

Privacy Policy

This Privacy Policy explains how **FireIQ Technologies GmbH** processes personal data when you use the **FireIQ mobile app** (the “App”), available on the Apple App Store and Google Play, together with the user account that connects the App to the FireIQ Cloud Hub.

Version 1.0 · Effective date: **1st of July 2026**. This Policy is published at fireiq.de and applies regardless of the platform through which the App is obtained.

01 · CONTROLLER

Who is responsible for your data

The controller within the meaning of the EU General Data Protection Regulation (GDPR) is:

FireIQ Technologies GmbH

Gleisdreieck 11 · 42651 Solingen · Germany

E-mail: info@fireiq.de · Web: fireiq.de

02 · SCOPE

What this Policy covers

This Policy covers the processing of personal data in connection with the App and the associated FireIQ user account. Separate privacy notices apply to the fireiq.de website and to the FireIQ Cloud Hub web platform where these involve additional processing. The App is a professional tool for operators, technicians, compliance officers and service partners managing connected fire-safety equipment; it is intended for business use.

Apple Inc. and Google Ireland Ltd. act as independent controllers for the processing they perform when you download the App from their stores (e.g. store account data, download statistics). Please refer to their respective privacy policies for details.

03 · DATA WE PROCESS

Categories of personal data

a) Account and authentication data

Name, e-mail address, organization, assigned role and permissions, login credentials, and settings associated with your FireIQ user account. Accounts are typically created and administered by your organization or its authorized administrator.

b) Device, log and diagnostic data

When you use the App, we process technical data required to deliver and secure the service: device model and operating-system version, App version, language settings, IP address, access timestamps, and technical event logs. Crash and diagnostic data may be processed to maintain the stability and security of the App. No third-party crash-reporting or analytics SDKs are integrated in the App.

c) Location data

The App uses your device's position only for specific functions you actively trigger - in particular the commissioning wizard, which can auto-capture the installation address of a device from your phone's position when you register a new unit. Location access requires your permission at operating-system level and can be revoked at any time in your device settings. The App does not track your location in the background.

d) Camera and photos

With your permission, the App uses the camera to scan QR codes on FireIQ devices and to take guided photos (e.g. device and type-plate photos during commissioning, or photo evidence attached to fault reports). Photos are linked to the relevant device record in the FireIQ Cloud Hub.

e) Service and activity records

Actions you perform in the App are recorded in the digital service record of the relevant device - for example activating maintenance mode, closing a job, or submitting a structured fault report. These records include your user identity, a timestamp and the action performed, and form part of the tamper-evident documentation trail that the FireIQ platform provides to operators for compliance purposes.

f) Push notifications

If you enable notifications, we process the push token assigned to your device by the operating-system provider (Apple/Google) in order to deliver alerts and status messages. You can disable notifications at any time in the App or in your device settings.

g) Equipment telemetry

Sensor data transmitted by connected FireIQ devices (e.g. pressure, temperature, humidity, motion, battery, position of the unit) relates to equipment, not to individuals, and is generally not personal data. Where telemetry is combined with user activity (e.g. a maintenance-mode entry logged to a named technician), the resulting records are processed as described under (e).

h) Support communication

If you contact our support, we process the information you provide (contact details, content of your request) to handle your enquiry.

Why we process your data

We process personal data on the following legal bases under Art. 6(1) GDPR:

Purpose	Data categories	Legal basis
Providing the App and account, authentication, synchronization with the Cloud Hub (incl. offline-first sync)	Account data; device and log data; service and activity records	Art. 6(1)(b) GDPR - performance of a contract, or Art. 6(1)(f) where you use the App on behalf of your organization
Commissioning functions (address auto-capture, QR scanning, guided photos)	Location data; camera and photo data	Art. 6(1)(a) GDPR - consent, given via the operating-system permission dialogs; revocable at any time
Delivering alerts and status notifications	Push tokens; account data	Art. 6(1)(a) GDPR - consent (notification opt-in), and Art. 6(1)(b) for contractually agreed alerting
Maintaining digital service records and compliance documentation for operators	Service and activity records	Art. 6(1)(b) and Art. 6(1)(f) GDPR - legitimate interest of operators and FireIQ in verifiable, audit-ready maintenance documentation
Security, stability, fault diagnosis and abuse prevention	Device, log and diagnostic data	Art. 6(1)(f) GDPR - legitimate interest in a secure and reliable service
Support and communication	Support communication data	Art. 6(1)(b) or (f) GDPR
Compliance with statutory obligations (e.g. commercial and tax retention duties)	Data required by the respective obligation	Art. 6(1)(c) GDPR

Permissions and how to control them

- **Camera** — QR-code scanning, commissioning photos and fault-report photo evidence. Optional; requested only when you use these functions.
- **Location** — address auto-capture during device commissioning. Optional; requested only when you use this function.
- **Notifications** — delivery of alerts and status messages. Optional.

All permissions can be granted or revoked at any time in your device's operating-system settings. Core App functions that do not depend on a permission remain usable if the permission is declined.

06 · USERS ACTING FOR ORGANIZATIONS

Business context and role-based access

The App is used in a professional context. Your organization (or the service partner you work for) typically determines which users receive accounts, which roles and permissions they hold, and how long accounts remain active. Access to data in the FireIQ platform is governed by role-based permissions: operators, technicians, compliance officers and service partners each see only the data assigned to their role and projects. Where FireIQ processes personal data on behalf of a customer organization, this is governed by a data processing agreement pursuant to Art. 28 GDPR.

07 · RECIPIENTS

Who receives your data

We share personal data only to the extent necessary to operate the App and platform:

- **Hosting providers** — the FireIQ platform is hosted on EU-based cloud servers. Data is encrypted in transit and at rest.
- **Communication providers** — technical service providers for the delivery of push notifications (Apple/Google), e-mail and SMS alerts.
- **Your organization and its service partners** — service and activity records are visible to the operator of the equipment and its authorized service partners in line with role-based permissions.
- **Authorities** — where we are legally obliged to disclose data.

All service providers acting on our behalf are bound by data processing agreements pursuant to Art. 28 GDPR.

Hosting providers - the FireIQ app and platform are hosted by The Real Insight GmbH, using Deutsche Telekom (T-Cloud Public) infrastructure located in the EU. Data is encrypted in transit and at rest.

Mapping and location services - Mapbox, to render maps and process device or building location data you actively provide (e.g. commissioning wizard, asset location).

Speech and transcription services - Microsoft Azure (server-side speech-to-text for live chat transcription) and Apple/Google native speech-recognition and text-to-speech services (on your device, for dictation and voice playback in the chat).

08 · INTERNATIONAL TRANSFERS

Where your data is processed

Personal data is hosted and processed on servers located in the European Union. Should a transfer to a country outside the EU/EEA become necessary in individual cases (for example, in connection with push-notification delivery by Apple or Google), it takes place only where an adequacy decision of the European Commission applies or appropriate safeguards within the meaning of Art. 46 GDPR (in particular EU Standard Contractual Clauses) are in place.

09 · RETENTION

How long we keep your data

- **Account data** — for the duration of the contractual relationship and account lifetime; deleted or anonymized after termination, subject to statutory retention duties.
- **Service and activity records** — for the documentation periods required for fire-safety compliance and the term agreed with the operator, as these records form the audit trail of the equipment.
- **Log and diagnostic data** — for a limited period appropriate to security and troubleshooting purposes, then deleted or anonymized. Server logs and diagnostic data are retained for a maximum of 30 days before automatic deletion.
- **Statutory retention** — where commercial or tax law (e.g. § 257 HGB, § 147 AO) requires longer storage, data is retained for the statutory period and blocked from other use.

10 · SECURITY

How we protect your data

FireIQ applies technical and organizational measures appropriate to the risk, including encryption of data in transit and at rest, user authentication, role-based access control, and EU-based hosting. Security has been part of the platform's design from the start of development. Measures are reviewed and updated on an ongoing basis.

11 · AI ASSISTANT AND AUTOMATED DECISIONS

No automated decision-making

The FireIQ platform includes an AI assistant that answers plain-language questions about your fleet (e.g. device status queries) using the data you are authorized to access. The assistant is an analysis and display function; it does not make decisions that produce legal effects concerning you or similarly significantly affect you. No automated decision-making within the meaning of Art. 22 GDPR takes place.

12 · YOUR RIGHTS

Your rights under the GDPR

You have the right to:

- **Access** (Art. 15 GDPR) — obtain information about the personal data we process about you;
- **Rectification** (Art. 16 GDPR) — have inaccurate data corrected;
- **Erasure** (Art. 17 GDPR) — have your data deleted where the legal conditions are met;
- **Restriction of processing** (Art. 18 GDPR);
- **Data portability** (Art. 20 GDPR);
- **Withdrawal of consent** (Art. 7(3) GDPR) — with effect for the future, e.g. by revoking an App permission;
- **Objection** (Art. 21 GDPR) — you may object at any time, on grounds relating to your particular situation, to processing based on Art. 6(1)(f) GDPR.

To exercise your rights, contact us at info@fireiq.de. You also have the right to lodge a complaint with a data protection supervisory authority (Art. 77 GDPR). The authority competent for FireIQ Technologies GmbH is the Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW), Düsseldorf; you may also contact the authority of your habitual residence or place of work.

13 · MINORS

No use by minors

The App is a professional tool and is not directed at children or minors. We do not knowingly collect personal data from persons under 16 years of age.

14 · CHANGES

Changes to this Policy

We may update this Policy when the App, our services or the legal framework change. The current version is always available at fireiq.de and within the App's store listings. Material changes affecting you will be communicated appropriately, e.g. in the App.

15 · CONTACT

Questions about privacy

FireIQ Technologies GmbH · Gleisdreieck 11 · 42651 Solingen · Germany · info@fireiq.de · fireiq.de

FIRE SAFETY THAT NEVER SLEEPS.