13 | Brevo EU data residency: no longer relevant for current processing (Scaleway TEM operates exclusively within the EU, fr-par; no configuration step required). Still open for the historical period: confirm whether EU residency was active for the mails Brevo delivered until the switch (DPA register, OI-6). Wind-down of the Brevo account is tracked in OI-05. | This record, Activity 5; ZDR §5.7; DPA register OI-6 | Medium — historical period only |
| OI-14 | Disk encryption at rest not enabled on production Hetzner Cloud volumes. Accepted gap with compensating controls (encrypted EU off-site backups Frankfurt → Helsinki, per-user access isolation, 30-day retention, bcrypt, TLS). Enabling LUKS/dm-crypt at-rest encryption before the hot-production cutover is a recommended hardening step.                        | DPIA action A1; ZDR §5.3                             | Medium                          |
| OI-15 | Incident-response procedure now drafted (INCIDENT_RESPONSE.md v1.0). Outstanding: external legal review, a first tabletop rehearsal, creation of the breach-register file, and a deputy for the Incident Lead and Authority Communicator roles.                                                                                                                      | INCIDENT_RESPONSE.md §12; DPIA §4.2                  | High                            |
| OI-16 | Art. 32 TOM annex now drafted (TOM.md v1.0), structured to the standard German AVV Anlage categories and suitable as a customer-DPA schedule. Outstanding: external legal review.                                                                                                                                                                                    | TOM.md §6                                            | Medium                          |
| OI-17 | Sub-processor / DPA register now drafted (DPA_REGISTER.md v1.0), recording nine entries and doubling as the execution tracker. Every Art. 28 entry is status "pending execution — not on file"; the register must be completed with counterparty version, scope and execution date as each DPA is signed (OI-01 through OI-05).                                      | DPA_REGISTER.md §5                                   | Medium                          |
| OI-18 | Activity 10 (performance telemetry): this record must be updated — confirming hosting location, retention period, legal basis, and any applicable DPA — before the OpenObserve export is enabled in production.                                                                                                                                                      | This record, Activity 10                             | Medium (pre-activation)         |
| OI-19 | ePrivacy / TDDDG position for cookie-free, identifier-free click-event tracking via self-hosted Plausible analytics not confirmed with counsel.                                                                                                                                                                                                                      | ZDR §5.8                                             | Low                             |
| OI-20 | VSRMark watermark (proprietary Unicode variation-selector scheme) as the primary machine-detectable marking mechanism under EU AI Act Art. 50(2): counsel's assessment of whether a non-standardised marking discharges Art. 50(2) is outstanding.                                                                                                                   | LAW_FIRM_BRIEFING §6.2; §12.2(8)                     | Medium                          |
| OI-21 | External legal review of this ROPA and the supporting compliance documents (DPIA, LIA, ZDR) has not yet been conducted. Review by qualified external counsel                                                                                                                                                                                                         | LAW_FIRM_BRIEFING §11                                | High                            |

| # | Item                                                                                              | Source | Priority |
|---|---------------------------------------------------------------------------------------------------|--------|----------|
|   | is required before this record is relied upon in regulatory proceedings or shared with customers. |        |          |

**Approved by:** Prof. Dr. Tim Landgraf, Managing Director, CIATA GmbH **Date:** 2026-09-27

**Status:** Draft — pending external legal review

**Revision 2026-10-08:** Activity 4 (billing): the B2B billing profile used to stay after account deletion. It is now deleted 90 days after the account (#193); the issued invoices stay with Qonto for the statutory period. The commercial register number and VAT ID are no longer sent to Mollie, whose billing address has no such fields. The privacy policy now lists billing data among the categories and states this retention.

**Revision 2026-10-04:** Activity 7 (technical logs): the erasure deadline described "Docker log rotation", which is not configured; a log used to live only until the next deploy. From issue #161 each deploy saves the container log to a compressed archive on the same server, deleted 90 days after the container started. Retention stated as at most 90 days, unchanged for the data subject. Research progress messages (questions, sub-questions, search queries, source titles) are no longer written to the server log (issue #164): they go to a log file inside the run's own directory, which is deleted with the run after 30 days. The server log keeps operational events and warnings, with e-mail addresses hashed or redacted and web addresses cut to their host name.

**Revision 2026-09-27 (second):** Consistency Checker added (issue #172). The new agent checks the finished report draft against itself on qwen3.8-27b with reasoning effort medium, running in parallel with the Paragraph Checker. Two additional LLM calls per report. No new model, no new processor, no new data category: the input is the report draft, which already goes to AKI.io for the Paragraph Checker and the Report Patcher. Flags are recorded in the run state next to the Paragraph Checker's and passed to the Report Patcher. Activity 2 (LLM processing via AKI.io) updated: Consistency Checker added to the qwen3.8-27b agent list.

**Revision 2026-09-27:** Language Guard moves from qwen3.6-chat-35b to gemma4-chat-26b with reasoning disabled (issue #167). qwen3.6-chat-35b is no longer used in any agent. Three models remain in use at AKI.io: gpt-oss-120b, qwen3.8-27b, gemma4-chat-26b. When a repair call fails, leaked characters are now removed in code rather than kept. Activity 2 (LLM processing via AKI.io) updated: model list for Language Guard changed. Sub-processor summary and OI-01 updated accordingly.

**Revision 2026-09-26:** Transactional email provider changed from Brevo SAS to Scaleway SAS (Scaleway Transactional Email, fr-par, EU-only; issue #152). Scaleway standard DPA (version June 2024) pending acceptance and filing by CIATA; not yet on file. Report-ready notification mail added to Activity 5 (issue #159): data categories extended to include report title, short summary (up to approximately 500 characters), link to report, and deletion date; notification is on by default, can be turned off in account settings. Activity 2 (Research Job Execution) updated to list Scaleway SAS as a recipient of report title and summary (research content). Activity 1 updated to reference Scaleway SAS as email provider. Sub-processor table updated:

Scaleway SAS replaces Brevo SAS; former-processor note added. Section 6 updated: former Brevo EU data-residency condition removed. OI-05 and OI-13 updated.

**Revision 2026-09-15 (second):** The Figure Sheet call is disabled by default in the same day's second deployment (`research.figure_sheet: false`): it made no measurable difference to reports and could mislead the writer. No call is made unless an operator enables it. Model set, data categories, recipient and retention unchanged.

**Revision 2026-09-15:** Report writing moved to per-section writing on 2026-09-15 (commit 466a41b, issue #136): the Section Writer on `qwen3.8-27b` writes one topic section per call, supported by a Glossary call on `gpt-oss-120b`. A Figure Sheet call on `gpt-oss-120b` is added with issue #139, and the Paragraph Checker now retries a failed batch once. All three process the research question and excerpts of the run's findings, already sent to AKI.io GmbH for the Outliner and the Synthesizer. No new model identifier, data category, recipient or retention period: the four-model DPA scope is unchanged.

**Revision 2026-09-13:** Model routing revised for run time (issue #135): the Relevance Gate moves from `qwen3.6-chat-35b` to `gpt-oss-120b` (same verdicts on 192 replayed results, 4.5x faster) and the Extractor from `qwen3.6-chat-35b` to `gemma4-chat-26b` with reasoning disabled (5x faster, more and better-grounded findings on 40 real pages). `gemma4-chat-26b` is a NEW model identifier — a fourth model now processes customer data (PII-filtered page excerpts) — so the DPA scope must name four models; `qwen3.6-chat-35b` remains in service for the Language Guard only. Same data categories, same recipient (AKI.io GmbH, Frankfurt).

**Revision 2026-09-12:** Post-synthesis verification restructured (issue #133): the Fact Checker — a whole-report check plus a per-citation alignment check, both on `gpt-oss-120b` — is replaced by the Paragraph Checker, and the Report Patcher is given its own routing; both now run on `qwen3.8-27b`. Same data categories (the draft report and the run's findings), same recipient (AKI.io GmbH), no new model identifier: the three-model set and the DPA scope instruction are unchanged.

**Revision 2026-09-10:** Synthesis model corrected from `mistral4-119b` to `qwen3.8-27b`, which has served the Synthesizer since 2026-08-23 (commit eb2a5b1); the Table Repair agent, added 2026-09-10, runs on the same model and is now named in Activity “LLM processing via AKI.io” and in the processor table. OI-01's DPA scope instruction is corrected in step — a DPA drafted from the previous wording would not have covered the model that writes every report.