



BioLog — Privacy Policy

Published by Terrastation SBC, a Minnesota specific benefit corporation · Last updated: October 16, 2026 · Version 1.6

This Privacy Policy explains how Terrastation SBC ("Terrastation," "we," "us"), a Minnesota specific benefit corporation, collects, uses, shares, and protects personal information in connection with the BioLog mobile application and related websites (the "Service"). Protecting privacy — especially the privacy of younger users — is central to our public-benefit mission. We aim to collect only what the Service needs, and we do not sell your personal information.

We apply a high global standard, drawing on the EU/UK General Data Protection Regulation (GDPR) and U.S. state privacy laws, to all users regardless of where they live.

1. Ages we serve and children's privacy

BioLog is intended for users who are at least 13 years old. Before an account can be created, the app checks an age-eligibility signal associated with your device's app-store account. An account is created only if that signal affirmatively indicates you are 13 or older. If it does not — including where you decline to share it or the check cannot be completed — the sign-up screen is not shown, no account is created, and no information is collected.

If you are between 13 and the age of majority where you live, you may use the Service only with the permission and supervision of a parent or legal guardian, who agrees to our Terms on your behalf. We do not permit accounts for children under 13 and do not knowingly collect their personal information. If we learn that a child under 13 has created an account, we will delete the account and its data. A parent or guardian may contact us at the address below with any question about a child's use of the Service.

2. Information we collect

Account information

When you create an account we collect your email address, display name, and chosen @handle. Authentication is handled by our identity provider (Supabase Auth).

Passkeys

If you add a passkey, your device creates it and keeps its private key; your fingerprint, face or other screen-lock data never leaves your device, and we never receive it. Our identity provider stores the passkey's public key and credential ID, an identifier for the kind of authenticator that created it, whether it is backed up (for example to your password manager), a counter that helps detect a copied passkey, a name, and when it was added and last used. You can remove a passkey at any time in the app, and your password keeps working.

Age eligibility

We check your age eligibility at sign-up using the age signal associated with your app-store account. We do not collect or store your date of birth or age. We store only whether your account may use the community features and AI species identification, as derived from that signal. The app also uses the signal on your device, without storing it, so that new sightings by users under 18 start as private.

Sightings and content you create

When you log a sighting we store the species names, your field notes, any photos you add, the sighting's location (GPS coordinates, and where available elevation and accuracy), and timestamps. If you choose a photo from your device's library, we read the date and location recorded in that photo, if it has them, to fill in the sighting. You may save named places. You choose for each sighting whether it is private (visible only to you) or public (shared to the community).

AI species identification

If you use AI species identification, the app first asks for your permission, and you can withdraw it at any time in Settings. We then send the photograph together with an approximate location for the sighting (rounded to about 1 kilometer), its elevation rounded to the nearest 50 meters, the month and year it was observed, and the category and names you entered, to our AI provider, Anthropic, PBC, which returns identification suggestions. Anthropic generally deletes the inputs and outputs of this processing within 30 days. Content that Anthropic's systems flag for policy review may be retained for up to two years, and related safety-classification scores for up to seven years. Anthropic is contractually prohibited from using this content to train its models.

If you accept a suggestion, the app saves two things it suggested with the sighting: the species' classification (kingdom, phylum, class, order, family, and genus, where the AI is confident of them) and a short description of the species' typical habitat. The classification describes the species, not you, and is shown wherever the sighting is visible, including on public sightings. The habitat description is shown only to you and your connections, like your field notes.

Profile pictures

Your profile picture is one you choose to upload. If you have not uploaded one, the app draws your initials on your device; no third-party avatar service is used.

Diagnostic and crash data

We use error logging (Sentry) to capture crashes and errors so we can fix them, retained for up to 90 days. This data does not include IP addresses, email addresses, or names. Error reports from our servers may include an internal account identifier, and error reports from the app may include technical details of recent requests, such as which part of our service was called. Reporting is disabled entirely in our development environment.

Cookies and browser storage

When you sign in to our website at app.biolog.live, it sets one cookie that keeps you signed in. The cookie holds your sign-in tokens, account ID, and email address; it cannot be read by scripts on the page, is sent only to app.biolog.live, and is removed when you sign out or after 14 days. It is strictly necessary for the website to work. Preferences you choose in the website's Settings, such as appearance and distance units, are saved only in your browser and are not sent to us. We do not use cookies or browser storage for advertising or analytics.

Information we do not collect

We do not serve advertising and do not collect advertising identifiers. We do not sell or "share" (as defined under U.S. state privacy laws) your personal information for cross-context behavioral advertising.

3. How we use your information

- Provide the Service: store your sightings, sync across devices, and power the map and nearby-sightings features.
- Provide AI species identification when you request it.
- Operate the community features you opt into (public sightings and connections).
- Enable safety and moderation: process reports and blocks, and enforce our Terms.
- Communicate with you: transactional email such as verification and password reset.
- Maintain reliability, protect the Service, and comply with law.

4. Legal bases for processing

- Performance of a contract — to provide your account and the core features you request.
- Consent — for device permissions (camera and location), for AI identification, and for making content public; you may withdraw consent at any time.

- Legitimate interests — to secure the Service, prevent abuse, and improve reliability.
 - Legal obligation — to comply with applicable law, including child-safety reporting.
-

5. How your information is shared

We do not sell your personal information. We share information only as follows:

- With other users, at your direction — your public sightings and public profile are visible to the community and your connections. Public sightings never expose your email address. Other users see a public sighting's location rounded to about 1 kilometer; users you have accepted as connections see its exact location and your notes.
 - With service providers under contract — Supabase (database, storage, authentication), Render (API hosting), Cloudflare (hosting for our website at app.biolog.live, which receives your IP address and the requests you make there, and an approximate country and time zone derived from them that the website uses to show dates and local help resources), Resend (delivery of account emails, such as verification and password reset), Sentry (crash reporting), Anthropic, PBC (AI species identification, which receives the photograph and the approximate location, elevation, and month and year of the sighting), Apple (App Store / TestFlight, the age-eligibility signal, and maps and place search, which receive the text you search for and the map location), and Google (Google Play and its age-eligibility signal, for BioLog for Android). Each processes data on our behalf under data-processing terms.
 - With map services in BioLog for Android — Google, which provides place search through your device and receives the text you search for and the map location, and OpenFreeMap, which provides the map images and receives your device's IP address and the map area shown. They receive this information under their own terms.
 - For legal and safety reasons — to comply with law and lawful requests, enforce our Terms, and protect users and the public, including reporting apparent child sexual abuse material as described below.
 - In a business transfer — in a merger, acquisition, or asset sale, subject to this policy.
-

6. Content scanning and child-safety reporting

We may scan content, including public photos, to detect illegal material and violations of our Terms. If we detect apparent child sexual abuse material, we will preserve it as required and report it to the National Center for Missing & Exploited Children (NCMEC) and, as appropriate, to law enforcement, consistent with applicable law.

7. Location data

Location is collected only while you are logging a sighting or viewing the map, and only after you grant permission, which you can revoke at any time in your device settings. If you are under 18, new sightings start as private. Otherwise a new sighting starts with the setting you chose for your last one, and your first starts as private. You can change a sighting between public and private before saving it and at any time afterwards. When a sighting is public, other users see its location rounded to about 1 kilometer; users you have accepted as connections see its exact location. When you use AI identification, an approximate location is also sent to our AI provider as described above. Because publishing location can be sensitive for you and for protected species, consider keeping sightings of sensitive species private.

8. Data retention

When you delete your account through the in-app deletion option, we immediately and permanently delete your live data — your account, sightings, saved places, authentication identity (including any passkeys), stored photos, and avatar — with no soft-delete or deactivation delay. Residual copies age out of backups as follows:

- Database backups (application and identity data) — retained for 7 days on a rolling basis, as nightly backups.
- Photo storage backups — retained for 30 days under an immutable object lock that prevents early deletion (including by a compromised key).
- Crash and diagnostic data (no IP addresses, email addresses, or names) — retained for up to 90 days.

For safety and moderation, we keep reports, including a copy of the reported content and the handles of the accounts involved, for as long as needed to handle the report, keep the Service safe, and meet legal obligations. Reports may be kept after the accounts involved are deleted.

9. Your privacy rights and choices

You can edit or delete your sightings, switch them between private and public, manage connections, update your profile, and delete your entire account at any time in the app.

Subject to applicable law, you may have rights to access, rectify, erase, restrict, or object to processing; to data portability; to withdraw consent; and to lodge a complaint with a supervisory authority. U.S. state residents may have rights to know, access, correct, delete, and obtain a portable copy of personal information, and to opt out of sale or targeted-advertising “sharing” (which we do not do). We will not discriminate against you for exercising these rights and, where required, will provide an appeal. To make a request, contact support@terrastation.io.

10. International data transfers

Our providers, including our AI provider, may process data in the United States and other countries. Where we transfer personal information out of the EEA, the UK, or Switzerland, we rely on an appropriate mechanism such as the Standard Contractual Clauses and the UK Addendum, with supplementary measures where needed.

11. Security

Access tokens are stored in the device keychain on iPhone, encrypted with a key held by the Android Keystore on Android, and in the secure sign-in cookie described in section 2 on our website, and API traffic uses HTTPS. A passkey is checked with public-key cryptography, so we never hold the key that signs you in. Photo backups are held under an immutable object lock. Photos are stored at long, randomly generated web addresses that are not listed or searchable; anyone who has a photo's address can view it, including a photo on a private sighting. We take reasonable measures to protect your information however no system is perfectly secure.

12. Changes and contact

We may update this policy; material changes will be posted here with a new “last updated” date and, where appropriate, additional in-app notice.

Terrastation SBC

Email: support@terrastation.io