Crowd Connected
Mobile App Privacy Policy

Version 2.0
Date: April 2026

1. Introduction

Crowd Connected Ltd ("**CC**", "**we**", "**us**", "**our**") is a company registered in England (number 08417106) with its registered office at Surrey Technology Centre, Guildford, GU2 7YG. This privacy policy explains how we collect, use, and protect your personal data when you use our mobile applications ("**Apps**"), including **Sail Indoor Positioning**, **Quick Scanner**, **Smart Map** and any other mobile applications we publish from time to time.

This policy applies only to data collected through our mobile Apps. For information about how we handle data collected through the CC Console (our web-based management dashboard), please see the CC Console Privacy Policy.

Data controller and data processor roles. The data controller for your personal data depends on how you use the App:

(a) Where you use the App directly (for example, downloading Sail Indoor Positioning to explore its features), CC is the data controller for your personal data.

(b) Where you use the App in connection with a service operated by a third party (for example, an event organiser using CC's technology for wayfinding at their event), that third party is typically the data controller, and CC acts as a data processor on their behalf. In such cases, the third party's privacy notice governs how your data is used and CC's processing is governed by a Data Processing Addendum agreed between CC and that third party.

2. Data we collect

The data we collect depends on the specific App you use and the features you interact with. The table below summarises the data collected by each CC App.

Data category	Description	Sail Indoor Positioning	Quick Scanner	SmartMap
Location data	GPS, Wi-Fi, and Bluetooth-derived position data	Yes (with consent)	No	Yes (with consent)
Badge ID data	Data embedded in a QR or barcode	No	Yes (with consent)	No
Diagnostic data	Sensor readings (accelerometer, gyroscope, barometer), signal strength, battery level	Yes	No	Yes
Device identifiers	Device model, OS version, unique device identifiers (such as IDFV on iOS or Android ID), and advertising ID (collected subject to your	Yes	Yes	Yes

	device platform permissions — see section 2.5)			
Usage data	App feature usage, session duration, interaction patterns	Yes	Yes	Yes
Camera data	QR code / barcode scan data (not stored as images)	No	Yes	No
Account data	Email address, name (if account creation required)	No	No	No

Note: *This table will be updated as CC publishes new Apps or adds new data collection capabilities to existing Apps.*

2.1 Data you provide directly

None of CC's current Apps require account creation or collect your name or email address directly. If a future App version introduces account functionality, this Policy will be updated accordingly and you will be notified in advance.

2.2 Data collected automatically

When you use an App, we may automatically collect device identifiers, diagnostic data, and usage data as described in the table above.

2.3 Location data

Where an App collects location data, we will request your consent through the App's permission system before activating location data collection. Location data may be derived from GPS, Wi-Fi access point scanning, Bluetooth beacon detection, or a combination of these technologies. You can withdraw consent at any time through the App settings or your device's operating system settings.

2.4 Sensitive location contexts and special category data

Location data can, in certain contexts, reveal information that falls within the "special categories" of personal data under Article 9 UK GDPR — including data concerning health, religious or philosophical beliefs, or political opinions. For example, sustained presence at a place of worship, medical facility, or political rally may, by inference, reveal such information about the device user.

Crowd Connected's Apps may be used across a wide range of venue and event types, and we cannot guarantee that no App deployment will occur in a context where location data could reveal special category information about users. Where we become aware that an App is being deployed in such a context — or where a deployment is reasonably likely to involve the inference of special category data from location — we will, in addition to the standard location permission, present a clear and specific in-App consent notice explaining the nature of the

deployment and the special category data risk. This notice will be presented before any location data is collected and will require your affirmative action to proceed.

Our legal basis for processing special category data in this context is your explicit consent under Article 9(2)(a) UK GDPR, in addition to Article 6(1)(a) consent for the underlying location data. You may withdraw this consent at any time as described in section 2.3 above, and doing so will not affect the lawfulness of any processing carried out before withdrawal.

Where CC acts as a data processor for an event organiser or venue operator, the responsibility for identifying sensitive deployment contexts and obtaining appropriate consent rests primarily with that data controller. CC will include a contractual obligation in its Data Processing Addendum requiring event operator data controllers to notify CC and App users where a deployment involves special category location data.

2.5 Advertising IDs and platform-specific rules

Our Apps may collect your device's advertising identifier — the Identifier for Vendors (IDFV) or Identifier for Advertisers (IDFA) on iOS, or the Android Advertising ID (AAID) on Android. These identifiers are used for App analytics and diagnostics, not for targeted advertising.

On iOS 14.5 and later, Apple's App Tracking Transparency (ATT) framework requires Apps to request your explicit permission before accessing your IDFA for purposes that constitute "tracking" as defined by Apple. Where our Apps access the IDFA, we will request ATT permission in addition to any GDPR consent. If you decline ATT permission, the IDFA will not be accessed, though the IDFV (which does not require ATT consent) may still be collected for diagnostic purposes.

On Android, you can reset or opt out of the advertising ID at any time through your device's Google Settings. If you opt out, our Apps will not access your advertising ID.

3. How we use your data

We use the data we collect for the following purposes:

(a) providing and operating the App's core features (for example, indoor positioning, wayfinding, or badge scanning);

(b) improving and calibrating CC's positioning technology using diagnostic data;

(c) analysing App usage to improve the user experience;

(d) providing technical support and responding to your enquiries;

(e) communicating important updates about the App (such as security patches or feature changes);

(f) complying with legal obligations; and

(g) where you use the App in connection with a third party's service, providing location and analytics services to that third party as described in their privacy notice.

4. Legal basis for processing

We rely on the following legal bases under the UK GDPR:

Consent (Article 6(1)(a)): For the collection of location data through the App (Article 6(1)(a) UK GDPR). Where location data may reveal special category information (see section 2.4), we additionally rely on your explicit consent under Article 9(2)(a) UK GDPR. You may withdraw either consent at any time.

Legitimate interests (Article 6(1)(f)): For collecting diagnostic data to improve and calibrate our positioning technology, and for collecting usage data to improve the App experience. Our legitimate interest is maintaining and improving the quality and accuracy of our technology.

Contract performance (Article 6(1)(b)): Where the App is provided as part of a service (for example, wayfinding at an event), processing your data is necessary to perform the service you have requested.

Legal obligation (Article 6(1)(c)): Where we are required to process data to comply with applicable law.

5. How we share your data

We may share your data with:

Service operators: Where you use the App in connection with a third party's service (such as an event or venue), we share location and usage data with that third party as their data processor. They determine how your data is used. Please refer to their privacy notice.

Cloud infrastructure providers: We use cloud hosting services (such as Amazon Web Services) to store and process data. These providers act as our sub-processors and are bound by contractual safeguards.

Analytics providers: We may use third-party analytics tools to help us understand App usage patterns. Data shared with analytics providers is anonymised or aggregated where possible.

Legal requirements: We may disclose data where required by law, regulation, or legal process.

Business transfers: In the event of a merger, acquisition, or sale of assets, your data may be transferred from us to the acquiring entity.

We do not sell your personal data to third parties.

6. International transfers

Your data may be transferred to and processed in countries outside the United Kingdom. Where we transfer data internationally, we ensure appropriate safeguards are in place, including:

(a) transfers to countries that the UK Government has determined provide an adequate level of data protection;

(b) the UK International Data Transfer Agreement (IDTA); or

(c) the UK Addendum to the EU Standard Contractual Clauses.

You may request a copy of the relevant transfer safeguards by contacting us at datasecurity@crowdconnected.com.

7. Data security

We implement appropriate technical and organisational measures to protect your data, including encryption of data in transit and at rest, access controls, regular security testing, and incident response procedures. For further details, please refer to our Information Security Policy.

While we take reasonable steps to protect your data, no method of electronic transmission or storage is completely secure. We cannot guarantee the absolute security of your data.

8. Data retention

We retain your personal data only for as long as reasonably necessary to fulfil the purposes for which it was collected, as described in this policy. In determining the appropriate retention period for each category of data, we consider:

(a) the nature and sensitivity of the data;

(b) the purposes for which we process it;

(c) whether we can achieve those purposes through other means;

(d) applicable legal, regulatory, and contractual requirements; and

(e) the potential risk of harm from unauthorised use or disclosure.

Location data collected through the Apps is retained for a limited period following the conclusion of the relevant event or service, after which it is anonymised. Diagnostic and usage data may be retained in anonymised or aggregated form for technology improvement purposes. Where you exercise your right to erasure, we will delete your personal data in accordance with our obligations under UK GDPR, subject to any overriding legal basis for continued processing.

We may retain data for longer periods where required by law or where necessary to establish, exercise, or defend legal claims.

9. Your rights

Under the UK GDPR, you have the following rights in relation to your personal data:

Right of access: You have the right to request a copy of the personal data we hold about you.

Right to rectification: You have the right to request correction of inaccurate or incomplete personal data.

Right to erasure: You have the right to request deletion of your personal data in certain circumstances.

Right to restriction: You have the right to request that we restrict processing of your personal data in certain circumstances.

Right to data portability: You have the right to receive your personal data in a structured, commonly used, machine-readable format.

Right to object: You have the right to object to processing based on legitimate interests.

Right to withdraw consent: Where processing is based on consent (such as location data collection), you may withdraw consent at any time without affecting the lawfulness of processing carried out before withdrawal.

To exercise any of these rights, please contact us at mail@crowdconnected.com.

Please note: where you use a CC App in connection with a service operated by a third party (such as an event organiser or venue operator), that third party is the data controller for your personal data collected in that context. Requests relating to access, erasure, restriction or portability of that data should be directed to that organisation, not to CC. CC, as data processor in those deployments, will refer any data subject requests it receives to the relevant

data controller and will cooperate with that controller's response in accordance with our Data Processing Addendum.

You also have the right to lodge a complaint with the Information Commissioner's Office (ICO) if you believe your data protection rights have been violated. The ICO can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF; telephone: 0303 123 1113; website: ico.org.uk.

10. Children's privacy

Our Apps are not directed at children under the age of 18. However, CC's Apps may be used at events — including at family-oriented venues — where children under 18 may be present and may use a device on which an App is installed. CC is subject to the UK Age Appropriate Design Code (Children's Code) to the extent its Apps are "likely to be accessed by children" as defined by that Code. Where a deployment is known to involve a venue or event with significant attendance by under-18s, CC will implement higher default privacy settings, will not collect or process data beyond what is strictly necessary for the core positioning service, and will not use advertising IDs or any form of profiling in that context. If you believe a child under 18 has had their data collected through a CC App without appropriate consent, please contact us at legal@crowdconnected.com.

11. Changes to this policy

We may update this privacy policy from time to time. We will notify you of material changes by posting the updated policy within the App with a new version number and effective date. We encourage you to review this policy periodically.

12. Contact us

If you have any questions about this privacy policy or our data practices, please contact us at:

Email: legal@crowdconnected.com

Postal Address: FAO the Data Protection Officer, Crowd Connected Ltd, Surrey Technology Centre, Guildford, GU2 7YG, United Kingdom