Privacy Policy

Last updated: 17/03/2026 · Effective for all Is Everyone Safe mobile and web experiences.

Download PDF

1. Who we are and how to reach us

Is Everyone Safe Limited (company number **15261287**) provides crisis-alert coordination tools across the web, iOS, and Android. We are the data controller for personal data processed through the platform. Contact our privacy team at **dataprotection@iseveryonesafe.com** or in writing at Is Everyone Safe Limited, 8 Mercia Business Village, Torwood Close, Westwood Business Park, Coventry, CV4 8HX, United Kingdom.

If your employer, school, local authority, or another organisation creates or administers your account, that organisation may also act as a controller for the personal data it decides to upload, manage, or review in the platform. In those cases, you should also read that organisation's own privacy information.

2. Data we collect

The exact data collected depends on the features you use, the permissions you grant, and whether you are a community or enterprise customer. We only collect data necessary to deliver the requested service.

Identity & contact details

Data examples: Name and display name, Email addresses provided (personal and organisational), Phone number (optional), Organisation or site details provided when an account is created for you

Why we collect it: Account creation, cohort membership, administrator controls, and support communications.

Legal basis: Performance of a contract; legitimate interests in operating the service.

Account & safety activity

Data examples: Organisation or cohort membership, roles, and permissions, Alert history, responses, escalation actions, and audit timestamps, Notification preferences, device tokens, and Flic button metadata

Why we collect it: Deliver emergency alerts, demonstrate audit history, enforce acceptable use, and provide diagnostics.

Legal basis: Performance of a contract; vital interests; legitimate interests in safeguarding our users.

Location & device information

Data examples: Foreground and background location (only when granted), Bluetooth and device identifiers related to personal safety buttons, App diagnostics, crash logs, analytics, and website usage telemetry (Expo, Supabase, Firebase, Vercel)

Why we collect it: Deliver proximity-based alerts, confirm notification delivery, detect and remediate crashes or abuse.

Legal basis: Explicit consent (location/background Bluetooth); legitimate interests in securing the platform.

Support & compliance data

Data examples: Support tickets, Abuse reports, Regulatory correspondence

Why we collect it: Respond to requests, fulfil legal obligations, and maintain records for regulators and law enforcement when required.

Legal basis: Legal obligation; legitimate interests in defending legal claims.

3. How we use your information

- Provide, customise, and maintain the safety platform, including personal safety button onboarding.
- Deliver push notifications, in-app alerts, and SMS/email escalations requested by your organisation.
- Operate Bluetooth/Flic integrations so button presses work in the background when you enable alerts.
- Monitor for abuse, fraud, or misuse and enforce our Terms and Acceptable Use Policy.
- Comply with legal obligations, respond to lawful requests, and maintain disaster-recovery records.

4. Where we get your information from

- Directly from you when you create an account, complete profile fields, contact support, or use the app and website.
- From the organisation, administrator, or responder group that invites you, provisions your account, or assigns you to a cohort.
- From your device, operating system, push-notification provider, and connected peripherals such as personal safety buttons when you enable those features.
- From our processors and infrastructure logs when they help us detect incidents, fraud, misuse, or service failures.

5. Sharing and international transfers

We do not sell personal data. We share it only with processors that help us deliver the service or when legally required. Where data leaves the UK/EEA, we rely on UK adequacy decisions, Standard Contractual Clauses, or equivalent safeguards.

You can request more information about the safeguards we use for restricted transfers by emailing dataprotection@iseveryonesafe.com.

- **Supabase (PostgreSQL, authentication, storage) – EU/UK regions:** Primary application database, authentication, and edge functions.
- **Expo & Apple/Google push notification services:** Delivery of device notifications and dev-client diagnostics.
- **Flic / Shortcut Labs SDK:** Bluetooth integration for personal safety buttons, including encrypted button IDs.
- **Payment or billing processors (only for licensed customers):** Subscription and invoice management.

6. Retention

We retain account and alert data while you maintain an active profile and for up to 12 months afterward to support regulatory enquiries and incident reviews. Aggregated analytics may be retained longer in anonymised form. You can request deletion sooner, and we will honour it unless law enforcement, litigation holds, or contractual obligations require us to keep certain records.

7. Your rights and choices

- Access: request a copy of the personal data we hold about you.
- Rectification: update inaccurate or incomplete details from inside the app or by contacting us.
- Erasure: delete your account via the in-app settings or by emailing us; we remove data unless retention is required by law.
- Restriction and objection: limit or object to processing carried out on legitimate-interest grounds.
- Data portability: request export of the personal data you provided to us in a structured format.
- Consent withdrawal: revoke consent for background location, Bluetooth, or marketing at any time in device settings.
- Complaint: lodge a complaint with the UK Information Commissioner's Office (ICO) or your local supervisory authority.

Exercise these rights from the profile/settings screens or by emailing **dataprotection@iseveryonesafe.com**. If we cannot resolve your concern, you may contact the Information Commissioner's Office at **ico.org.uk/make-a-complaint**.

8. When information is required and what happens if you do not provide it

- Core account and contact details are required to create and operate an account, verify access, send alerts, and administer your organisation's workspace.
- If you do not provide required account data, we may be unable to create your account, deliver alerts, or provide support.
- Background location, Bluetooth, notifications, and certain device permissions are optional, but disabling them may prevent core safety features from working as intended.

9. Automated decision-making

We do not currently use solely automated decision-making or profiling that produces legal effects or similarly significant effects about you. We do use rules and automation to route alerts, trigger notifications, and manage operational workflows, but those processes support the service rather than replace human judgement about your rights or status.

10. Account deletion & push/bt permissions

You can delete your account any time from Settings > Account > Delete Account in the mobile app or by emailing **superadmin@iseveryonesafe.com** from the registered email. Device-level permissions for location, Bluetooth background monitoring, and notifications can be changed via system settings. Disabling these features may limit the functionality of safety alerts.

11. Children’s privacy

Our services are designed for adults and authorised corporate responders. We do not intentionally collect data from children under 16. If you believe a child has provided information, contact us so we can delete it.

12. Security

We implement defence-in-depth controls including encryption at rest and in transit, least-privilege access, logging, and automated alerting. Despite our efforts, no system is perfectly secure, and we encourage you to use strong passwords, device biometrics, and promptly install software updates.

13. Changes to this policy

We update this policy when our practices change or to reflect legal requirements. Material changes will be communicated via in-app notice or email. Continued use after the effective date constitutes acceptance of the updated terms.