

Privacy Policy for Daily Signal

Effective date: 10 July 2026

Developer: Gobeond

Contact: contact@gobeond.com

1. Overview

This Privacy Policy explains how Daily Signal ("the App"), developed by Gobeond ("we", "our" or "us"), accesses, uses, stores and discloses information. Daily Signal monitors movement of the Android device on which it is installed and can send inactivity alerts and scheduled check-in emails to recipients selected by the user.

This policy applies to the self-hosted release of Daily Signal, in which email is sent directly from the user's device through an SMTP email account configured by the user.

2. Information the App accesses or stores

2.1 Motion and activity information

The App accesses motion-sensor readings available on the device to detect movement. Sensor processing occurs locally on the device. The App may store activity events, motion counts, timestamps and the time of the most recent detected movement so that it can determine when an inactivity alert is due.

The App does not use motion information to determine the user's precise location, and the self-hosted release does not transmit raw motion-sensor readings to Gobeond.

2.2 Email and recipient information

To send notifications, the user may provide:

- one or more recipient email addresses;
- an SMTP server hostname and port;
- an SMTP username and sender address;
- an SMTP app password or other SMTP credential; and
- a preference indicating whether TLS should be used.

Recipient addresses and SMTP configuration are used only to send emails requested or scheduled by the user. SMTP usernames, sender addresses and passwords are stored in encrypted preferences protected using Android security components. Other configuration values, including recipient addresses and SMTP host settings, are stored in the App's private application storage.

2.3 Device and app information

The App may access or record limited technical information needed for operation and troubleshooting, including the device manufacturer and model, Android version and API level, App version, battery state, sensor name, whether monitoring is enabled, and a user-defined device label.

The App also creates a locally generated random device identifier. This identifier is used within the App and, in the self-hosted release, is not provided to Gobeond.

2.4 Diagnostic logs

The App keeps rolling diagnostic logs in its private storage. These logs may include timestamps, motion events or counts, scheduling events, email-send status, alert status, battery information, device and App version information, and the user-defined device label.

Diagnostic logs remain on the device unless the user explicitly exports, shares or attaches them to an email. A diagnostic export may therefore be disclosed to the person or service selected by the user.

3. How information is used

The App uses the information described above to:

- detect device movement and maintain a record of recent activity;
- schedule and send inactivity alerts and daily check-in emails;
- send manual test emails requested by the user;
- restore monitoring and schedules after device restart;
- display status and diagnostic information in the App; and
- identify faults and improve compatibility and reliability.

We do not use App information for advertising, behavioural profiling, marketing, sale of personal information, or cross-app tracking.

4. How email data is transmitted

When the App sends an email, the message, recipient addresses, sender address and any attachment selected by the user are transmitted directly from the device to the SMTP service configured by the user. The transmission and subsequent processing of that email are subject to the terms and privacy practices of the user's email provider and the recipient's email provider.

If TLS is enabled and supported by the configured SMTP service, the App requests an encrypted connection. The user is responsible for selecting a trustworthy SMTP provider, using valid credentials and configuring the connection securely.

5. Sharing and disclosure

Gobeond does not sell, rent or trade personal information handled by the self-hosted release of Daily Signal.

Information may be disclosed in the following limited circumstances:

- to email recipients and email service providers when the App sends an email configured by the user;
- to a person or service selected by the user when the user exports or shares diagnostic information;
- where disclosure is required by applicable law, regulation, court order or lawful governmental request; or
- where reasonably necessary to protect legal rights, safety or the integrity of the App.

6. Data storage, security and retention

App settings, activity records and diagnostic logs are stored in the App's private storage on the Android device. Sensitive SMTP credentials are stored using encrypted Android preferences backed by Android's cryptographic key-management facilities.

Information is generally retained until it is replaced by newer information, cleared by the user, removed through Android settings, or deleted when the App is uninstalled. Rolling diagnostic logs are limited by the App's log-management process rather than being kept indefinitely.

No method of electronic storage or transmission is completely secure. Although the App uses reasonable technical safeguards, we cannot guarantee absolute security.

7. Permissions and device capabilities

Depending on Android version and device configuration, Daily Signal may request or use permissions and system capabilities necessary to provide its functions, including internet access, notifications, foreground-service operation, alarm scheduling, wake locks, startup after device reboot, and access to device motion sensors.

The user can manage available permissions through Android settings. Revoking a required permission or restricting background operation may prevent alerts or scheduled emails from working reliably.

8. User choices and controls

The user can:

- disable monitoring within the App;
- change or remove recipient and SMTP settings;
- choose whether diagnostic logs are attached to check-in emails;
- export diagnostic logs only when desired;
- manage App permissions and background-operation settings in Android; and
- delete locally stored App data by clearing App storage or uninstalling the App.

9. Children's privacy

Daily Signal is not directed to children under 13, and we do not knowingly collect personal information from children. The App should be configured and supervised by an adult where it is used in connection with a child or another dependent person.

10. International processing

Email messages may be processed or stored in countries other than the user's country, depending on the SMTP service and recipient email services selected by the user. Those providers' privacy policies and legal obligations govern their handling of the email.

11. Third-party services

The self-hosted release does not include advertising services and does not send App analytics or motion data to Gobeond. The App relies on Android platform services and on the SMTP/email providers chosen by the user. Those third parties operate under their own terms and privacy policies.

12. Changes to this policy

We may update this Privacy Policy to reflect changes to the App, legal requirements or data practices. The revised policy will show a new effective date. Material changes may also be communicated through the App or its Google Play listing where appropriate.

13. Contact

Questions, concerns or privacy requests relating to Daily Signal may be sent to:

Gobeond
Email: contact@gobeond.com

14. Important limitation

Daily Signal is a wellbeing-assistance utility. It is not an emergency service, medical device, security system or substitute for direct contact, professional care or emergency assistance. Email delivery and background operation can be affected by device settings, network availability and third-party email services.