Alphix Association

Privacy Policy

Last updated: 4 February 2026

This Privacy Policy explains how the Alphix Association ("**Association**," "**we**," "**us**," "**our**") processes personal data in connection with www.alphix.fi (the "**Website**"), our web-application user interface (the "**App**"), our documentation site, and related communications (together, the "**Services**"). Capitalised terms not defined here have the meanings given in the Terms of Service (the "**Terms**").

For the purposes of the EU General Data Protection Regulation (Regulation (EU) 2016/679, the "**GDPR**"), the UK GDPR, and the Swiss Federal Act on Data Protection ("**FADP**"), the Association is the data controller for the processing described in this Policy.

If you are located in the UK, EEA, or Switzerland, you have statutory rights—see **Section 6 (Your Rights)** below.

---

1. Data We May Collect

- **Technical and usage data:** IP address, approximate location (derived from IP), device and browser details, operating system, language and time zone, access timestamps, event telemetry, performance and error logs, and referrers.
- **Wallet and on-chain data:** Public wallet addresses you connect, transaction hashes, and smart-contract interactions surfaced in the App (public blockchain data).
- **Compliance signals:** Outcomes from geofencing, sanctions-screening, and wallet-screening (e.g., pass/fail, reason codes).
- **Communications:** Email address, name (if provided), message contents, and related metadata when you contact us.
- **Acceptance records:** Timestamp, IP address, device metadata, and wallet address and/or signed message evidencing acceptance of the Terms and this Privacy Policy.
- **Cookies and similar technologies:** Strictly necessary cookies; analytics and other non-essential cookies only with consent where required by applicable law.

We do not intentionally collect special category data (e.g., health, biometric, racial, or political data); please do not submit such data to us.

We do not perform KYC/AML identity verification for users. If any third-party service integrated with the Protocol conducts such processing, it does so under its own privacy notice as an independent controller.

We apply data minimisation principles and collect only what is necessary for the purposes described in this Policy.

---

2. Purposes and Legal Bases

We process personal data only for the purposes below. Where more than one legal basis applies, we rely on each in the alternative.

Purpose	Legal Basis (GDPR/FADP)
Operate and secure the Services (availability, performance, debugging, fraud/abuse prevention)	Legitimate interests (operate and protect the Services); Contract where processing is necessary to deliver requested features
Render blockchain data in a non-custodial interface	Legitimate interests (provide a functional, non-custodial interface)
Apply geo-/sanctions- and wallet-screening controls	Legal obligation (where applicable); Legitimate interests (compliance risk management)
Create and retain acceptance records (evidential logs of consents/agreements)	Legitimate interests (record-keeping; defence of legal claims); Contract where the request relates to services you use
Respond to enquiries and support requests	Legitimate interests; Contract where applicable
Product analytics and UX improvement (non-essential)	Consent — withdraw at any time via the cookie banner/settings
Legal, regulatory, and dispute management	Legal obligation; Legitimate interests (establish, exercise, or defend legal claims)

We apply data minimisation and do not process personal data beyond these purposes. Where we rely on legitimate interests, we have conducted a balancing test and can provide key considerations on request.

---

3. Public Blockchains and Your Rights

Public blockchains are public, append-only networks operated by independent third parties. We do not control those networks and cannot delete, alter, hide, or overwrite on-chain records (e.g., wallet addresses, transactions, calldata).

3.1 What We Can Do (Off-Chain)

- Suppress or restrict further processing of any off-chain copies or references we hold.
- Unlink or pseudonymise wallet-to-profile mappings we maintain.
- Cease display of associated data in our UI and, where appropriate, apply UI-level blocking to specified addresses.

3.2 What We Cannot Do (On-Chain)

- Remove, edit, or obfuscate transactions or addresses already recorded on public ledgers.
- Interfere with third-party block explorers or archival nodes.

3.3 Verification

We may ask you to prove wallet control (e.g., via a signed on-chain message) before actioning requests relating to that address.

3.4 Portability and Erasure

We will provide portable copies of off-chain personal data we hold upon valid request. For erasure, we will delete or isolate off-chain data where possible; we may retain limited evidential logs (e.g., acceptance records) where required by law or for the establishment, exercise, or defence of legal claims, and will minimise and restrict access to those records.

3.5 Practical Caution

Please do not embed personal information in on-chain memo or data fields. Such disclosures are permanent and outside our control.

---

4. Sharing and International Transfers

4.1 Who We Share With

We do not sell personal data. We disclose personal data only where necessary to operate, secure, and support the Services, or where required by law, to:

- **Processors** — hosting/CDN providers, DDoS/security services, logging/observability tools, analytics (consent-based where required), acceptance-log storage, and geo/sanctions/wallet-screening vendors.
- **Professional advisers and auditors** — legal, regulatory, tax, and audit advisers.
- **Corporate transaction counterparties** — in connection with mergers, acquisitions, financings, or similar events (subject to strict confidentiality).
- **Competent authorities** — in response to lawful, proportionate requests.

4.2 International Transfers

Where personal data is transferred outside Switzerland or the EEA (e.g., to the US), we implement appropriate safeguards, including:

- EU Standard Contractual Clauses (2021/914) and/or the Swiss Federal Data Protection and Information Commissioner's approved clauses;
- documented transfer impact assessments and supplementary measures (e.g., encryption in transit and at rest, strict access controls, data minimisation) where required; and
- contractual limits on onward transfers, audit rights, and mandatory incident notice by processors and sub-processors.

4.3 Data-Residency Note

Our primary hosting and infrastructure providers currently operate in the EU/EEA, Switzerland, and the USA. We will update this Policy if our hosting footprint materially changes.

4.4 Sub-Processor Transparency

A current list of processors and sub-processors and related safeguards is available on request at privacy@alphix.fi. We require sub-processors to apply protections no less protective than ours.

4.5 Law-Enforcement Requests

We assess governmental and law-enforcement demands for legality, necessity, and scope, and seek to narrow or object where appropriate. Where lawful, we will notify affected users before disclosure or as soon as permitted thereafter.

---

5. Retention

We retain personal data only for as long as needed for the purposes in this Policy, then delete or irreversibly anonymise it.

- **Acceptance logs and key legal records** — 10 years from last interaction (or longer if required by applicable limitation periods, audits, or disputes, consistent with Swiss commercial record-keeping requirements under the Swiss Code of Obligations).
- **Technical and operational logs** — 90 days to 12 months, depending on security, troubleshooting, and integrity needs.
- **Support correspondence** — up to 3 years from ticket closure.
- **Analytics** — per your consent settings; thereafter held in aggregated or anonymised form where feasible.

5.1 Criteria

Retention periods reflect the purpose of processing, legal and contractual duties, applicable limitation periods, and risk. Legal holds suspend deletion until lifted.

5.2 Backups

Deleted data may persist transiently in encrypted backups; backups roll off on a fixed schedule and access is strictly restricted.

5.3 Disposal

On expiry, we perform secure deletion or one-way anonymisation and restrict any residual artefacts to time-bound, controlled access.

---

6. Your Rights

Subject to applicable law and verification requirements, you may have the following rights with respect to your personal data:

- **Access** — request confirmation of whether we process your personal data and obtain a copy.
- **Rectification** — request correction of inaccurate or incomplete data.

- **Erasure** — request deletion of personal data (subject to blockchain constraints and legal retention requirements).
- **Restriction** — request that we restrict processing in certain circumstances.
- **Objection** — object to processing based on legitimate interests.
- **Portability** — receive your personal data in a structured, commonly used, machine-readable format.
- **Withdraw consent** — where processing is based on consent, withdraw at any time (without affecting the lawfulness of processing before withdrawal).

How to Exercise Your Rights

Email **privacy@alphix.fi**. We may ask you to verify your identity and, where relevant, prove wallet control (e.g., by a signed on-chain message).

Timelines and Fees

We aim to respond within one month; we may extend by up to two further months for complex or numerous requests (we will notify you). We do not charge a fee unless a request is manifestly unfounded, repetitive, or excessive, in which case we may charge a reasonable fee or refuse to act.

On-Chain Limits

Public blockchain records cannot be altered or deleted by us; we will action off-chain data (e.g., suppression, restriction, unlinking wallet-to-profile mappings) as set out in Section 3.

Complaints

You may lodge a complaint with the Swiss Federal Data Protection and Information Commissioner (FDPIC) or, if you are in the EEA or UK, with your local supervisory authority (e.g., the ICO in the UK). You may also contact us first, and we will seek to resolve the matter.

---

7. Children

The Services are intended for adults (18+). We do not knowingly collect personal data from children. If you believe a child has provided personal data, contact privacy@alphix.fi; we will delete it and, where appropriate, disable related access.

---

8. Security and Incidents

We implement technical and organisational measures appropriate to risk (GDPR Art. 32; FADP requirements), including:

- Role-based access controls and multi-factor authentication;
- Least-privilege access principles;
- Encryption in transit and at rest with managed key rotation;
- Network segmentation and rate-limiting;
- Secure software development practices (peer review, dependency scanning, SCA/SAST);

- Periodic security assessments and third-party penetration tests;
- Vulnerability management with defined response timelines;
- Centralised logging, monitoring, and anomaly detection;
- Hardened build and patch processes;
- Data minimisation and segregation;
- Processor agreements (DPAs) and vendor due diligence.

8.1 Incident Response

We maintain a documented incident-response plan (containment → assessment → notification → remediation → post-incident review).

- **Breach notification:** If we become aware of a personal-data breach likely to pose a risk to individuals, we will notify the relevant supervisory authority without undue delay (and, where GDPR applies, within 72 hours of awareness where feasible: Art. 33). Where required (e.g., high risk to individuals), we will also notify affected individuals without undue delay (Art. 34). Under FADP, we will notify the FDPIC as soon as possible where the breach is likely to result in a high risk to the personality or fundamental rights of data subjects.
- **Vulnerability disclosure:** Report security issues to **security@alphix.fi** with steps to reproduce so we can triage promptly.

---

9. Automated Decision-Making

We do not engage in solely automated decision-making that produces legal or similarly significant effects about you (GDPR Art. 22).

The Association may use automated screening signals (e.g., geofencing, sanctions/wallet screening) to gate access to features for compliance purposes. These controls operate under legitimate interests and/or legal obligations and are subject to human review on request. You may request human intervention, express your view, and challenge an outcome by contacting privacy@alphix.fi (we may ask you to prove wallet control).

---

10. Third-Party Protocols and Links

When you interact with Third-Party Protocols through the App (e.g., Uniswap, Aave, Sky), your interactions are governed by those protocols' own terms and, where applicable, privacy practices. The Association is not responsible for, and does not endorse, third-party content, policies, or practices.

Access to third-party sites, tools, or integrations is at your discretion and governed by the relevant provider's terms and privacy notice.

---

11. Cookies

We use strictly necessary cookies to operate the Services. Analytics and other non-essential cookies run only with your consent where required by applicable law.

You can manage your cookie preferences at any time via the cookie banner or cookie settings in the App.

Types of Cookies We Use

Category	Purpose	Consent Required
Strictly Necessary	Essential for the Services to function (e.g., session management, security)	No
Analytics	Understand how users interact with the Services to improve functionality	Yes (UK/EEA/CH)
Functional	Remember your preferences (e.g., language, display settings)	Yes (UK/EEA/CH)

---

12. Changes

We may update this Policy from time to time. We will post a new "Last updated" date and, where required (e.g., new processing purposes or materially different practices), provide additional notice and/or seek fresh consent.

We encourage you to review this Policy periodically to stay informed about our data practices.

---

13. Contact

Questions, requests, or complaints:

Email: privacy@alphix.fi

Alphix Association: Canton of Zug, Switzerland

Summary of Key Points

Topic	Summary
Data Controller	Alphix Association (Swiss association, Canton of Zug)
Data Collected	Technical/usage data, wallet addresses, compliance signals, communications, acceptance records, cookies
Legal Bases	Contract, legitimate interests, consent (where required), legal obligation

Topic	Summary
International Transfers	Safeguards including SCCs, TIAs, encryption, access controls
Retention	10 years for legal records; 90 days–12 months for operational logs
Your Rights	Access, rectification, erasure (off-chain), restriction, objection, portability, withdraw consent
Blockchain Limitations	On-chain data cannot be altered or deleted
Supervisory Authority	Swiss FDPIC; UK ICO or local EEA authority if applicable
Contact	privacy@alphix.fi