

Personal Data Breach Response Procedure

CIATA DeepResearch — Art. 33/34 GDPR

Version: 1.2 **Date:** 2026-09-26 **Status:** DRAFT — not yet reviewed by external legal counsel

Controller: CIATA GmbH, Arnimallee 7, 14195 Berlin · HRB 266084 B · MD: Prof. Dr. Tim

Landgraf **Contact:** privacy@ciata.io

Version	Date	Summary
1.2	2026-09-26	Log retention corrected: no Docker log rotation exists; each deploy saves the container log to a compressed archive deleted 90 days after the container started (issue #161). The "preserve logs" step now covers the live log and the archives.
1.1	2026-09-26	Transactional email processor updated from Brevo SAS to Scaleway SAS (issue #152); report-ready mail data added (issue #159). Brevo retained as former processor in breach scenarios where its historical sending logs remain relevant.
1.0	2026-08-11	Initial draft.

How to use this document. If you are holding it because something has gone wrong, go directly to §6 (Step-by-step response). Return to the earlier sections once the immediate steps are underway.

Table of Contents

1. [Scope and Definitions](#)
2. [Detection Sources](#)
3. [The 72-Hour Clock](#)
4. [Severity Triage](#)
5. [Roles](#)
6. [Step-by-Step Response](#)
7. [Supervisory Authority](#)
8. [Notification Templates](#)
9. [Breach Register](#)
10. [Sub-Processor Breaches](#)
11. [Post-Incident Review and Testing](#)
12. [Open Items](#)

1. Scope and Definitions

1.1 What is a personal data breach?

Under **Art. 4(12) GDPR**, a personal data breach is any security incident that leads to the accidental or unlawful:

- **destruction** of personal data (loss of data that cannot be recovered),
- **loss** of personal data (data is no longer accessible, even if it still exists somewhere),
- **alteration** of personal data (data has been modified without authorisation), or
- **unauthorised disclosure of, or access to**, personal data.

All three confidentiality, integrity, and availability failure modes qualify.

1.2 Concrete examples drawn from this system's risk register

The following are candidate breach events for CIATA DeepResearch. This list is illustrative, not exhaustive.

#	Scenario (DPIA risk)	Type
B1	An attacker gains read access to the Hetzner Cloud server (e.g. via an exposed SSH key or API token) and exfiltrates the SQLite database (<code>./data/</code>) containing email addresses, bcrypt password hashes, billing profiles, and API key hashes	Confidentiality
B2	An attacker exfiltrates one or more research run directories (<code>./runs/</code>), which contain research questions, generated reports, and PII-filtered page-text stored in <code>state.json</code>	Confidentiality
B3	An authorisation logic bug allows one authenticated user to access another user's research runs (<code>GET /v1/research/{job_id}</code>) — a lateral-access defect	Confidentiality
B4	A JWT or API key is compromised (e.g. leaked via an insecure log line) and used to access a user's account and data before revocation	Confidentiality
B5	The Hetzner Cloud volume is deleted or becomes unavailable; data cannot be recovered before the encrypted off-site backup is restored	Availability
B6	A bug silently deletes or corrupts research run data outside the normal 30-day TTL	Integrity / Availability
B7	Docker stdout logs are inadvertently included in a log-shipping stream that reaches an unintended destination, exposing request metadata (paths, status codes, request IDs)	Confidentiality
B8	A sub-processor (AKI.io, Staan, Scaleway) reports that they have suffered a breach affecting data they processed on CIATA's behalf. Note: Brevo SAS (former email processor until 2026-09-26) holds sending logs of mails it delivered before the switch; a breach at Brevo could still affect those historical logs.	Confidentiality (third-party)

Note on scope: Not every security incident is a personal data breach. An attempted attack that is blocked, a system outage that affects no personal data, or accidental deletion of internal configuration files are security incidents but not automatically breaches under Art. 4(12). Apply the definitions above before starting this procedure.

2. Detection Sources

CIATA is a small company with no dedicated security team and no 24/7 monitoring rota. Realistic breach-detection paths are:

2.1 Server logs (primary internal source)

- **Access logs:** AccessLogMiddleware writes a structured INFO line for every HTTP request to Docker stdout: method, path, status code, duration, and request ID. The running container keeps its log until the next deploy; each deploy saves it to `/var/log/deepresearch/api-<container_start>Z.log.gz` on the same server (root-only) and deletes such archives 90 days after the container started (issue #161). No Docker log rotation is configured.
- **Error logs:** `global_exception_handler` writes full tracebacks (including request ID) for every unhandled exception to Docker stdout.
- **Useful patterns to watch:**
 - Unusual volume of 4xx or 5xx responses on data endpoints (`/v1/research/`, `/v1/auth/`)
 - Repeated authentication failures (POST `/v1/auth/login` with 401 responses)
 - Access to GET `/v1/admin/` endpoints from unexpected IP addresses
 - Requests for job IDs that do not belong to the authenticated user (which return 404 — but a flood of these is a reconnaissance signal)

Retrieve logs:

```
docker compose logs api --since 24h 2>&1 | grep -E "(ERROR|WARNING|40[13]|500)"
```

2.2 A sub-processor notifying CIATA

Any of our processors (AKI.io, Staan, Hetzner, Mollie, Scaleway) may contact us to report a breach on their systems affecting data we sent them. Brevo SAS, the former email processor, holds sending logs of mails delivered before the 2026-09-26 switch; a breach report from Brevo should be handled as any other sub-processor notification. The email address to use is `privacy@ciata.io`. See §10 for handling.

2.3 A user report

A user notices unexpected account activity, a research run they did not initiate, or credentials that no longer work. User-facing contact is `privacy@ciata.io`.

2.4 A security researcher

A researcher discloses a vulnerability via `privacy@ciata.io` or via a public disclosure. Treat a credible researcher report as a potential breach until assessed.

2.5 Routine monitoring or audit

A periodic review of access logs, or an audit of run directories, surfaces anomalies.

2.6 Detection gaps — honest assessment

- **No intrusion detection system (IDS) is deployed.** Anomalous access patterns in logs must be noticed manually.
 - **No alerting is configured** for authentication failures, error spikes, or unusual data-volume egress.
 - **No real-time log aggregation** (e.g. Loki, Elasticsearch) is in place; log inspection is manual and ad-hoc.
 - **No external integrity monitoring** on the SQLite database file or run directories.
 - **No disk encryption at rest** (confirmed 2026-07-15). Physical or hypervisor-level access to the Hetzner Cloud volume would expose data that is not encrypted.
 - **Sub-processor notification is not contractually secured.** None of the Art. 28 DPAs with processors (AKI.io, Staan, Hetzner, Mollie, Scaleway) are yet executed. Brevo SAS (former email processor) also has no executed DPA. The obligation for processors to notify the controller "without undue delay" after discovering a breach (Art. 33(2)) is therefore not contractually binding on any of them. See §10.
-

3. The 72-Hour Clock

3.1 When the clock starts

The 72-hour period begins when CIATA **becomes aware** of a breach — that is, when CIATA has a reasonable degree of certainty that a security event has occurred that has led to the compromise of personal data (EDPB Guidelines 01/2021 on notification of personal data breaches, §3.1).

"Aware" does not require certainty about the full scope of the breach. An initial, incomplete detection suffices to start the clock. CIATA may continue investigating while simultaneously notifying.

If a sub-processor becomes aware of a breach, the clock starts when CIATA itself is notified by the sub-processor, not when the sub-processor first discovered the breach.

Document the time of awareness (step 6.2 below) immediately. Everything else flows from that timestamp.

3.2 What must happen within 72 hours

Hour	Action
0–4	Confirm the incident, contain it, document the time of awareness (§6.1–6.2)
0–12	Complete severity triage (§4); if notification threshold is met, begin drafting Art. 33 notification

Hour	Action
0-24	If threshold is met: file Art. 33 notification with BlnBDI, even if investigation is incomplete (incomplete notification is explicitly permitted – see §8.1 for the template)
0-72	File any supplementary information with the authority as it becomes available

If you cannot meet the 72-hour deadline: Notify the authority anyway, explain the delay, and state that you are continuing to investigate. A late notification with a clear reason is far better than no notification.

3.3 Notifications that do not require Art. 33 reporting

If the breach is assessed as **unlikely to result in a risk to the rights and freedoms of natural persons** (Art. 33(1) threshold), you must still record it in the breach register (§9) but do not notify the authority. Document the reasoning.

4. Severity Triage

Use this matrix to determine what to do within the first four hours.

4.1 Triage questions

Answer these in order. Each "Yes" escalates the severity.

1. Are personal data of data subjects involved? (If No → security incident, not a breach; record but do not notify.)
2. How many data subjects are affected?
3. What categories of data are involved?
4. Has data actually been accessed or exfiltrated, or was it merely exposed (i.e. a vulnerability existed but may not have been exploited)?
5. Could the data enable identity theft, financial harm, discrimination, or physical harm?
6. Are vulnerable persons affected (consumers, patients)?

4.2 Severity matrix

Level	Criteria	Action
No notification	The breach is unlikely to result in any risk to data subjects. Example: a server log file containing only request IDs and HTTP status codes (no PII) was briefly accessible.	Record in breach register (§9). No Art. 33 or Art. 34 notification required.
Notify authority only (Art. 33)	The breach results in a risk to data subjects but is not likely to result in high risk . Examples: bcrypt password hashes (without salts or plaintexts) exposed; PII-filtered page text from one job briefly accessible to another authenticated user.	Notify BlnBDI within 72 hours. No Art. 34 data-subject notification required unless assessment changes.

Level	Criteria	Action
Notify authority + data subjects (Art. 33 + Art. 34)	The breach is likely to result in high risk to data subjects. Examples: plaintext credentials or API keys exposed; email addresses combined with research queries (which could reveal business-sensitive investigations); bulk account-data exfiltration; Art. 9 data in research questions leaked.	Notify BlnBDI within 72 hours. Notify affected data subjects without undue delay.

4.3 Art. 34(3) exemptions — when data-subject notification is not required even at "high risk"

You may not need to notify data subjects directly if: - **(a) Technical measures:** The data was protected by appropriate technical measures (e.g. strong encryption) such that it is unintelligible to anyone who accessed it without authorisation. **Note:** bcrypt hashes are strong; the SQLite file and run directories are not encrypted at rest — this exemption therefore does not apply to a disk-level breach. - **(b) Subsequent measures:** CIATA has taken subsequent measures that ensure the high risk is no longer likely to materialise. - **(c) Disproportionate effort:** Notifying data subjects would involve disproportionate effort, in which case a public communication or similar measure must be used instead.

Document the basis for invoking any exemption.

4.4 Examples applied to this system's risk scenarios

Scenario	Likely triage outcome	Notes
B1 — Full SQLite DB exfiltrated	Notify authority + data subjects	Email addresses + billing profiles exposed; bcrypt hashes alone low risk but billing data is high risk
B2 — Run directories exfiltrated	Notify authority; escalate to authority + data subjects if research queries are sensitive	Research questions may be commercially sensitive; PII-filtered but names may remain
B3 — Lateral access bug (one user sees another's job)	Notify authority; escalate if any sensitive data confirmed accessed	Depends on how many users affected and what data was visible
B4 — JWT/API key compromise	Notify authority + affected user	Revoke immediately via token_version (see §6.3)
B5 — Availability loss (volume deleted)	No notification if backup restored within reasonable time with no access by unauthorised party	Document
B6 — Corrupt deletion of runs	Availability breach; notify authority if widespread	Data subjects' right of access (Art. 15) may be affected
B7 — Log stream misdirected	Assess: request metadata alone is low risk; escalate if logs contain PII (e.g. research question in query parameter)	
		See §10

Scenario	Likely triage outcome	Notes
B8 — Sub-processor breach	Depends on data affected; treat as any other breach once scope is known	

5. Roles

Single point of failure notice. CIATA has one managing director and no dedicated DPO. Every critical role identified below has only one named owner and no deputy. This is a real operational risk. If Prof. Dr. Landgraf is unavailable during an incident, there is no pre-designated person to take decisions. This gap is flagged as an open item (§12, OI-5).

Role	Function	Named owner	Gap
Incident Lead	Declares the incident; takes all decisions on containment, notification, and communication; owns the breach register entry	Prof. Dr. Tim Landgraf (MD)	No deputy designated
Technical Responder	Executes containment actions on the server (revoke tokens, rotate secrets, preserve logs, take container down); assesses scope and affected data	Prof. Dr. Tim Landgraf (MD) / whichever engineer is available	No dedicated role; depends on availability
Authority Communicator	Files the Art. 33 notification with BlnBDI; follows up with supplementary information	Prof. Dr. Tim Landgraf (MD)	No deputy designated
Data Subject Communicator	Sends Art. 34 notifications to affected data subjects (using privacy@ciata.io)	Prof. Dr. Tim Landgraf (MD)	No deputy designated
DPO / Privacy Advisor	Provides independent assessment and advice	Not designated — this is an open action item (DPIA §7, OI-4 below)	Role vacant

6. Step-by-Step Response

Phase 1 — Contain

6.1 Confirm the incident

- [] Determine whether personal data is actually involved (see §1 definitions).
- [] Gather first facts: what data, how many data subjects, how long exposed, by what vector.
- [] Decide whether to escalate immediately or investigate first. Default: escalate immediately; investigate in parallel.

6.2 Record the time of awareness

- [] Write down: date, time (with timezone), how the breach was discovered, who became aware.
- [] This timestamp starts the 72-hour clock.

6.3 Containment actions — what is available on this stack

Execute as many of the following as are relevant, in order of impact:

Action	Command / Step	Effect
Revoke all tokens for affected user(s)	Call <code>db.bump_token_version(user_id)</code> — or trigger a password reset via the API, which calls <code>bump_token_version</code> internally	<code>token_version</code> (schema v12) is incremented; every outstanding JWT access and refresh token for that user immediately returns HTTP 401 on next use, independently of its remaining TTL
Revoke API keys for affected user(s)	Delete the API key row from the SQLite <code>api_keys</code> table, or call <code>DELETE /v1/auth/api-keys/{key_id}</code> as the admin	API key access stops immediately
Rotate the JWT signing secret	Change <code>JWT_SECRET</code> in the production <code>.env</code> and restart the container (the application refuses to start if it is unset or left at the insecure default)	Invalidates all JWT tokens for all users system-wide — use only when a full compromise of the signing secret is suspected
Rotate other secrets	Change <code>API_KEY</code> or other credentials in production <code>.env</code>	Stops access via compromised credentials
Preserve logs before they are deleted	Copy the running container's log and the relevant archives off the server before a deploy replaces the container or the 90-day archive retention deletes them. Do not deploy before the live log is copied.	<code>docker compose logs --no-color --timestamps api > /tmp/incident_\$(date +%Y%m%d_%H%M%S).log</code> ; archives: <code>/var/log/deepresearch/api-*.log.gz</code> (search with <code>zgrep</code>) — then transfer securely off the server. (Run from the compose project directory; the service is named <code>api</code> and no fixed container name is set, so addressing it by service is more reliable than by container id.)
Take the container down	<code>docker compose down</code>	Stops all new traffic and processing. Only if the threat is ongoing and cannot be stopped by key rotation alone. Note: this makes the service unavailable.
Isolate the server	Via Hetzner Cloud Firewall — block inbound traffic from all IPs except a known-good address	Stops ongoing exfiltration without taking the container down
Block a specific IP	Add a firewall rule in Hetzner Cloud console	Targeted containment if attacker IP is known

Action	Command / Step	Effect
Take a backup snapshot	Via Hetzner Cloud console: create a manual snapshot of the volume	Preserves state for forensic analysis; do before any destructive remediation

Phase 2 — Assess

6.4 Assess the breach scope

- ☐ Which data categories were involved? (Use the data categories table from LAW_FIRM_BRIEFING.md §4.2 as a checklist.)
- ☐ How many data subjects are affected? (Estimate if exact count is not yet possible; state the estimate and basis in the record.)
- ☐ Was the breach a one-time snapshot or is it ongoing?
- ☐ Is there evidence of actual access/exfiltration, or only of a vulnerability that may have been exploited?
- ☐ Are there any Art. 9 special-category data involved (health, political opinion, etc.) in research questions or reports?
- ☐ Apply severity triage (§4).

6.5 Determine notification obligations

- ☐ Is the Art. 33(1) threshold met (any risk)? → Notify BlnBDI.
- ☐ Is the Art. 34(1) threshold met (high risk)? → Notify data subjects.
- ☐ Do any Art. 34(3) exemptions apply? → Document the basis.

Phase 3 — Record

6.6 Open a breach register entry (§9)

- ☐ Create a new entry in the breach register immediately — even before the assessment is complete.
- ☐ Record all known facts at the time; update as the investigation progresses.
- ☐ The register entry must exist whether or not a notification is filed.

Phase 4 — Notify authority

6.7 File Art. 33 notification with BlnBDI

- ☐ Use the template at §8.1.
- ☐ File within 72 hours of becoming aware (§3.1 for the start of the clock).
- ☐ If the investigation is incomplete, file what you know and state that supplementary information will follow.
- ☐ Notification route: see §7.
- ☐ Record the filing: date, time, reference number received from the authority (if any).

Phase 5 — Notify data subjects

6.8 Notify affected data subjects (if Art. 34(1) threshold is met)

- ☐ Use the template at §8.2. Draft in both German and English (users are B2B EEA; the B2B account may prefer either).
- ☐ Send from `privacy@ciata.io`.
- ☐ Notify "without undue delay" — aim for within 24–72 hours of the Art. 34 determination.
- ☐ Record: date sent, channel (email), number of data subjects notified.
- ☐ If individual notification is disproportionate (e.g. large number of affected users, contact details unavailable), use a public communication or a prominent notice on the product website instead.

Phase 6 — Remediate

6.9 Remediate the root cause

- ☐ Identify and fix the underlying vulnerability or misconfiguration.
- ☐ Test the fix before reopening the system to users.
- ☐ Review related code paths for similar issues.
- ☐ If the attack vector involved an unexecuted DPA with a processor, escalate DPA execution (§10).

6.10 Restore from backup if required

- ☐ Restore from the encrypted EU off-site backup (Hetzner Frankfurt → Helsinki).
- ☐ Verify integrity of restored data.
- ☐ Document the recovery timeline.

Phase 7 — Review

6.11 Post-incident review (§11)

- ☐ Complete the breach register entry with all final findings.
- ☐ Conduct a post-incident review within 14 days (§11).
- ☐ Update controls and this procedure if gaps were identified.

7. Supervisory Authority

The authority responsible for CIATA GmbH (registered and operating in Berlin, Germany) is the:

Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) Friedrichstraße 219
10969 Berlin, Germany Phone: +49 30 13889-0 Email: mailbox@datenschutz-berlin.de Website:
<https://www.datenschutz-berlin.de/>

Online breach notification: The BlnBDI accepts breach notifications online. Navigate to <https://www.datenschutz-berlin.de/> and locate the section for data breach reporting ("Meldung von Datenpannen"). If the online form is unavailable, send by email to mailbox@datenschutz-berlin.de with subject: "Art. 33 GDPR Breach Notification – CIATA GmbH."

Source verification: The address above is taken from `frontend/privacy.html §16` (confirmed 2026-08-11). Verify against the live BlnBDI website before filing – authority addresses change occasionally.

8. Notification Templates

8.1 Authority notification template — Art. 33(3) GDPR

File this with BlnBDI. Mark clearly if information is preliminary or will be supplemented.

Subject: Art. 33 GDPR Personal Data Breach Notification — CIATA GmbH

Controller: CIATA GmbH Arnimallee 7, 14195 Berlin HRB 266084 B, Amtsgericht Charlottenburg Managing Director: Prof. Dr. Tim Landgraf Contact: privacy@ciata.io

Date and time of notification: [INSERT] **Date and time of becoming aware of the breach:**

[INSERT] **Notification is:** [] Complete [] Preliminary — supplementary information will follow

1. Nature of the breach (Art. 33(3)(a))

Describe: what happened; how it was discovered; whether it was a confidentiality, integrity, or availability breach; whether data was accessed, exfiltrated, altered, or destroyed.

[INSERT]

Categories and approximate number of data subjects affected: [INSERT — e.g.

"Approximately [N] registered users; categories: email addresses, bcrypt-hashed passwords, [and/or] research questions, [and/or] billing profiles"]

Categories and approximate number of records affected: [INSERT]

2. Contact for further information (Art. 33(3)(b))

Prof. Dr. Tim Landgraf privacy@ciata.io +49 [INSERT phone]

3. Likely consequences of the breach (Art. 33(3)(c))

Describe the likely harm to data subjects: identity theft, financial loss, reputational damage, loss of confidentiality, discrimination, or other Recital 75 harm types.

[INSERT]

4. Measures taken or proposed (Art. 33(3)(d))

List containment steps already taken (token revocation, key rotation, server isolation, log preservation, container restart) and remediation steps planned.

[INSERT]

5. Data subjects notified?

☐ Yes — data subjects were notified on [DATE] via [CHANNEL] ☐ No — we assess that the breach is unlikely to result in high risk to data subjects because [REASON] ☐ No — we assess that an Art. 34(3) exemption applies because [REASON] ☐ Under assessment — supplementary information will follow

6. Sub-processors involved

If a sub-processor suffered the breach or was involved: [INSERT name, role, and what data of theirs was affected]

Signature: Prof. Dr. Tim Landgraf, Managing Director, CIATA GmbH Date: [INSERT]

8.2 Data-subject notification templates — Art. 34(2) GDPR

Send these via email from privacy@ciata.io. Adapt for the specific breach; do not use generic boilerplate that does not describe what actually happened.

English version

Subject: Important security notice regarding your CIATA DeepResearch account

Dear [Name / Account holder],

We are writing to notify you of a security incident that affected your personal data held by CIATA GmbH, the operator of CIATA DeepResearch (research.ciata.io).

What happened [Describe in plain language: what occurred, when, and how it was discovered. Be specific about what data was affected. Example: "On [DATE], we discovered that an unauthorised party gained access to our user database. The data exposed includes your email address and password (stored as a secure one-way hash — your actual password was not stored in readable form)."]

What data was affected [List specifically: email address / research questions / generated reports / billing information — only what was actually affected. Do not list data that was not involved.]

What we have done - [List containment steps already taken, e.g.: "We have immediately revoked all active login sessions for your account", "We have patched the vulnerability", "We have notified the Berlin data protection authority".]

What you should do - Change your CIATA DeepResearch password at research.ciata.io immediately. - [If API keys may be affected:] Regenerate your API key in your account settings. - [If email addresses were exposed:] Be alert to phishing emails that reference your CIATA account. - If you use the same password on other services, change it there too.

Your rights You have the right to request access to your personal data, to request its erasure, and to lodge a complaint with the supervisory authority: Berliner Beauftragte für Datenschutz und Informationsfreiheit Friedrichstraße 219, 10969 Berlin mailbox@datenschutz-berlin.de · www.datenschutz-berlin.de

If you have questions, please contact us at privacy@ciata.io.

We sincerely apologise for this incident and the concern it may cause.

Prof. Dr. Tim Landgraf Managing Director, CIATA GmbH

German version / Deutsche Fassung

Betreff: Wichtige Sicherheitsmitteilung zu Ihrem CIATA-DeepResearch-Konto

Sehr geehrte/r [Name / Kontoinhaber/in],

wir schreiben Ihnen, um Sie über einen Sicherheitsvorfall zu informieren, der Ihre bei der CIATA GmbH gespeicherten personenbezogenen Daten betroffen hat. CIATA GmbH betreibt CIATA DeepResearch (research.ciata.io).

Was ist passiert? [Sachverhalt in verständlicher Sprache schildern: Was ist wann passiert, wie wurde es entdeckt? Konkret angeben, welche Daten betroffen waren. Beispiel: „Am [DATUM] haben wir festgestellt, dass eine unbefugte Person Zugriff auf unsere Nutzerdatenbank erlangt hat. Betroffen sind Ihre E-Mail-Adresse und Ihr Passwort, das bei uns ausschließlich als sicherer, nicht umkehrbarer Hash gespeichert wird — Ihr Klartext-Passwort war zu keinem Zeitpunkt lesbar gespeichert.“]

Welche Daten sind betroffen? [Konkret auflisten: E-Mail-Adresse / Forschungsfragen / erstellte Berichte / Rechnungsdaten — nur was tatsächlich betroffen ist.]

Was haben wir unternommen? - [Ergriffene Maßnahmen auflisten, z. B.: „Wir haben alle aktiven Anmeldesitzungen Ihres Kontos sofort widerrufen.“, „Die Sicherheitslücke wurde geschlossen.“, „Wir haben die Berliner Beauftragte für Datenschutz und Informationsfreiheit informiert.“]

Was sollten Sie tun? - Ändern Sie Ihr CIATA-DeepResearch-Passwort unter research.ciata.io umgehend. - [Falls API-Schlüssel betroffen:] Erstellen Sie in Ihren Kontoeinstellungen einen neuen API-Schlüssel. - [Falls E-Mail-Adressen betroffen:] Seien Sie auf Phishing-E-Mails aufmerksam, die Bezug auf Ihr CIATA-Konto nehmen. - Falls Sie dasselbe Passwort bei anderen Diensten verwenden, ändern Sie es auch dort.

Ihre Rechte Sie haben das Recht, Auskunft über Ihre personenbezogenen Daten zu verlangen, deren Löschung zu beantragen und bei der Aufsichtsbehörde Beschwerde einzureichen:
Berliner Beauftragte für Datenschutz und Informationsfreiheit Friedrichstraße 219, 10969 Berlin mailbox@datenschutz-berlin.de · www.datenschutz-berlin.de

Bei Fragen wenden Sie sich bitte an privacy@ciata.io.

Wir entschuldigen uns aufrichtig für diesen Vorfall und die damit verbundenen Unannehmlichkeiten.

Prof. Dr. Tim Landgraf Geschäftsführer, CIATA GmbH

9. Breach Register

Under **Art. 33(5) GDPR**, CIATA must maintain a record of every personal data breach, including those that do not meet the notification threshold. This obligation does not expire — the register is a permanent record.

9.1 Where the register lives

File location: `docs/compliance/BREACH_REGISTER.md` in the project repository (or a private equivalent outside the repository if confidential investigation details should not be version-controlled).

OPEN ITEM (OI-1): The breach register file does not yet exist. It must be created before this procedure is operational. See §12.

9.2 Minimum content of each entry — Art. 33(5)

Each breach entry must include:

Field	Content
Breach ID	Sequential identifier, e.g. BR-2026-001
Date/time of awareness	When CIATA first became aware; this starts the clock
Date/time of occurrence	Estimated when the breach actually happened (may differ from awareness)
How discovered	E.g. user report, log review, sub-processor notification
Nature of the breach	Confidentiality / integrity / availability; description of what happened

Field	Content
Data categories affected	Which personal data categories; reference to LAW_FIRM_BRIEFING §4.2 categories
Approximate number of data subjects	Estimate with basis
Approximate number of records	
Consequences	Likely impact on data subjects
Measures taken	Containment and remediation steps with dates
Notification to authority	Date filed / reason not filed
Notification to data subjects	Date sent / reason not sent / Art. 34(3) exemption relied on
Supplementary submissions	Dates and content of any follow-up information sent to authority
Status	Open / Closed
Closed date	When the incident was fully resolved and reviewed

The register must capture breaches that are NOT notified, with a clear documented reasoning for why the Art. 33(1) threshold was not met.

10. Sub-Processor Breaches

10.1 Our processors' obligation to notify us

Under Art. 33(2) GDPR, a processor must notify the controller "without undue delay" after becoming aware of a personal data breach. This allows the controller to meet the 72-hour notification window to the authority.

Current status: None of the Art. 28 DPAs with our processors (AKI.io GmbH, European Perspective SAS / Staan, Hetzner Online GmbH, Mollie B.V., Scaleway SAS) have been executed. Brevo SAS (former email processor, switched on 2026-09-26) also had no executed DPA; its wind-down (account closure, log-deletion request) is an open item. The Art. 33(2) notification obligation is therefore **not contractually secured with any of our processors**. We cannot compel timely notification by contract because no contract yet binds them.

This is a real gap. If any of these processors suffers a breach affecting data they hold on our behalf, we may: - receive no notification, or - receive notification significantly later than the GDPR contemplates, leaving us unable to notify the authority within 72 hours.

OPEN ITEM (OI-2): Execute all outstanding processor DPAs as a priority, and ensure each includes an explicit Art. 33(2) notification obligation with a defined maximum notification period (recommended: 24 hours after the processor becomes aware, to give CIATA time to assess and notify the authority within 72 hours). See DPIA §9 open actions A (all DPA items).

10.2 How to handle a sub-processor breach notification

When a sub-processor notifies CIATA of a breach (by email to privacy@ciata.io or by any other means):

1. **Record the time you received the notification.** The 72-hour clock to the authority starts when CIATA receives the notification (the processor's awareness date does not start our clock).
2. **Obtain from the processor:**
 3. When they became aware
 4. What data of ours was affected (categories, approximate number of records)
 5. What data subjects of ours are affected
 6. What containment measures they have taken
 7. Their own regulatory notification status (if they filed separately)
 8. **Apply severity triage (§4)** to the data affected.
 9. **Proceed through §6** as for any other breach.
10. In the Art. 33 notification to BlnBDI, identify the processor and describe their role.

10.3 Billie GmbH and Qonto SAS

Billie and Qonto are classified as independent controllers (not processors). If they suffer a breach affecting data they received from our users, they have their own notification obligations to their supervisory authority. They do not have a contractual obligation to notify CIATA. However, if such a breach affects CIATA users, CIATA should assess whether it has any independent notification obligation as the originating data source. Contact privacy@ciata.io and seek legal advice.

11. Post-Incident Review and Testing

11.1 Post-incident review

Within **14 days of closing any breach**, conduct a review covering:

- ☐ What went wrong? (Root cause)
- ☐ How was it detected? Could it have been detected earlier?
- ☐ Were the 72-hour obligations met? If not, why not, and what would have needed to be different?
- ☐ Were the response steps in §6 adequate and actionable?
- ☐ What controls need to be added or changed?
- ☐ What changes to this procedure are needed?
- ☐ Update the breach register entry.

Document the review findings. If control changes are made, update the DPIA (§4) accordingly.

11.2 Periodic rehearsal

This procedure should be tested at least **once per year**, even without a real breach. A tabletop exercise covering a realistic scenario (e.g. scenario B1 or B3 from §1.2) takes approximately 1–2 hours and should confirm:

- That the responsible persons know where this document is.
- That the containment commands in §6.3 work on the current production environment.
- That the BlnBDI notification route is still current.
- That the breach register location is known and accessible.
- That sub-processor DPAs (if executed by then) include the Art. 33(2) obligation.

OPEN ITEM (OI-3): No rehearsal has yet been conducted. Schedule the first tabletop exercise after this procedure is approved and before the production launch.

12. Open Items

The following items must be resolved before this procedure is fully operational. Unresolved items mean the procedure contains gaps that could prevent a legally compliant response during a real incident.

ID	Item	Urgency	Owner
OI-1	Create the breach register file (docs/compliance/BREACH_REGISTER.md or equivalent). It must exist before any incident can be properly recorded.	High — needed immediately	MD (Prof. Dr. Landgraf)
OI-2	Execute all outstanding processor DPAs (AKI.io, Staan, Hetzner, Mollie, Scaleway). Each DPA must include an explicit Art. 33(2) breach-notification obligation binding the processor to notify CIATA without undue delay (recommend: ≤ 24 hours after the processor's awareness). For Scaleway, the standard DPA is the "Version of 1 June 2024". Also close the Brevo account (former email processor) and obtain deletion confirmation of its sending logs. Until DPAs are executed, sub-processor breach notification is not contractually secured.	Critical — pre-launch	MD / Legal counsel
OI-3	Conduct the first tabletop rehearsal of this procedure before production launch. Confirm containment commands, notification routes, and register location.	High — pre-launch	MD
OI-4	Designate a DPO or document a reasoned decision not to designate one (with external legal input — see DPIA §7). Until a DPO is designated, the Art. 35(2) consultation step cannot be verified as independent, and the DPO role in incident response is vacant.	High — pre-launch	MD / Legal counsel
OI-5	Designate at least one deputy who can act as Incident Lead and Authority Communicator if Prof. Dr. Landgraf is unreachable during a breach. Currently no deputy exists — this is a single point of failure for every incident-response role.	High	MD

ID	Item	Urgency	Owner
OI-6	Configure at minimum a basic alerting mechanism for authentication failure spikes, error-rate anomalies on data endpoints, and unusual access patterns. Current detection gap means breaches may go unnoticed until a user reports them.	Medium – post-launch	Engineering
OI-7	Confirm that the BlnBDI online breach-notification form URL is current (https://www.datenschutz-berlin.de/) and test that submissions can be filed. Note the URL in the breach register for use under pressure.	Medium	MD
OI-8	Obtain external legal review of this procedure. The procedure was drafted internally without legal counsel input and may not fully reflect the current state of BlnBDI guidance or EDPB opinion on specific scenarios (e.g. sub-processor chain notification timing, Art. 34(3) exemption application).	Medium	MD / Legal counsel
OI-9	Assess and decide on disk encryption at rest (Hetzner volume). Currently the production disk is unencrypted (confirmed 2026-07-15, DPIA action A1). A disk-level breach (hypervisor access, stolen volume image) would expose all SQLite data and run directories in plaintext. Enabling LUKS/dm-crypt encryption would allow Art. 34(3)(a) to be invoked for disk-level incidents.	Medium	Engineering / MD
OI-10	Confirm statutory retention period for withdrawal_consent records (DPIA action A7) and company_profiles table (DPIA action A8). These affect how long certain data must be preserved even after an erasure request following a breach.	Medium	Legal counsel

Approved by: Prof. Dr. Tim Landgraf, Managing Director, CIATA GmbH **Date:** 2026-08-11 **Next review:** 2027-08-11 (or immediately following any breach, whichever comes first)