

Privacy Policy

Robert E Holden dba EAWF.com, hereinafter referred to as EAWF.

Rancho Cordova, California, United States

Contact: support@eawf.com

Version 1.0 | Policy approved: October 12, 2026 | Revision: October 13, 2026

Your privacy is a fundamental responsibility at EAWF. Personal information must be collected only for a necessary, defined purpose, protected against unauthorized access, and kept no longer than justified. Convenience, curiosity, or commercial opportunity is not a justification for collecting or disclosing your information.

1. Scope and data minimization

This policy applies exclusively to EAWF.com, its accounts, and its handling of personal information. EAWF collects and retains personal information only when specifically necessary for a defined system or business function, or a legal obligation. Each data category must have a justified purpose and retention rule.

2. Information and purposes

Account processing is limited to usernames, account status, access levels, and necessary profile details such as name, telephone number, and postal address. Authentication records include password hashes, login events and, when enabled, authenticator and security-key records. Communications and transaction records are limited to what is necessary to answer requests, provide services, substantiate transactions, and meet legal obligations. Security evidence is used to detect, investigate, and prevent abuse.

3. Public access and account age

People of all ages may browse the public website. Account holders must be at least 18. Browsing may generate operational cookie data and analytics. Parents or guardians can contact support about a child's information. EAWF must enforce account-age restrictions and assess analytics collection involving child visitors before enabling affected features.

4. Cookies, analytics and browser choices

EAWF uses operational cookies for consistent page behavior and session-based access. Blocking these cookies may prevent account features from working. Browser settings let you manage or delete cookies.

EAWF presently uses Statcounter for general page counts. Depending on project settings, Statcounter can process page URLs, referring links, timestamps, IP addresses, browser/device information, and cookies distinguishing visits. This third-party analytics processing is separate from EAWF account information. Statcounter settings and retained information must be limited to the documented analytics purpose and reviewed against this policy. Its independently held information follows its own policies and settings.

Statcounter provides privacy and cookie information and an analytics-cookie refusal option through the links below. Refusing cookies does not necessarily stop page counting. EAWF does not currently represent that its website responds to Do Not Track signals or Global Privacy Control. Legally required preference-signal handling must be implemented before any affected processing is enabled.

[Statcounter privacy information](#)

[Statcounter cookie information](#)

[Statcounter analytics-cookie refusal](#)

5. Security and authorized access

EAWF requires encryption of stored account personal information and TOTP/Google Authenticator shared secrets, and secure hashing of passwords and recovery codes. WebAuthn security keys retain their private keys on the user's device; EAWF stores public-key credentials and necessary metadata. Critical data must be stored outside the public website on protected private infrastructure, with access restricted to authorized EAWF operations. Payment signing must be isolated from the public application. Corresponding controls must be verified before affected services are enabled. No system can guarantee absolute security.

Security logs may contain source IP, timestamp, endpoint, event category, outcome, and selected metadata needed for investigation. Credentials, tokens, session cookies, private keys, recovery codes and unnecessary personal information must be redacted. Security evidence is separate from visitor analytics and must not be used for advertising or profiling. An IP address or suspicious event is not proof of a person's identity or wrongdoing.

6. Disclosure and legal requests

EAWF prohibits voluntary disclosure of account information for unrelated purposes or advertising. Statcounter's visit-data processing is described above. Any additional outside provider receiving personal information must be assessed and disclosed before use. External links, including eBay, lead to independently operated services with their own practices.

EAWF reviews legal requests for authenticity, authority, scope and applicable law. The normal mechanism is a limited export for a specifically identified account, rather than general database access. Broad demands require legal review and efforts to narrow or challenge them where appropriate. Binding legal process may require broader disclosure; not all demands require a warrant. Users are notified when legally permitted. Lawful preservation obligations can temporarily suspend deletion of covered records.

7. Retention requirements

The following approved schedule governs EAWF records. All periods are subject to applicable legal, regulatory, contractual and preservation requirements. Implementation must enforce the correct category-specific rule; a hosting-data deadline does not erase separately retained business records. Statcounter's independently held analytics information requires separate configuration and retention review.

Record category	Approved retention rule
Account personal information	Account lifetime, then deletion, subject to separately retained necessary business records and narrowly applicable incident or legal holds.
Non-identifying aggregate page counts	Retain for long-term comparisons without identifying details.
Terminated hosting files and mailboxes	30 calendar days after the effective termination date.
Final website archives, requested email exports and download access	30 calendar days after the effective termination date. Required backup preparation and verification must be complete before hosting data is deleted. Failed exports: contact EAWF support.
Invoices and payment records	7 years.
Agreements and accepted Terms	7 years after termination.
Rejected applications	1 year after rejection.
Support tickets	3 years after closure; open tickets are not deleted solely because hosting ended.

Record category	Approved retention rule
Security and access logs	90 days; incident records under an applicable investigation or preservation hold remain until release.
Backup download audit logs	1 year.
Routine disaster-recovery backups	Existing backup rotation schedule. Historical sets are not selectively rewritten unless legally required. Restored data must be reconciled with current deletion and termination records before service access.
Privacy-related records	Only as long as required by applicable law or a documented legitimate business purpose.

8. Account deletion, backups and transaction records

EAWF requires permanent deletion of account personal information and authentication records, subject to necessary accounting, contractual, incident and legal-preservation exceptions. Until permanent self-service deletion is available, direct deletion requests to support@eawf.com. Deactivation alone does not fulfill a deletion request. A completion log records the deletion event without retaining the deleted account identity or values; separately required business and legal-hold records follow their own schedules.

Historical disaster-recovery backups may retain deleted information until they expire under the existing rotation. EAWF must prevent deleted or terminated account data from being restored into accessible services without reconciliation and appropriate authorization. A restricted restore-suppression record may be retained only as necessary for this purpose. Legal holds must be limited in scope and resume ordinary retention processing when released.

For EAWF's own products and services, approved payment methods are Bitcoin and U.S. dollar cash. Necessary transaction records may include the business purpose, counterparty information required for accounting, amount, date, valuation, payment reference and confirmation. Bitcoin valuations use a recorded Bitstamp reference price and timestamp. EAWF does not offer custody or transmission of customer funds. Bitcoin on-chain records are public and cannot be erased by EAWF.

9. Privacy requests and choices

Contact support@eawf.com to request access, correction or deletion, or raise a privacy concern. Available account features also let you review and update your profile. Identity verification must be proportionate; do not send passwords, authentication secrets or unnecessary identity documents through ordinary email.

Applicable privacy rights, exceptions and response deadlines depend on the governing law. Requests affecting legally retained records require review. EAWF must maintain appropriate request procedures and provide jurisdiction-specific notices where required before enabling affected processing.

10. Policy changes and contact

Material changes will be described in an updated policy with a revision date. Additional notice or consent required by law must be provided. Policy updates do not themselves authorize new uses of personal information. Version history is preserved in source control.

For questions or privacy requests, contact EAWF at support@eawf.com. EAWF is based in Rancho Cordova, California, United States.