Privacy Policy

Effective date: 1 June 2026

Version: 1.0

Operator: 0xposed — a worldwide, decentralised initiative supporting victims of cryptocurrency theft. No registered legal entity at this stage; structure may evolve into a DAO or another form. See "Operating model" section below.

Platform: https://0xposed.io

Single contact point: contact@0xposed.io

Operating model — please read first

0xposed is currently a worldwide, informal initiative. It does not have a registered legal entity, a corporate seat, or designated country representatives at this stage. Its structure may evolve into a DAO or another legal form. Throughout this Policy, references to "we", "us" and "0xposed" mean the people who collectively operate the Platform. We commit to updating this Policy as soon as a formal legal entity is established. Until then, the single point of contact for any matter relating to personal data is contact@0xposed.io.

This Privacy Policy explains how 0xposed processes personal data when you visit https://0xposed.io (the "Platform"), submit information about cryptocurrency-theft incidents, post testimonials or comments, or otherwise interact with us. We have written it in plain English in line with Article 12 of the EU General Data Protection Regulation (GDPR).

Although 0xposed is not yet incorporated in any jurisdiction, the GDPR (EU/EEA), UK GDPR, the California Consumer Privacy Act (CCPA/CPRA), the LGPD (Brazil), the PIPL (China), PIPEDA (Canada), the Australian Privacy Act and similar laws apply to us by reason of our handling of personal data of residents of those jurisdictions. We treat this Policy as our binding global standard.

If you do not agree with how we handle personal data, please do not use the Platform.

Table of contents

1. Who we are and how to contact us

0xposed operates the platform at https://0xposed.io (the "Platform"), which (a) maintains a public radar of crypto-security incidents, (b) accepts confidential case-intake submissions from victims, and (c) hosts community testimonials and comments.

0xposed has no registered legal entity, corporate seat, or designated country representatives at this stage. Our structure may evolve over time (for example, into a DAO). Until a formal entity is constituted, the single way to reach us for any matter relating to personal data is by email.

Single contact point: contact@0xposed.io

Where applicable law (GDPR Art. 27, UK GDPR Art. 27) requires the appointment of a representative inside the EU/EEA or the UK, 0xposed will appoint one as soon as practicable and update this Policy accordingly. If you are in the EU/EEA or the UK and need to lodge a formal request before such appointment, please use the contact email above; we will treat your request with the same diligence as if a representative had already been designated.

2. Scope of this Policy

This Policy applies to all personal data we process in connection with the Platform — whether you:

- simply read the public radar,
- submit a public incident report for inclusion in the radar,
- submit a confidential case-intake form,
- post testimonials or comments, or
- contact us.

It does not apply to third-party websites linked from the Platform, including those of our security-firm partners. We encourage you to read those parties' own privacy policies.

3. Summary at a glance

The table below is a layered notice. Each row is detailed in the sections that follow.

Activity	Who is affected	What we collect	Lawful basis (GDPR)	How long we keep it
Reading the radar	Anyone	IP, browser/device data, cookies	Legitimate interest; consent for analytics/marketing cookies	Up to 13 months for cookies; 30 days for server logs

Public radar submission	Reporters	Email (optional), wallet addresses, incident description, supporting URLs	Legitimate interest; consent where required	Lifetime of the radar entry (subject to right to erasure / rectification)
Confidential case intake	Victims	Email, wallet addresses, supporting documents (screenshots, transaction proofs, communications), narrative	Performance of a service / pre-contract; legitimate interest; consent for sensitive content; legal obligation when responding to law enforcement	Up to 5 years from case closure unless required for ongoing investigation
Testimonials / comments	Authors and anyone named	Username, content, IP	Legitimate interest / consent	Lifetime of the post + 12 months in backups

4. Categories of personal data we collect

4.1 From you directly

- Identifiers: email address; chosen username (which may be a pseudonym); name and postal address only if you opt in to law-enforcement contact.
- Wallet addresses (your own, and those of the alleged scammer or compromised protocol).
- Transaction hashes, chain identifiers, amounts and token types.
- Free-text narrative describing the incident.
- Supporting documents: screenshots of transactions; screenshots of communications with the alleged scammer; copies of contracts or whitepapers; KYC documents you choose to submit.
- Content you post in testimonials and comments.

4.2 Collected automatically

- IP address (truncated where possible), user-agent, device type, language, referrer, pages visited, time stamps.
- Cookies and similar technologies (see our Cookie Policy).

4.3 From other sources

- Reports about the same incident from other users or from our security-firm partners.
- Public blockchain data (transaction graphs, address attributions).
- Public open-source intelligence (OSINT) about an alleged scam.
- Information from law-enforcement requests.

If you provide us with information about another person (a co-victim, a witness, an alleged scammer), you confirm you have a lawful basis to do so and that you will inform them of this Policy where required by applicable law.

5. How we collect personal data

We collect personal data through:

- forms on the Platform (public report, confidential intake, testimonials, comments);
- automated logging by our servers, hosting provider and analytics tools;
- disclosures from our security-firm partners (e.g., SlowMist, Chainalysis, TRM Labs, PeckShield, CertiK) within the scope of our cooperation agreements;
- publicly available blockchain explorers and OSINT sources.

6. Purposes and lawful bases

Under the GDPR (and equivalent regimes), we must have a "lawful basis" for every processing operation. The table below sets out our purposes and lawful bases.

Purpose	Lawful basis (GDPR Art. 6)	Notes
(a) Operate the public radar and inform the community	Art. 6(1)(f) legitimate interest in public-interest information and fraud prevention	Subject to a balancing test; rights of alleged wrongdoers respected via the notice-and-action procedure (see §7)
(b) Provide confidential case-intake support to victims	Art. 6(1)(b) performance of a service requested by the victim; Art. 6(1)(f) where Art. 6(1)(b) does not strictly apply	We process special-category or criminal-offence data only with explicit consent (Art. 9(2)(a)) or where authorised by Member-State law (Art. 10)
(c) Cooperate with law enforcement and judicial authorities	Art. 6(1)(c) legal obligation; Art. 6(1)(f) legitimate interest in fraud prevention; Art. 6(1)(d) vital interests in emergencies	
(d) Share with vetted security-firm partners for investigation	Art. 6(1)(f) legitimate interest	Subject to Data Processing Agreements and confidentiality obligations
(e) Publish anonymised / aggregated statistics and threat-intelligence reports	Art. 6(1)(f) legitimate interest	Data is de-identified to a level where re-identification is not reasonably likely (CJEU Breyer; EDPS v SRB)
(f) Send service emails	Art. 6(1)(b)	
(g) Send marketing emails	Art. 6(1)(a) consent	Withdrawable at any time without affecting prior lawful processing
(h) Security, anti-spam, anti-abuse	Art. 6(1)(f)	

7. Special note on wallet addresses, transaction data, and "alleged" attacker information

Wallet addresses are personal data when they are reasonably linkable to a natural person. This reflects the European Data Protection Board's Guidelines 02/2025 on processing of personal data through blockchain technologies (Section 3.2: "If the user is a natural person and those public keys can be used to identify the individuals by means reasonably likely to be used, for example in case of a data breach, then those identifiers qualify as personal data") and the Court of Justice of the European Union's ruling in Breyer (C-582/14).

When we publish wallet addresses, transaction hashes, project names, contact handles, or other identifiers tied to an alleged crypto theft, hack, rug-pull, phishing scheme or other malicious conduct:

- we do so on the basis of our legitimate interest in fraud prevention, victim assistance, and the public's right to information, balanced against the rights and freedoms of the data subject;
- we treat such information as descriptive of a reported incident, not as a finding of guilt or wrongdoing. Every public radar entry is labelled as a report and bears a disclaimer to that effect;
- where the information may qualify as *personal data relating to criminal convictions and offences within the meaning of Article 10 GDPR*, we limit our processing to what is strictly necessary for the public-interest purposes set out above, and we apply enhanced safeguards (limited internal access, mandatory review before publication, clear "alleged" labelling, and prompt response to rectification or erasure requests). 0xposed will obtain a formal legal opinion on the Member-State lawful basis as soon as it constitutes a legal entity;
- any named individual or entity may at any time invoke their right to rectification (Art. 16 GDPR) and right to erasure (Art. 17 GDPR) by writing to contact@0xposed.io or using the notice-and-action form. We respond within one month per Art. 12(3);
- we operate a Digital Services Act (DSA) Article 16 notice-and-action mechanism with a statement of reasons under Article 17 and an internal complaints-handling system under Article 20.

8. Who we share personal data with

We share personal data only with the following categories of recipients, and only as needed for the purposes stated above:

- **Hosting and infrastructure providers:** Vercel Inc. (hosting), and other technical providers we engage as processors under data processing agreements.
- **Security-firm partners** (e.g., SlowMist, Chainalysis, TRM Labs, PeckShield, CertiK) — only where investigation assistance is needed and under appropriate data processing agreements or joint controller arrangements. Where we share submitted wallet addresses for risk-control synchronisation (analogous to SlowMist's "InMist Threat Intelligence Network"), we say so on the relevant form.
- **Law-enforcement and judicial authorities** — in response to lawful subpoenas, warrants, court orders or comparable legal process, or where we believe in good faith that disclosure is necessary to prevent imminent harm to life or to comply with a legal obligation. Once 0xposed publishes Law Enforcement Guidelines, they will be linked here.

- **Professional advisors** (lawyers, accountants, auditors, insurers we engage in the future) — under duties of confidentiality.
- **Successors** — in a future formal incorporation, merger, acquisition, or governance transition (e.g., from informal initiative to DAO or registered entity), subject to the same protections.
- **Other users** — anything you post publicly (radar reports, testimonials, comments) is visible to all visitors.

We do not sell personal data and we do not "share" personal data for cross-context behavioural advertising within the meaning of the California Consumer Privacy Act (CCPA).

9. International data transfers

Because 0xposed operates worldwide and engages partners and providers in multiple jurisdictions (including the United States), personal data may be transferred outside your country of residence. We rely on the following safeguards as applicable to the data subject's location:

- **EEA/UK to third countries without adequacy:** 2021 EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), with the UK International Data Transfer Addendum / IDTA where UK personal data is involved, plus a documented Transfer Impact Assessment per the CJEU's Schrems II ruling (C-311/18).
- **EU/UK to U.S. partners certified under the EU–US Data Privacy Framework:** we rely on Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 where the recipient is certified.
- **Brazil transfers:** ANPD-approved Standard Contractual Clauses under Resolution CD/ANPD No. 19/2024.
- **China transfers:** PIPL Standard Contract or other valid mechanism; security assessment where thresholds are met.

Copies of safeguards are available on request to contact@0xposed.io. Brazilian data subjects may request the full text of the SCCs we use within 15 days of request.

10. How long we keep personal data (retention)

We retain personal data only as long as necessary for the purpose for which it was collected:

Data type	Retention
Cookies	Up to 13 months (see Cookie Policy)
Server logs	30 days, save where required for security investigation
Public radar entries	Lifetime of the entry; subject to rectification / erasure
Confidential case files (victim narrative + supporting documents)	Up to 5 years from case closure, unless we are required to hold them longer for an active law-enforcement matter or legal claim
Testimonials and comments	Lifetime of the post + 12 months in encrypted backups after deletion
Marketing email lists	Until you withdraw consent + 30 days for purge propagation
Accounting records (after formal	Statutory period applicable to the jurisdiction of incorporation (typically 7

incorporation)	to 10 years)

We do not use blockchain immutability as a justification for indefinite retention (consistent with EDPB Guidelines 02/2025 §4.7: "this is not a reason to assume that the lifetime of the blockchain is an appropriate data retention period; rather, data should be deleted when the end of the processing activity is reached").

11. How we keep personal data secure

We implement technical and organisational measures appropriate to the risk under Art. 32 GDPR, including:

- encryption in transit (TLS 1.2 or higher) and at rest for confidential case files;
- strict role-based access control to victim files;
- internal access logging;
- periodic security testing and vendor due diligence;
- data processing agreements with our processors;
- an incident-response plan and a 72-hour breach-notification protocol (Art. 33 GDPR).

12. Your rights and how to exercise them

Subject to applicable law and limited exceptions, you have the rights to:

- access (Art. 15), rectification (Art. 16), erasure / "right to be forgotten" (Art. 17),
- restriction (Art. 18) and data portability (Art. 20),
- object (Art. 21), including objection to processing based on legitimate interest,
- withdraw consent at any time (Art. 7(3)) without affecting prior lawful processing,
- not be subject to a decision based solely on automated processing producing legal effects (Art. 22) — we do not engage in such processing.

To exercise any right, write to contact@0xposed.io. We respond within one month (Art. 12(3)), extendable by two further months for complex requests, with notice to you. There is no fee unless the request is manifestly unfounded or excessive. If we cannot identify you on the basis of your request, we may ask for additional verification (Art. 12(6)).

13. Children

The Platform is intended for adults aged 18 and over. We do not knowingly collect personal data from children. If you become aware that a child has provided us personal data, please contact contact@0xposed.io; we will delete it without undue delay. Where applicable law sets a lower digital-consent age (13–16), we apply that age in the relevant jurisdiction.

14. Automated decision-making

We do not make decisions producing legal or similarly significant effects on you based solely on automated processing.

15. Regional supplements

15.1 EEA / UK supplement (GDPR / UK GDPR)

Operator: 0xposed (worldwide informal initiative — no incorporated entity at this stage)

EU/UK Representative (Art. 27): to be appointed upon formal incorporation; until then, contact us at contact@0xposed.io

Data Protection Officer: not appointed at this stage; contact contact@0xposed.io for any privacy matter

Supervisory authorities: you may complain to the data-protection authority in your EU Member State of habitual residence; in the UK, the Information Commissioner's Office (ico.org.uk).

15.2 California (CCPA / CPRA) supplement

Categories of personal information collected in the past 12 months, sources, business/commercial purposes, and categories of recipients: see §4 and §8 of this Policy, which constitute our "notice at collection".

We do not sell or share personal information for cross-context behavioural advertising, and we have not done so in the preceding 12 months. We do not have actual knowledge of selling or sharing personal information of consumers under 16.

Sensitive personal information: we collect and process financial-related information and content of communications you submit to us as part of a case intake. We only use this sensitive personal information to perform the services you request, comply with the law, and protect security — we do not use it for purposes triggering the "Right to Limit" under the CPRA.

California rights: right to know, delete, correct, limit use of sensitive personal information, opt out of sale/sharing (we do not sell or share), and non-discrimination. Submit requests to contact@0xposed.io. An authorised agent may submit a request on your behalf.

15.3 Brazil (LGPD) supplement

We will provide, in Portuguese, the information required by ANPD Resolution CD/ANPD No. 19/2024 on international data transfers (form, duration, purpose, recipient countries, data-subject rights, complaints channel). Brazilian data subjects may request a copy of any SCC we use, in full, within 15 days, by writing to contact@0xposed.io.

15.4 China (PIPL) supplement

Cross-border transfers of data subjects in mainland China occur only where lawful (CAC Standard Contract, security assessment, or certification, as applicable) and with the data subject's separate consent where required.

15.5 Canada (PIPEDA) and Australia (Privacy Act 1988) supplements

We process personal information in line with PIPEDA principles and the Australian Privacy Principles, including reasonable security safeguards and openness about practices. Canadian residents may complain to the Office of the Privacy Commissioner of Canada; Australian residents to the Office of the Australian Information Commissioner.

16. Changes to this Policy

We may update this Policy, in particular when 0xposed transitions from an informal initiative to a formal legal entity (whether a DAO, a foundation, a company, or another structure). The effective date at the top will change accordingly. Where the change is material, we will notify users with an active account by email and via a prominent banner on the Platform.

17. Complaints

If you believe we have not handled your data properly, please contact us first at contact@0xposed.io. You also have the right to complain to your local data-protection authority.

This Privacy Policy was last updated on the effective date shown above. It must be reviewed by qualified legal counsel before publication. 0xposed will revise this Policy when a formal legal entity is constituted and as soon as a designated EU/UK Representative is appointed (where required by Art. 27 GDPR/UK GDPR).