

Security

Where zeepler runs, what it keeps, and who can reach it. Every statement on this page is traced to its code or live configuration.

Last reviewed 2026-10-20

Where zeepler runs

zeepler runs on Amazon Web Services in the United States (us-east-1).

It is operated by Bates Solutions Inc., a British Columbia company.

Your label data

A label request is used to generate the label and is then discarded. zeepler does not store request bodies and does not write them to its logs.

Kept per label generated	Account id, time, endpoint, response time, number of labels. A refused request leaves no record.
Never kept	The label's data or layout
Deleted after	365 days

Encryption

- In transit: HTTPS only. The website requires TLS 1.2 or later and redirects plain HTTP. The API accepts TLS 1.2 or later.
- At rest: every database table is encrypted by AWS. Secrets, such as the payment processor's credentials, are held in AWS Systems Manager as encrypted parameters.

API keys

An API key is shown to you once, when it is created. zeepler stores only a SHA-256 hash of it, plus its last four characters so you can tell your keys apart. A lost key cannot be recovered, only replaced.

Accounts and passwords

Sign-in is handled by Amazon Cognito using the Secure Remote Password protocol, so your password is never sent to zeepler's servers. Passwords must be at least 8 characters, with upper-case, lower-case and a number. Multi-factor authentication is not available yet.

Who can access production

- The deployment pipeline (GitHub Actions) holds no stored key: it signs in with OpenID Connect and gets a session that expires within an hour.
- Backend functions run under roles scoped to their job. Billing, payment webhooks, sign-up screening, the waitlist, administration and the health check each have their own; the rest share one. The public label endpoint can look up a single account by its key, but it cannot list accounts and cannot reach the payment processor's credentials.
- One person, the operator, has account-level access. The operator holds two long-lived access keys: an administrator key, and one whose only permission is to take on a role that can deploy, in sessions that expire.

Backups and logs

The account, client, usage, billing and waitlist tables have point-in-time recovery: they can be restored to any point in the last 35 days.

Operational logs are kept for 365 days. They contain account ids and payment-processor customer ids, and no label content. Website access logs are also kept for 365 days: for each request, the address requested with its query string, the time, the status, the browser, the referring page and the visitor's IP address.

Until September 2026 the sign-up and password pages put the visitor's email address in the page address, so access logs from before then contain email addresses. They expire by September 2027.

Reporting a security problem

Email info@zeepler.com. You will get a reply within 2 business days.