FlinQ App Privacy Policy

Effective Date: 01-01-2023

Updated: 01-12-2025

FlinQ & Co B.V. and its subsidiaries (“we”, “us”, “our”, “FlinQ Commerce”) are committed to protecting your privacy. This Privacy Policy (“Policy”) describes how we collect, use, store, share and otherwise process your personal data when you use our mobile applications and connected services (collectively, the “Products”).

This Policy applies in particular to:

- FlinQ Mobile Application (the “App”)

- Smart devices and related services that are connected to, or controlled via, the App (collectively, the “Smart Devices”).

Please read this Policy carefully before using our Products so that you understand how and why we process personal data, and which rights you have.

By registering an account in the App, by connecting Smart Devices, or by otherwise using our Products, you acknowledge that you have read and understood this Policy. If you do not agree with this Policy, you should not use our Products.

If you have any questions or concerns about this Policy, please contact us at:

FlinQ & Co B.V.

Havenstraat 76M
1271AG Huizen

The Netherlands

Email: info@flinqproducts.nl

For other branded mobile applications powered by FlinQ Commerce, our clients (for example, other brands or companies) control all personal data collected through those applications. In those cases, we process personal data on behalf of our clients and in accordance with their instructions. If you are a customer of one of our clients and no longer wish to be contacted by them, please contact that client directly.

1. Definitions

In this Policy:

“Personal Data” means any information that relates to an identified or identifiable natural person, and that is generated, collected, recorded and/or stored by us electronically or otherwise. This includes data that can identify you directly (such as name or email address) or indirectly in combination with other data.

“Personal Sensitive Data” includes, for example, biometric information, communication contents, health information, transaction information, and precise location information. When we collect Personal Sensitive Data from you, we will clearly notify you and obtain your explicit consent where required by law.

“Smart Devices” are physical devices produced or manufactured by hardware manufacturers with a human-machine interface and the ability to transmit data wirelessly, such as smart home appliances, smart lighting, cameras, security devices, wearables, air cleaning devices, and similar products.

“Apps” are mobile applications developed by FlinQ Commerce that enable end users to remotely control Smart Devices and connect to the relevant IoT platform.

2. What Personal Data Do We Collect?

We only collect the personal data that is necessary to provide our services and to improve your experience. If you choose not to provide certain personal data, some features of the Products may not be available or may not function correctly.

2.1 Information You Voluntarily Provide to Us

a) Registered Account Data

When you register an account in the App, we may collect:

- Name (if you choose to provide it)
- Email address and/or phone number
- Username
- Password or other login credentials

During your use of the Products, you may also choose to add:

- Nickname
- Profile picture
- Country/region
- Language preference
- Time zone

If you use a third-party account (such as a social media or platform account) to log in to the App, we may obtain certain information from that third party (such as profile picture, nickname, region, gender) to enable quick login and account binding. We will process such data in accordance with applicable data protection laws and with any agreements or policies applicable to that third-party service.

b) Information for Additional Functions

To provide more convenient and higher-quality services and to optimize user experience, we may request access to certain functions or data on your mobile device. You can choose whether to grant or deny these permissions. If you do not grant them, you can still use the basic functions of the App and Smart Devices, but some features may not be available.

These additional functions include:

1. Location-based services

When you enable location permissions, we may collect:

- Real-time precise location (e.g. for automation scenarios for controlling Smart Devices)

- Non-precise geo-location (e.g. for certain Smart Devices or weather-related functions)

If you enable geo-fence features, your location data may be shared with map service providers (such as Google Maps) to provide these services. You can disable location collection in the App or in your device settings at any time:

My → Settings → Privacy Settings → Location Information.

2. Camera-based services

When you enable camera permissions, you can:

- Scan QR codes to pair Smart Devices

- Record video or capture images within the App

We will only access the camera when you actively use these functions. You can disable camera permissions at any time:

My → Settings → Privacy Settings → Camera.

3. Photo/Video Library access

When you enable photo album / media library permissions, you can:

- Upload photos or videos (e.g., to change your avatar or to report device usage issues)

We will only access the photos/videos you choose to upload. You can disable this permission at any time:

My → Settings → Privacy Settings → Photo Album.

4. Microphone-based services

When you enable microphone permissions, you can:

- Send voice commands or voice messages
- Record videos with audio
- Use voice assistant features

We will only collect voice data when you actively use these functions. You can disable microphone permissions at any time:

My → Settings → Privacy Settings → Microphone.

5. Storage permission (Android)

When you grant storage permissions, we may:

- Read/write necessary files to ensure stable App operation
- Access images, files and crash logs for error analysis and reporting

You can revoke this permission at any time:

My → Settings → Privacy Settings → Storage.

6. Notification permission

When you enable notifications, we may send you push notifications, for example:

- Alerts and messages related to the status of your Smart Devices

- Security alerts if you use security-related services

You can manage or disable notifications at any time:

My → Message Center → Settings → Notifications.

7. Alert Window permission

If you bind a camera in the App, you may allow the App to display real-time camera images in a separate window.

You can disable this permission at any time:

My → Settings → Privacy Settings → Alert Window.

8. Bluetooth permission

When you enable Bluetooth, we may communicate with Smart Devices via Bluetooth to:

- Discover nearby Smart Devices

- Configure network settings

- Display status and allow control of Smart Devices

We only use Bluetooth in these specific scenarios. You can disable Bluetooth permissions at any time via your device settings or:

My → Settings → Privacy Settings → Bluetooth.

9. HomeKit permission (iOS)

When enabled, we may:

- Discover compatible HomeKit devices

- Configure networks for HomeKit devices

- Control HomeKit devices and display their status

We interact with the iOS “Home” app only for these purposes. You can disable HomeKit integration at any time:

My → Settings → Privacy Settings → HomeKit.

10. HealthKit (iOS)

For certain health-related Smart Devices (such as body fat scales, smart bands, or watches), you may choose to connect with Apple Health via HealthKit. If you do so, measurement data such as body weight, height, BMI and body fat percentage may be shared with Apple Health solely for health analysis.

You can revoke HealthKit access at any time in your device’s HealthKit settings.

If you enable any of these permissions, you authorize us to collect and use the relevant personal data to provide the associated services. If you disable a permission, we will no longer collect personal data based on that permission. Disabling a permission does not affect the lawfulness of processing based on your consent before you disabled it.

2.2 Information We Collect Automatically

When you use the App or interact with our Services, we automatically collect certain information, including:

- Mobile Device Information

Device model, operating system, application version, IP address, wireless connection information, mobile network information, push notification identifier, and information about other installed applications or software where necessary to maintain security and functionality.

- Usage Data

Information about how you interact with the App and Services, such as visits, clicks, feature usage, downloads, and messages sent/received.

- Log Information

System logs and error logs, including IP address, language settings, operating system version, access date and time, and crash logs, to help us identify and resolve issues.

On their own, these types of information do not generally identify a specific individual. However, if we combine them with other data in a way that makes it possible to identify you, we will treat them as Personal Data.

2.3 Smart Devices Related Information

When you connect Smart Devices to the App, we may collect:

- Basic Smart Device Information

Device name, device ID, device type, online/offline status, activation time, firmware version, and upgrade information.

- Information collected during setup

Depending on the device type, this may include Wi-Fi network name (SSID), device MAC address and other configuration data needed to connect the device to your network.

- Information reported by Smart Devices

Depending on the Smart Device and the features you use, this may include, for example:

- For smart cameras: device status, motion detection events, video stream metadata or thumbnails
- For smart plugs: on/off status, power consumption statistics
- For smart lighting: brightness level, color settings, on/off status
- For security sensors: door/window open/close status, alerts

If you connect health-related Smart Devices to Apple Health (via HealthKit, as described above), we may share measurement data (such as height, weight, BMI, body fat %) with Apple Health solely to provide health-related features. This data will not be shared with other third parties for unrelated purposes.

3. Purposes and Legal Bases for Processing Personal Data

We process your Personal Data for the following purposes and on the legal bases indicated:

3.1 Provide You with Our Services

We process account data, Smart Device information, mobile device information, usage data and location data as necessary to:

- Create and manage your App account
- Connect and configure Smart Devices
- Provide remote control and monitoring of Smart Devices
- Provide core App functionalities and related services you request

Legal basis: performance of a contract (User Agreement) with you (Article 6(1)(b) GDPR).

3.2 Improve Our Services

We process mobile device information, usage data, log data, location information and Smart Device information to:

- Ensure the functionality, security and stability of the App and Smart Devices

- Develop, test and improve features and user experience

- Monitor the performance and efficiency of our operations

- Detect, prevent and trace misuse, fraud or security incidents

Legal basis: performance of contract and our legitimate interests in maintaining and improving the Services (Article 6(1)(b) and 6(1)(f) GDPR).

3.3 Non-Marketing Communication

We use your Personal Data to send you:

- Administrative messages about the App and Services

- Important information about changes to our terms, conditions or policies

- Notifications related to services you have purchased (e.g., security alerts, device alerts, critical updates)

These communications are considered part of the Services and are not marketing messages. You can manage some of these notifications within the App under:

Me → Message Center → Settings → Notification Settings.

Legal basis: performance of our contract with you (Article 6(1)(b) GDPR) and our legitimate interests in providing safe and reliable services (Article 6(1)(f) GDPR).

3.4 Email Newsletters and Direct Marketing

We may use your email address to send you electronic commercial messages, such as:

- Newsletters about FlinQ Commerce and our products
- Special offers, promotions and discount codes
- Information about new or improved smart products and services
- Tips and inspiration about using your Smart Devices and creating a smart home

We will only send these types of emails if you have given us your prior, explicit consent, for example:

- By subscribing via our website or online forms
- By registering a product and opting in to receive the newsletter
- By ticking a newsletter checkbox in the App or another FlinQ channel

We may send such emails weekly, and in some cases multiple times per week.

You can withdraw your consent at any time by:

- Clicking the unsubscribe link at the bottom of each marketing email; or
- Contacting us at info@flinqproducts.nl.

Withdrawing your consent does not affect the lawfulness of processing based on consent before its withdrawal and will not affect your use of the FlinQ App or your contractual rights (such as warranty).

Legal basis: your consent (Article 6(1)(a) GDPR) and compliance with applicable e-privacy and anti-spam rules (including the Dutch Telecommunications Act).

3.5 Data Analysis

We may analyze data you provide to us, and data we collect automatically, to:

- Diagnose and resolve malfunctions or technical issues
- Improve product performance and usability
- Understand how users interact with the App and Smart Devices
- Optimize features and scenarios for better user experience

Where data analysis is strictly necessary to ensure functionality, quality and security, you may not be able to fully opt out, as this is closely related to the performance of the product and service.

For other data analysis activities (for example, optional analytics), you can manage your choices in the App:

My → Settings → Privacy Settings → Data Analysis.

Legal basis: our legitimate interests in analyzing and improving our Services (Article 6(1)(f) GDPR) and, where required, your consent (Article 6(1)(a) GDPR).

3.6 Marketing Communication and Personalization (In-App and Online)

We may process your account data, usage data and device information to:

- Personalize the App interface and content

- Recommend products or features within the App or on our websites that may be relevant to you

- Display non-intrusive ads, suggestions or in-App banners related to our products and services

- Invite you to participate in surveys about your use of the Services

Email newsletters and other direct electronic marketing are covered separately under "Email Newsletters and Direct Marketing" and are only sent if you have given us your prior consent.

You can opt out of certain personalization features via the App:

My → Settings → Privacy Settings → Personalization.

Legal basis: our legitimate interests in customizing and improving user experience (Article 6(1)(f) GDPR) and, where applicable, your consent (Article 6(1)(a) GDPR).

3.7 Legal Compliance and Protection

We may process or disclose your Personal Data where necessary to:

- Comply with a legal obligation, request or process

- Enforce our User Agreement and other applicable agreements, policies or standards

- Protect the rights, property or safety of FlinQ Commerce, our users, third parties or the public

- Detect, prevent or address security, fraud or technical issues

Legal basis: compliance with legal obligations (Article 6(1)(c) GDPR) and our legitimate interests in protecting our business and users (Article 6(1)(f) GDPR).

4. Who Do We Share Personal Data With?

We only share your Personal Data in the ways described in this Policy:

- Service Providers

With third-party service providers who perform services on our behalf, such as hosting, data analysis, payment processing (if applicable), IT support, customer service, email delivery, and other similar services. These providers may only use the data as necessary to provide services to us and are bound by confidentiality and data protection obligations.

- Business Partners and Clients

With customers or other business partners who provide you, directly or indirectly, with Smart Devices, networks or systems through which you access our Services, where necessary to enable the Services.

- Affiliates

With our subsidiaries and affiliates within our corporate group, for regular business activities, in accordance with this Policy and applicable law.

- Corporate Transactions

In connection with any reorganization, merger, sale, joint venture, assignment, transfer, or other disposition of all or part of our business, assets or stock (including in connection with bankruptcy or similar proceedings). If such a transaction occurs, you will be notified of any change in ownership and of any choices you may have regarding your Personal Data.

- Legal and Security

Where we believe in good faith that access, use, preservation or disclosure of the data is reasonably necessary to:

(a) comply with applicable law, regulation, legal process or governmental request;

(b) enforce our User Agreement or other agreements, policies and standards;

(c) protect our operations and business systems;

(d) protect the rights, property or safety of us, our users, third parties or the public; or

(e) perform risk management, screening and checks for unlawful, fraudulent, deceptive or malicious activities.

Except as described above, we will only disclose your Personal Data to third parties with your consent or where we are legally permitted or required to do so.

5. International Transfers of Personal Data

Your Personal Data may be transferred to and stored on servers located in countries other than your country of residence. These countries may have data protection laws that are different from the laws in your country.

Where we transfer Personal Data from the European Economic Area (EEA) or the United Kingdom to a country that does not provide an adequate level of data protection, we will ensure an appropriate level of protection by using one or more of the following safeguards:

- Using Standard Contractual Clauses (SCCs) approved by the European Commission under Article 46 GDPR; and/or

- Other appropriate safeguards as permitted by applicable data protection law.

You can contact us at info@flinqproducts.nl if you would like more information about the safeguards we use for international data transfers.

6. Your Rights Relating to Your Personal Data

Subject to applicable law, you have the following rights in relation to your Personal Data:

- Right of access – You can request confirmation whether we process your Personal Data and obtain a copy of such data. In the App, you may export certain data via:

My → Settings → Privacy Settings → Personal Data Export.

- Right to rectification – You can request correction of inaccurate or incomplete Personal Data. In the App you may, for example:

- Change your email address or phone number: My → Settings → Account and Security → Change Account;

- Modify your nickname or time zone: My → Personal Information.

- Right to erasure ("right to be forgotten") – You can request deletion of your Personal Data. You can delete your account in the App via:

My → Settings → Account and Security → Delete Account (Deactivate Account).

When you confirm deletion of your account, Personal Data associated with that account will be deleted or anonymised, unless we must keep certain data for legal obligations.

- Right to restriction of processing – You can request that we restrict processing of your Personal Data in certain circumstances. You can send such a request via the App:

My → FAQ & Feedback, or by emailing us at info@flinqproducts.nl.

- Right to data portability – Where processing is based on your consent or on a contract and carried out by automated means, you may request a copy of your Personal Data in a structured, commonly used and machine-readable format, and request that we transmit this data to another controller where technically feasible.

- Right to object – You may object to processing of your Personal Data where we rely on legitimate interests as the legal basis. We will stop processing unless we have compelling legitimate grounds or the processing is needed for legal claims.

- Right to withdraw consent – Where we rely on your consent (e.g. for email newsletters, optional analytics or personalization), you can withdraw your consent at any time. This will not affect the lawfulness of processing before withdrawal. You can:

1. Change device-level permissions (location, camera, photo library, microphone, Bluetooth, notifications) in your mobile device settings or in the App:

My → Settings → Privacy Settings.

2. Manage non-marketing notifications via:

Me → Message Center → Notification Settings.

3. Opt out of optional data analysis via:

My → Settings → Privacy Settings → Data Analysis.

4. Opt out of personalization features via:

My → Settings → Privacy Settings → Personalization.

5. Unbind Smart Devices in the App so that we no longer collect data from those devices.

6. Withdraw consent for linkage to third-party platforms (e.g., health platforms) on the relevant third-party platform.

7. Unsubscribe from email newsletters and other direct marketing by clicking the unsubscribe link at the bottom of each marketing email, or by sending a request to info@flinqproducts.nl.

After you unsubscribe, we will no longer use your email address for direct marketing, but we may still process it for other lawful purposes (such as account administration or compliance with legal obligations).

You do not have to pay a fee to exercise your rights. We may ask you to verify your identity before responding to your request. We aim to respond within one month, or within a longer period if allowed by law, in which case we will inform you.

7. Security Measures

We use commercially reasonable physical, administrative and technical safeguards to protect the integrity and security of your Personal Data.

For example, FlinQ Commerce employs:

- Secure algorithms and encryption protocols for data transmission;
- Access controls and authentication mechanisms to prevent unauthorized access;
- Data isolation and authorization management for device access;
- Strict data filtering, validation and logging for data processing;
- Encryption of confidential user information during storage.

Although we take reasonable steps to protect your Personal Data, no system or transmission can be guaranteed to be 100% secure. If you believe that your interaction with us is no longer secure (for example, if you suspect that your account has been compromised), please notify us immediately at info@flinqproducts.nl.

8. Data Retention

We retain your Personal Data only for as long as necessary for the purposes described in this Policy, unless a longer retention period is required or permitted by law.

We determine the appropriate retention period by considering:

- The amount, nature and sensitivity of the Personal Data;
- The potential risk of harm from unauthorized use or disclosure;
- The purposes for which we process the data and whether we can achieve those purposes through other means;

- Applicable legal, regulatory, tax, accounting or other requirements.

In general:

- We retain Personal Data for as long as your account is active and we are providing the Services to you under the User Agreement.

- If you request deletion of your Personal Data or deletion of your account, we will delete or anonymise your Personal Data within a reasonable period, unless we are legally required or permitted to retain certain data for longer (for example, for tax, legal or compliance purposes).

Where we are no longer able to fully delete certain data for technical reasons, we will ensure that appropriate safeguards are in place and that such data is no longer actively processed for any purpose other than storage.

9. Children's Privacy

Protecting the privacy of young children is especially important to us.

Our Services are not directed to individuals under the age of sixteen (16), and we request that such individuals do not provide any Personal Data to us.

In the Netherlands, children under the age of 16 cannot validly give consent for the processing of their personal data for information society services. Where we rely on consent as a legal basis, such consent must be given or authorised by the holder of parental responsibility.

We do not knowingly collect Personal Data from children under 16 without permission from a parent or legal guardian. If we become aware that we have collected Personal Data from a child under 16 without such permission, we will take steps to delete that information and, if applicable, delete the child's account.

If you believe that we might have any information from or about a child under 16, please contact us at info@flinqproducts.nl.

10. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements, or other factors.

If we make material changes, we will notify you by:

- Sending an email to the address associated with your account; and/or

- Displaying a prominent notice in the App.

We encourage you to periodically review this Policy for the latest information on our privacy practices. Your continued use of the App and Services after the effective date of the updated Policy will constitute your acceptance of the changes.

11. Contact Us

If you have any questions, concerns or complaints about this Privacy Policy or our handling of your Personal Data, or if you wish to exercise your data protection rights, please contact us:

FlinQ & Co B.V.

Havenstraat 76M
1271AG Huizen

The Netherlands

Email: info@flinqproducts.nl

We will do our best to address your concerns. You also have the right to lodge a complaint with your local data protection authority if you believe that our processing of your Personal Data infringes applicable data protection law.