

Flussonic LLC

PRIVACY POLICY

Effective Date: 11 September 2026

1. General Provisions.

1.1. This Privacy Policy describes how we collect, use, store, disclose and protect personal data of users of the website <https://flussonic.com/>, its subdomains, the personal account, web applications, and the Flussonic Watcher mobile application for iOS and Android, as well as the Flussonic App Tester mobile application for Android (hereinafter collectively referred to as the “Products”).

1.2. This Policy applies to all users of the Products, including users of the website, the personal account, web applications and the Flussonic Watcher mobile application and the Flussonic App Tester mobile application.

1.3. In this Privacy Policy, the terms “the Company”, “we” and “us” refer to Flussonic LLC.

1.4. By using the Products, the user confirms that they have read this Policy. If the user does not agree to the terms of this Policy, they must cease using the relevant Product.

1.5. This Policy is intended to disclose the types of data that may be collected, transmitted from the user’s device, used, stored and protected when using the Products, including the Flussonic Watcher mobile application and the Flussonic App Tester mobile application.

1.6. This Policy has been drawn up in accordance with the requirements of the Google Play User Data Policy, the Google Play Data Safety section, the Apple App Store Review Guidelines and the Apple App Privacy Details. Information regarding the collection, use, transfer, storage and deletion of data, as set out in the Google Play Console, App Store Connect, the app listing and other materials, must comply with this Policy and the actual operation of the Products. Should there be any changes to the types of data collected, the purposes of processing, the SDKs used, the service providers, the retention periods or the data deletion mechanisms, the Company will update this Policy and, where necessary, the information in the Google Play Console and App Store Connect.

2. Important information about the Flussonic Watcher mobile app.

2.1. When using the Flussonic Watcher mobile app, some user and technical data is transferred from the user’s device to the Company’s servers and/or the servers of service providers used by the Company to ensure the app functions properly.

2.2. Such data transfer is necessary for user authentication, providing access to video surveillance functions, viewing video streams and archives, delivering push notifications, diagnosing faults, ensuring security, analysing the app’s stability and improving the user experience.

2.3. The Company does not use the Flussonic Watcher mobile application to sell users’ personal data, display behavioural advertising, or transfer data to advertising partners for their own marketing purposes.

2.4. Certain data may be processed locally on the user’s device. If such data is not transferred outside the device, it is used solely to ensure the application functions properly and is not considered to have been transferred to the Company or to third parties.

2.5. The Flussonic Watcher mobile app may request access to certain device functions only to the extent necessary for the relevant app functions to operate.

2.6. Depending on the app version, operating system and features used, the app may request permissions to receive push notifications, access the network, local network, camera, microphone, photos/videos, files, geolocation or other device features.

2.7. The user can manage these permissions in the iOS or Android settings and/or within the app's settings. Restricting certain permissions may affect the availability of the relevant features.

2.8. If the app requests a system permission, the purpose of such a request is disclosed to the user via the app's interface, an operating system notification or another available notification.

3. What data we collect.

3.1. Data provided by the user.

To register, identify you and grant access to the Products, we collect information that you voluntarily provide when creating an account, taking out a subscription or contacting support. This may include your name, email address, telephone number, username and user ID within the system.

3.2. Data collected automatically.

Whilst you are using our Products, we automatically collect technical information necessary for their stable operation and improvement: details about your device and operating system, your IP address, data on your actions within the app (including interactions with the interface and video player), as well as diagnostic information regarding errors and malfunctions. We use push tokens to deliver notifications to mobile devices. For Flussonic App Tester, automatically collected data is limited to the FCM push token and server-side build download logs containing the IP address, request time and account identifier.

3.3. CCTV data.

As part of the Flussonic Watcher service, we may process video streams from users' cameras, archived video recordings, video clips, images/frames, camera settings, camera, channel or stream identifiers, as well as other data necessary for connecting to the video surveillance system and viewing live video and archived footage. This data is processed solely for the purpose of providing video surveillance functions, at the request of the user, operator or system administrator. The company does not use video data for advertising, data sales, independent user profiling or any other purposes not related to the provision of video surveillance functions.

3.4. Cookies.

On the Website and in web applications, we use cookies to ensure functionality, analyse user behaviour and remember settings. You can manage your cookie settings in your browser.

3.5. Password, token or other login credentials.

To enable authorisation and the automatic renewal of tokens, the Flussonic Watcher and Flussonic App Tester mobile applications may store a password, token or other login credentials locally on the user's device in the operating system's secure storage. Such data is used solely for logging into the app, maintaining the user's session and automatically renewing tokens. It is not used for analytics, advertising, marketing or profiling. If the transmission of credentials to the server is required for authorisation or to renew a token, such transmission is carried out exclusively to verify access rights and ensure the account functions correctly.

4. Purposes of data processing.

We process personal data for the following purposes:

- a. to provide access to the Products, their Updates and technical support;
- b. to improve the user experience, performance and stability of the services;
- c. to ensure security and prevent fraud;
- d. to provide information on the status of the service, updates and new features (with the option to unsubscribe);
- e. to comply with legal requirements.

5. Services, SDKs and data processing channels used.

To ensure the operation of the Products, analytics, diagnostics, logging, notification delivery and improved stability, we may use the following services and SDKs:

5.1. Flussonic Mobile Logger.

Flussonic Mobile Logger is the primary channel for collecting technical telemetry from the mobile application. It is not used in Flussonic App Tester.

It can process: login; operator_id; device technical context; application version; interface events; video player events; diagnostic data; error information; performance data; technical events required for analysing the application's stability.

This data is used for diagnostics, technical support, bug fixes, analysing the app's performance and improving the Products.

5.2. Firebase Analytics.

Firebase Analytics may be used on a limited basis as a backup analytics channel. It is not used in Flussonic App Tester.

It may process technical device or app instance identifiers, app usage events, details of interactions with the app, and other technical data necessary for analysing the app's performance.

Firebase Analytics is not used by the Company to sell users' personal data or to transfer data to advertising partners for their own marketing purposes.

5.3. Firebase Crashlytics.

Firebase Crashlytics is used to collect and analyse information about app crashes. It is not used in Flussonic App Tester.

It may process crash logs, stack traces, and information about the device, operating system, app version and the technical state of the app at the time of the crash.

This data is used to diagnose and resolve errors, and to improve the stability and security of the app.

5.4. Firebase Cloud Messaging.

Firebase Cloud Messaging is used to deliver push notifications in Flussonic Watcher and Flussonic App Tester.

For this purpose, the device's FCM token and technical information required to deliver notifications may be processed.

6. Disclosure of data to third parties.

6.1. Data may be disclosed where necessary for the provision of the Products, the performance of the contract, security, technical support, analytics, diagnostics, the delivery of notifications, payment processing, and in other cases provided for by applicable law.

6.2. Data may be transferred to the following categories of recipients: hosting providers and cloud services, analytics, diagnostics and crash-reporting services, push notification services, payment partners, technical support contractors, operators or administrators of video surveillance systems, as well as government authorities in cases provided for by law.

6.3. The Company does not sell users' personal data nor does it transfer it to advertising partners for the purpose of displaying behavioural advertising, independent marketing or independent profiling.

6.4. Service providers acting on behalf of the Company are required to ensure confidentiality, security and a level of data protection consistent with applicable contractual and legal requirements. Other recipients receive data only to the extent necessary for the purposes described in this Policy.

7. Data retention periods.

We retain personal data for as long as is necessary to fulfil the purposes for which it is processed, or for the period specified by applicable legislation. User accounts and profile data are retained until they are deleted by the user. Analytical data is retained for up to 36 months, and error logs for up to 12 months. Once the retention period has expired, the data is destroyed or anonymised.

8. Users' rights.

You have the right to access your personal data, to have it rectified, erased or its processing restricted, and to withdraw your consent to processing at any time. To exercise these rights, you may contact us via your personal account, by email at info@mail.flussonic.com, or by sending a written request to the Company's address. We undertake to respond to your request within 30 days.

9. Data security.

We take organisational and technical measures to protect data from unauthorised access, destruction, alteration or disclosure: encryption during transmission and storage, access controls, regular system updates and vulnerability monitoring. In the event of an incident, we will notify the relevant authorities and data subjects within the timeframes set out by law.

10. Data relating to minors.

Our Products are not intended for persons under the age of 16. We do not deliberately collect data relating to minors. Should we become aware of any such processing, we will delete this data.

11. Data deletion.

11.1. A user may request the deletion of their personal data by submitting a request to customer support or by using the relevant functions in their personal account, where such functions are available.

11.2. When an account is deleted, certain data may be retained for as long as necessary if this is required to: comply with legislation; ensure security; prevent fraud; resolve disputes; fulfil contractual obligations; protect the rights of the Company, users or third parties.

11.3. If a user accesses the Products via an operator, system administrator or video surveillance service provider, the deletion of an account, video data or access rights may depend on the settings and decisions of the relevant operator, administrator or service provider.

12. Changes to the Policy.

12.1. The Company reserves the right to amend this Policy. The updated version will be published on the website <https://flussonic.com/privacy-policy> or in another location accessible to users.

12.2. Changes shall take effect from the date of publication, unless a different date is specified in the revised version of the Policy or is required by applicable law.

12.3. Continued use of the Products after the changes take effect shall be deemed to constitute the user's acceptance of the updated version of the Policy.