



Privacy Policy

Status: approved. **Version:** 0.1.9.

0. What this covers

This describes what Foreshock collects when you use the Service (the public site, monitoring product, and forensics product), how it's used, and what you can do about it.

Foreshock is the controller of the personal data described in this policy. Foreshock is the trading name under which the Service is operated (Terms of Service, clause 1.1, at

<https://foreshock.tech/legal/terms>).

Contact for any question about this policy or about your personal data, including data-protection requests: contact@foreshock.tech.

1. Information we collect

- **Account information:** email, name, and password (stored as a salted hash, never in plain text), if you sign up for monitoring or submit an authenticated forensics request. In Settings, you may optionally add your organization and a role (e.g., individual investor, analyst, fund manager) - both are optional and never required to use the Service.
- **Sign-in with Google or Apple (only if you use it):** if you choose to sign in with Google or Apple instead of setting a password, that provider sends us your name, email address and profile picture, an identifier for your account with them, and the tokens needed to complete the sign-in. We never receive your password for that account, and we cannot read or post anything else in it. If you use Apple's Hide My Email, we receive Apple's relay address rather than your own and everything works the same way. Signing in this way is optional - email and password remains available - and an account created this way holds no password at all.
- **Portfolio data:** the protocols you add to your watchlist, and optional position sizes you choose to record.
- **Contact and coverage-check submissions:** whatever you enter on <https://foreshock.tech/contact> - your email, message, and (for protocol-check requests) the protocol you're asking about.
- **Forensic request details:** the exploit contract address, transaction hash(es), your policy text if you submit one, and your contact details (name and email, if you submit anonymously without an account) or your account identity (if submitted from <https://foreshock.tech/app/reports>).
- **Alert and billing history:** which alerts fired for you, and subscription/payment status. Where you pay by card, the card details themselves are handled entirely by the payment processor named at checkout - Foreshock never sees or stores your card number.
- **Cryptocurrency payment details (only if you pay that way):** the blockchain network you chose, the transaction hash you give us, and the wallet address that sent the payment, which we read from the public transaction rather than asking you for it. We keep these to confirm the payment, to answer a later question about it, and to have somewhere to send a refund. A wallet address and a transaction hash are public on the blockchain to anyone who looks; what is personal here is that we hold them next to your account, and that is the part this bullet is disclosing.
- **Basic usage data:** standard server logs (IP address, request timestamps) generated by normal web traffic. We run no analytics, no advertising and no cross-site tracking. Our hosting platform counts page views without cookies or cross-site identifiers, and nothing it counts is linked to your account.

2. How we use it

- To provide the Service: render your watchlist and alerts, process your subscription, generate and deliver your forensic report.
- To notify you: alert emails, forensic status/quote/delivery emails, billing notifications.
- Internally, to improve Foreshock: contact submissions, coverage-check requests, and forensic requests are also recorded as internal signals. This is Foreshock's own internal product-feedback process, not sharing your data with any outside party.

We do not sell your personal information.

3. Third parties

Providing the Service necessarily involves a small number of third parties:

- **A payment processor, where you pay by card** - payment processing for subscriptions and forensic-engagement charges, as merchant of record. The processor is named on the checkout page before you pay. It receives what's needed to process payment; Foreshock does not receive or store your card details. Because a merchant of record is the seller, it is an independent controller of the payment data it collects, and its own privacy policy applies to that processing alongside this one.
- **No processor at all, where you pay in cryptocurrency** - a direct payment involves no third party. We read the transaction you name from public blockchain nodes to confirm it, which is a public lookup of public data; nothing about you is sent to anyone.
- **Google and Apple** - identity providers, used only if you choose to sign in with one of them. They tell us that the sign-in succeeded and pass the profile fields listed in §1; we send them nothing about you beyond what completing that sign-in requires, and we do not use them for analytics or advertising.
- **Resend** - sends transactional email (verification, password reset, alerts, forensic status updates).
- **Our hosting and database providers** - they run the Service and store what section 1 lists, on our instructions and for no purpose of their own.
- **Public blockchain infrastructure** - when you submit a forensics request, the exploit contract address and transaction hash(es) you provide are looked up against public blockchain nodes and DeFiLlama's public pricing API, in order to independently verify the transaction and calculate loss. These are public blockchain queries by nature (the same data anyone could look up given the same address/hash) and don't include your policy text, contact details, or any other information you submit.

We don't share your policy text, contact details, or account information with any of the above beyond what's listed here.

4. Data retention and deletion

You can delete your account at any time from

<https://foreshock.tech/app/settings>.

This removes your account (including any optional profile fields you added, such as organization or role), watchlist, subscription record, and any forensic requests linked to your account.

Internal signal records derived from your contact or forensic submissions (see §2) are retained without a link to your identifying account information after deletion - they inform product decisions in aggregate but no longer point back to you specifically.

Anonymous forensic requests (submitted without an account) are retained as part of the engagement record for as long as reasonably needed for the engagement and its own recordkeeping requirements (see the Forensic Engagement Terms), since they may be relevant evidence in a later dispute over the report's findings.

5. Your rights

You can access, correct, or delete your account information directly from

<https://foreshock.tech/app/settings>.

For anything not self-serviceable there (e.g., a question about an anonymous forensic request, or a data question not covered above), contact us at contact@foreshock.tech.

6. Cookies

The Service uses a small number of functional cookies necessary to keep you signed in and to support the sign-in flow itself (e.g., remembering where to return you to after you sign in). We don't use advertising or cross-site tracking cookies. We run no analytics and no cross-site tracking. Our hosting platform counts page views, setting no cookie and collecting no personal data.

7. Children

The Service isn't directed at, or intended for use by, anyone under 18.

8. Changes to this policy

We may update this policy as the Service changes. Material changes will be reflected here with an updated version number.

9. Contact

Questions about this policy: contact@foreshock.tech, or via

<https://foreshock.tech/contact>.