MAKINA (BVI) LTD

PRIVACY POLICY

Last updated 25 September 2025

This Privacy Policy explains how Makina (BVI) Ltd. ("**Company**", "**we**", "**us**", "**our**") processes personal data in connection with www.makina.finance (the "**Website**"), our web-application user interface (the "**App**"), our documentation site, and our social channels (together, the "Services"). Capitalised terms not defined here have the meanings given in the Terms of Service (the "**Terms**").

For the purposes of the UK GDPR and EU GDPR, the Company is the data controller for the processing described in this Policy. Operators (as defined in the Terms) act as independent controllers for any KYC/AML and issuance-related processing and are not our processors. For BVI purposes, the Company is also a data controller under the BVI Data Protection Act, 2021 and adheres to its seven data-protection principles.

If you are in the UK or EEA, you have statutory rights—see Your Rights below.

1 Data we may collect

- **Technical & usage data**: IP address, approximate location (derived from IP), device and browser details, language and time zone, event telemetry, performance/crash logs, and referrers.
- **Wallet & 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.
- **Acceptance records**: timestamp, IP address, device metadata, and wallet address and/or signed message evidencing acceptance of the Terms and this Privacy Policy.
- **Cookies/SDKs**: strictly necessary cookies; analytics only with consent in the UK/EEA.

We do not intentionally collect special-category data; please do not submit it to us. We do not perform KYC/AML for issuances. Operators (or their vendors) conduct such processing under their own notices. We apply data minimisation and collect only what is necessary for the purposes described in this Policy.

2 Purposes and lawful bases

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

Purpose	Lawful basis (UK/EU)
Operate and secure the Services or Covered Activities, as defined in the Terms (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 and Operator parameters in a non-custodial UI	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 notices/consents)	Legitimate interests; 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 (UK/EEA) — withdraw at any time via the 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 beyond these purposes. Where we rely on legitimate interests, we have conducted a balancing test and can provide key considerations on request. For BVI processing, we also align with the BVI Data Protection Act, 2021 principles (Notice & Choice, Disclosure, Security, Retention, Data Integrity, Access).

3 Public blockchains and your rights

Public blockchains are public, append-only networks operated by third parties. We do not control those networks and cannot delete, amend, 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/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. 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 and will minimise and restrict access to those records.

3.5 Practical caution

Please do not embed personal information in on-chain memo/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 certain Covered Activities, or where required by law, to:

- **Processors** — hosting/CDN, DDoS/security, logging/observability, analytics (consent-based in the UK/EEA), acceptance-log storage, and geo/sanctions/wallet-screening.
- **Professional advisers and auditors** — legal, regulatory, tax and audit.
- **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 the UK/EEA (e.g., to the US or BVI), we implement appropriate safeguards, including:

- EU Standard Contractual Clauses (2021/914) and/or the UK IDTA/UK Addendum (as applicable);
- documented transfer impact assessments and supplementary measures (e.g., encryption in transit/at rest, strict access controls, data minimisation, logical segregation) where required; and
- contractual limits on onward transfers, audit rights, and mandatory incident notice by processors/sub-processors.

4.3 Data-residency note

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

4.4 Sub-processor transparency

A current list of processors/sub-processors and related safeguards is available on request at

privacy@makina.finance (or via our public registry, if provided). We require sub-processors to apply protections no less protective than ours.

4.5 BVI alignment

Cross-border transfers in BVI-scoped processing are undertaken in line with the BVI Data Protection Act, 2021 principles (including Security, Retention and Disclosure).

4.6 Law-enforcement requests

We assess governmental/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 & key legal records** — 6 years from last interaction (longer if required by limitation periods, audits or disputes).
- **Technical/operational logs** — 90 days–12 months, depending on security, troubleshooting and integrity needs.
- **Support correspondence** — up to 3 years from ticket closure.
- **Analytics** — per your consent settings; then held aggregated/anonymised where feasible.

5.1 **Criteria**. Periods reflect purpose, legal/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 (UK/EEA)

Subject to conditions, you may have rights to access, rectification, erasure (subject to blockchain constraints), restriction, objection, portability, and to withdraw consent (for consent-based processing).

- **How to exercise**: email privacy@makina.finance We may ask you to verify identity and, where relevant, prove wallet control (e.g., by a signed on-chain message).
- **Timelines & 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 complain to 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@makina.finance; 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; BVI DPA principles), including: role-based access and MFA; least-privilege; encryption in transit and at rest with managed key rotation; network segmentation and rate-limiting; secure SDLC (peer review, dependency scanning, SCA/SAST), periodic third-party penetration tests; vulnerability management with defined SLAs; centralised logging/monitoring and anomaly detection; hardened build/patch processes; data minimisation and segregation; processor DPAs and vendor due diligence.

8.1 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, aim to notify within 72 hours of awareness: Art. 33). Where required (e.g., high risk), we will also notify affected individuals without undue delay (Art. 34).
- Vulnerability disclosure. Report security issues to security@makina.finance 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 Company may use automated screening signals (e.g., geofencing, sanctions/wallet screening) to gate access to features for compliance. 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@makina.finance (we may ask you to prove wallet control, e.g., via a signed on-chain message).

10 Operators and third-party links

When you engage with an Operator (e.g., KYC/AML or a primary issuance), your personal data is processed under that Operator's own privacy notice as an independent controller. We are not

responsible for, and do not endorse, third-party content, policies or practices. Access to third-party sites, tools or SDKs is at your discretion and governed by the relevant provider's terms and privacy notice.

11 Cookies (PECR/ePrivacy)

We use strictly necessary cookies to operate the Services. Analytics run only with your consent in the UK/EEA.

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 cookie categories or materially different purposes), provide additional notice and/or seek fresh consent).

13 Contact

Questions or requests: privacy@makina.finance.