VAETHRA

Data Processing Agreement

Vaethra · Version 1.0

Issued 8 September 2026

The current version of this document is always at vaethra.com

security@vaethra.com · vaethra.com/trust

VAETHRA.COM/LEGAL/DPA

Data Processing Agreement

VERSION 1.0 · 7 SEPTEMBER 2026

> **What this is.** A Data Processing Agreement ready to execute. It applies automatically to every customer whose use of the Services involves Vaethra processing personal data on their behalf, and it is incorporated into the Terms by reference — so in most cases there is nothing to sign. If your process requires a countersigned copy, or your own DPA template, write to security@vaethra.com and you will have it within five business days.
>
> **Read this first.** Vaethra has no user accounts and holds very little personal data. In practice the categories below are business contact details, API key records and webhook destinations. See /security/privacy for the plain-language version of everything in this document.

1. Parties, scope and order of precedence

This Data Processing Agreement ("**DPA**") is entered into between the customer identified in the applicable order or agreement ("**Customer**", the controller) and **Vaethra Technologies LLC**, a limited liability company organised under the laws of the State of Wyoming, United States, with its mailing address at 30 N Gould St Ste N, Sheridan, Wyoming 82801, United States ("**Vaethra**", the processor).

It applies to Vaethra's processing of Personal Data on Customer's behalf in providing the Services, and forms part of the agreement between the parties (the "**Agreement**").

Where this DPA conflicts with the Agreement in respect of the processing of Personal Data, **this DPA prevails**. Where this DPA conflicts with the Standard Contractual Clauses incorporated under §10, **the Standard Contractual Clauses prevail**.

2. Definitions

"**Applicable Data Protection Law**" means Regulation (EU) 2016/679 (GDPR), the UK GDPR and Data Protection Act 2018, and any other data protection law applicable to the processing — including the national implementing law of the Member State in which Customer is established.

"**Personal Data**", "**controller**", "**processor**", "**data subject**", "**processing**" and "**personal data breach**" have the meanings given in the GDPR.

"**Subprocessor**" means any processor engaged by Vaethra to process Personal Data on Customer's behalf.

3. Roles

Customer is the controller of Personal Data it submits to or configures within the Services, and warrants that it has a lawful basis for that processing and has provided any notices required of it.

Vaethra is the processor of that data and processes it only on Customer's documented instructions.

Vaethra is an **independent controller**, not a processor, in respect of: (a) business contact details of Customer's personnel used to administer the relationship; (b) billing and contract records; and (c) the public record that constitutes the Services' own dataset, which is not Customer data. That processing is described in the Privacy Policy and is outside this DPA.

4. Processing details (Annex I)

Subject matter. Provision of the Vaethra Services.

Duration. The term of the Agreement, plus the deletion period in §12.

Nature and purpose. Hosting, storage, transmission, authentication, rate limiting, delivery of alerts, and support.

Categories of data subject. Customer's personnel who administer or use the Services; recipients of alerts Customer configures.

Categories of Personal Data.

- Business contact details — name, work email address, organisation, and where supplied, telephone number.
- API credential records — a SHA-256 digest of the issued key, its owner, its scope and its usage. **The key itself is never stored.**
- Request logs — path, status code, response size, timing, and the key that made the request.
- Alert rule configuration — the destination URL Customer registers and the conditions it fires on.
- Technical metadata inherent to any web request — IP address, user-agent, timestamp.

Special categories of Personal Data. None. Customer must not submit special-category data, children's data, or data subject to sector-specific regimes such as HIPAA, to the Services.

Vaethra does not sign Business Associate Agreements.

Frequency. Continuous, for the duration of the Agreement.

5. Vaethra's obligations

Vaethra shall:

1. **Process only on documented instructions** from Customer, including as to international transfers, unless required otherwise by applicable law — in which case Vaethra will inform Customer before processing, unless that law prohibits it on important grounds of public interest.
2. **Inform Customer immediately** if, in Vaethra's opinion, an instruction infringes Applicable Data Protection Law.
3. **Ensure confidentiality.** Every person authorised to process Personal Data is bound by a written confidentiality obligation.
4. **Implement the technical and organisational measures** set out in Annex II (§14), and not materially reduce them during the term.
5. **Respect the conditions on engaging Subprocessors** in §6.
6. **Assist Customer** with data subject requests, as set out in §7.
7. **Assist Customer** with obligations under Articles 32 to 36 GDPR — security, breach notification, impact assessments and prior consultation — taking into account the nature of the processing and the information available to Vaethra.
8. **Delete or return** Personal Data as set out in §12.
9. **Make available** the information necessary to demonstrate compliance, and allow for audits, as set out in §9.
10. **Not sell, rent, share or otherwise disclose** Personal Data to any third party except as permitted by this DPA. Vaethra operates no advertising, no analytics brokerage and no data brokerage of any kind.

6. Subprocessors

Customer grants **general written authorisation** for Vaethra to engage Subprocessors, subject to this section.

The current list of Subprocessors, including each one's purpose, the data it processes, its location and its own attestations, is published and kept current at vaethra.com/security/subprocessors.

Vaethra shall:

- Give Customer **30 days' notice by email** before adding or replacing a Subprocessor.
- Impose on each Subprocessor, by written contract, data protection obligations **no less protective** than those in this DPA.
- Remain **fully liable** to Customer for each Subprocessor's performance.
- Assess each Subprocessor before engagement and review it at least annually.

Objection. Customer may object to a new Subprocessor on reasonable data-protection grounds within the 30-day notice period. The parties will discuss in good faith. **If no resolution is reached, Customer may terminate the affected Services without penalty**, with a pro-rata refund of prepaid fees for the unused term and a full export of its data under §12.

7. Data subject rights

Taking into account the nature of the processing, Vaethra shall assist Customer by appropriate technical and organisational measures, insofar as possible, in fulfilling Customer's obligations to respond to requests to exercise rights of access, rectification, erasure, restriction, portability and objection.

Where Vaethra receives a request directly from a data subject relating to Customer's Personal Data, Vaethra will **not respond to it substantively itself**, and will notify Customer without undue delay so Customer can respond as controller.

Customer can exercise most rights directly through the Services: alert rules can be deleted at any time, keys revoked immediately, and an export requested at any time. Requests to privacy@vaethra.com are answered within **one month**, extendable by two months for a genuinely complex request, in which case Customer is told within the first month and given the reason.

8. Personal data breach

Vaethra shall notify Customer **without undue delay and in any event within 72 hours** of becoming aware of a personal data breach affecting Customer's Personal Data.

The notification will describe, to the extent known and with further information supplied as it becomes available:

- the nature of the breach, including the categories and approximate number of data subjects and records concerned;
- the name and contact details of the point of contact;
- the likely consequences; and
- the measures taken or proposed, including to mitigate adverse effects.

Vaethra will additionally notify Customer of **any confirmed unauthorised access to production systems, whether or not Personal Data was involved**. Customer's assessment of that risk is Customer's to make.

A written post-incident report follows within **5 business days** of resolution. The full process is published at vaethra.com/security/incident-response.

9. Audit

Vaethra shall make available to Customer all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, conducted by Customer or an auditor mandated by Customer.

In practice, and in this order:

1. **Published documentation.** The trust centre at vaethra.com/trust answers most audit questions in public.
2. **The evidence pack, under NDA**, within two business days: security policies, risk register, access-control evidence, disaster-recovery test results, vulnerability assessment and vendor assessments.
3. **Security questionnaires** completed in writing, typically within five business days.
4. **A call with the engineering owner** to answer architecture questions directly.
5. **An on-site or remote audit** where the above is genuinely insufficient: on 30 days' written notice, no more than once in any 12-month period except following a personal data breach, during business hours, subject to confidentiality, and without unreasonable disruption. Customer bears its own costs; Vaethra bears its own for the first such audit in any 12-month period.

Vaethra's controls are built to the SOC 2 Trust Services Criteria and the ISO/IEC 27001:2022 Annex A control set, with a control-by-control map published at vaethra.com/compliance. **Attestation and certification are in progress and neither is yet issued**, which is stated in this agreement rather than only in marketing material, because Customer's audit rights above stand in their place until they are.

10. International transfers

Vaethra processes Personal Data in the **United States**, in AWS region `us-east-2`, and at Cloudflare edge locations globally. **An EU region is available on enterprise agreements**; where residency is agreed at contract, the database is provisioned accordingly and the transfer mechanism below applies only to edge processing.

For transfers of Personal Data from the EEA to a third country without an adequacy decision, the parties incorporate the **Standard Contractual Clauses** approved by Commission Implementing Decision (EU) 2021/914, **Module Two (controller to processor)**, which are hereby incorporated by reference, with:

- **Clause 7 (docking)**: included.
- **Clause 9 (subprocessors)**: Option 2, general written authorisation, with the 30-day notice period in §6.
- **Clause 11 (redress)**: the optional independent dispute resolution body is *not* included.
- **Roles**: Customer is the *data exporter* and controller; Vaethra is the *data importer* and processor. Vaethra is established in the United States and is not established in the EEA.
- **Clause 17 (governing law)**: Option 2 — the law of the EU Member State in which the data exporter is established. Where that law does not allow third-party beneficiary rights, or where the data exporter is not established in the EEA, the law of **Ireland**.
- **Clause 18(b) (forum)**: the courts of the Member State whose law governs under Clause 17.
- **Annex I**: the parties are as identified in the Agreement; the processing details are in §4; the competent supervisory authority under Clause 13 is that of the Member State in which the data exporter is established.
- **Annex II**: the measures in §14.
- **Annex III**: the Subprocessor list at vaethra.com/security/subprocessors.

For transfers from the United Kingdom, the parties incorporate the **UK International Data Transfer Addendum** (version B1.0) to the above, with Tables 1 to 4 completed by reference to this DPA and neither party able to terminate under Section 19.

Supplementary measures. Encryption in transit and at rest; pseudonymisation of credentials as digests; strict data minimisation, since the Services hold almost no Personal Data at all; and the government-access commitments in §11.

11. Government and law enforcement access

If Vaethra receives a legally binding request from a public authority for Customer's Personal Data, Vaethra shall:

- **Notify Customer** before disclosure, unless legally prohibited — and where prohibited, use reasonable efforts to obtain a waiver and to challenge the prohibition.
- **Challenge the request** where there are reasonable grounds to consider it unlawful under the law of the requesting country or under Applicable Data Protection Law.
- **Disclose only the minimum** that a reasonable interpretation of the request requires.

- **Document** the request and the response, and make that record available to Customer and to the competent supervisory authority.

Vaethra has never received a government request for customer data, has never provided any government with direct or indirect access to any system, and operates no facility that would allow it. Should the first of these cease to be true, this paragraph will change.

12. Deletion and return

On termination or expiry of the Agreement, at Customer's election, Vaethra shall **delete or return** all Personal Data processed on Customer's behalf, and delete existing copies, unless retention is required by Union or Member State law.

- **Export** in a machine-readable format is available at any time during the term, and for **30 days** after it ends. There is no export fee and no exit fee.
- **Deletion** completes within **30 days** of the request or of the end of the 30-day export window, across primary storage and caches.
- **Backups age out** rather than being surgically edited. Deleted data disappears from backups within the backup retention window (currently 7 days). Backups remain encrypted and access-controlled throughout. This is stated plainly because no honest provider edits a backup to remove a row.
- **Statutory retention.** Contract and billing records are retained for **7 years** to meet tax and accounting record-keeping requirements. This is a legal obligation and cannot be waived by either party.

13. Liability, term and general

Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement, save that nothing limits either party's liability to a data subject under Clause 12 of the Standard Contractual Clauses or under Applicable Data Protection Law.

This DPA takes effect on the effective date of the Agreement and continues for as long as Vaethra processes Personal Data on Customer's behalf.

If any provision is held invalid, the remainder continues in force. This DPA is governed by the laws of the State of Wyoming, United States, without regard to its conflict-of-laws rules, and the state and federal courts sitting in Wyoming have exclusive jurisdiction — without prejudice to the governing law and forum elected for the Standard Contractual Clauses in §10, or to a data subject's rights under Clauses 18(c) and (d) of those Clauses.

Vaethra may update this DPA to reflect a change in law, a regulator's guidance, or an improvement in its own measures, provided no update materially reduces the protection

afforded to Customer. Material updates are notified **30 days** in advance by email.

14. Technical and organisational measures (Annex II)

These are the measures referred to in Article 32 GDPR and in Clause 8.6 of the Standard Contractual Clauses. Each is described in full at vaethra.com/trust; the cross-references are given so this annex can be read against evidence rather than taken on trust.

14.1 Pseudonymisation and encryption

- TLS 1.2 minimum and TLS 1.3 preferred for all data in transit, with HSTS for one year including subdomains.
- AES-256 encryption at rest for the database, its backups, and object storage.
- API keys stored as SHA-256 digests only. The key is displayed once at creation and is not recoverable by anyone, including Vaethra.
- Secrets held in platform secret stores, injected at runtime, not readable back after being set.
- Alert rules owned by an anonymous browser-generated token rather than by an identity.
- No cookies, no third-party trackers and no third-party fonts on any Vaethra property, and no Personal Data processed under this DPA is disclosed to any party outside the subprocessor list in §6. Separately, and not in scope of this DPA: a visitor who opens the map in the free Terminal has their browser fetch tiles, map label fonts and — only if they switch it on — the aircraft layer directly from those providers, which therefore see the requesting IP address and nothing else. They are named in the Privacy Notice.
- Reference: /security/data-protection.

14.2 Confidentiality, integrity, availability and resilience

- Row-level security enabled deny-by-default on all 50 tables in the analytical schema, verified 7 September 2026.
- The public database role holds EXECUTE on 0 of 77 database functions, verified 7 September 2026; the privileged role never leaves the database provider's boundary.
- Administrative endpoints gated twice — identity-aware proxy at the network edge, and an application bearer token — neither origin-based.
- Multi-factor authentication mandatory on every administrative account, with no exception process. Hardware-backed factors preferred; SMS not used.
- Least privilege, with production access held by a single named individual, reviewed quarterly.

- Stateless, globally distributed edge compute with automatic routing around a failed location.
- Per-caller rate limiting; WAF, bot management and DDoS protection at the edge.
- Reference: /security/access-control, /security/availability.

14.3 Restoring availability and access

- Continuous encrypted database backup with daily snapshots, stored separately from the primary. Retention 7 days standard, 28 days on enterprise agreements.
- Committed recovery objectives: RPO 24 hours and RTO 4 hours standard; **RPO 5 minutes and RTO 2 hours on enterprise agreements**, using point-in-time recovery.
- Restore tested to a scratch instance, with a written report of what was restored, from which backup, how long it took and what failed.
- Automated invariant checks run against a restored system before recovery is declared, so a restore that has silently lost an index, a trigger or a licence gate is detected rather than declared healthy.
- Immutable versioned deployments with rollback in about one minute.
- Reference: /security/business-continuity.

14.4 Testing and evaluating effectiveness

- 985 automated tests and static type checking as hard gates before any deployment, including tests asserting that security controls refuse.
- Continuous automated dependency scanning with pinned, lockfile-controlled versions.
- Commit scanning for credential patterns.
- An automated data-invariant suite that detects controls which have silently stopped working, including a probe for licence-gate leakage that pages on detection.
- Patch windows: 24 hours critical, 7 days high, 30 days medium, 90 days low.
- An independent penetration test is scheduled ahead of general availability; the report will be provided under NDA once complete. Stated here because an annex of measures that omitted its status would be incomplete. See /security/vulnerability-management.

14.5 Identification, authorisation and transfers

- Individual accounts only; no shared human accounts. Service credentials are not attached to a person.
- Access granted at the minimum level for the role; production access not granted by default.

- Offboarding within one business day, immediate for an involuntary departure, with rotation of any credential the departing person could have seen.
- Annual credential rotation as a floor, and immediate rotation on any suspicion of exposure.
- Transfers to Subprocessors governed by written contracts with protections no weaker than this DPA.
- Reference: /security/access-control, /security/subprocessors.

14.6 Governance

- Written policies covering access control, change management, incident response, cryptography, acceptable use, vendor management and business continuity. Available under NDA.
- A risk register reviewed quarterly and after any incident.
- An Article 30 record of processing activities.
- Confidentiality undertakings signed before any access is granted; background checks for roles with production access, to the extent applicable employment law permits.
- Subprocessors assessed before engagement and reviewed annually.
- Reference: /security.

15. Contact

Data protection matters: privacy@vaethra.com.
Security, DPAs, evidence and questionnaires: security@vaethra.com.
Everything else: support@vaethra.com, or +43 678 1261314 for enterprise customers.

Notices. Vaethra Technologies LLC, 30 N Gould St Ste N, Sheridan, Wyoming 82801, United States. Notices are also valid by email to legal@vaethra.com.

Supervisory authority. Vaethra is established in the United States and has no lead supervisory authority of its own. Where Customer is established in the EEA or the United Kingdom, the competent authority is the one with jurisdiction over Customer — the supervisory authority of Customer's own Member State, or the UK Information Commissioner's Office.