Data Safety Summary – EterGam Reporter LIVE

Last updated: December 31, 2025

Data collected

The following data is collected and processed to provide the core functionality of the App:

- Pseudonymous user ID (unik_id): Used for subscription management, free trial enforcement, fraud prevention, and abuse mitigation. It does not directly identify the user.
- Reported spam/scam numbers: Submitted voluntarily by users to improve country-based spam detection.
- Technical logs: Limited logs such as IP address, timestamp, and request metadata, retained temporarily for security, diagnostics, and abuse prevention.

Data not collected but accessed locally on the device

The App accesses certain device data strictly locally. This data is never uploaded, stored on servers, or shared with third parties:

- Contacts: Used only to prevent known contacts from being flagged as spam.
- Call logs: Used only for local spam detection logic during incoming calls.
- Notification metadata: Used solely to detect incoming calls. Notification content is not read, interpreted, or stored beyond what is strictly necessary to detect incoming call events.

Data sharing

EterGam does not sell or share user data with third parties for their own purposes. Data is processed only by infrastructure providers acting as processors under strict data processing agreements and confidentiality obligations.

Encryption and security

All communication between the App and EterGam servers is encrypted using HTTPS/TLS. Appropriate technical and organizational measures are applied to protect data against unauthorized access or misuse.

User controls and rights

Users can manage or revoke Android permissions at any time via system settings. Users may request deletion of their pseudonymous data (unik_id, reports, subscription references) by contacting support@etergam.com.

Purpose of processing

Data is processed strictly for spam and scam detection, core application functionality, subscription management, fraud prevention, and infrastructure security.

Sensitive permissions justification

READ_CALL_LOG: Required to detect incoming calls and perform local spam and scam matching. Call log data is accessed only on the device and is never uploaded or stored on servers.

READ_CONTACTS: Required to prevent known contacts from being incorrectly flagged as spam or scam calls. Contacts are accessed locally and are never transmitted or shared.

Notification Listener: Required to reliably detect incoming calls on supported Android versions where direct call information is not always available. Notification content is not read, interpreted, or stored beyond what is strictly necessary to detect incoming call events.

Overlay (Draw over other apps): Required to display real-time warning alerts during incoming calls, allowing users to make informed decisions before answering. Overlay content is generated locally and does not collect or transmit data.