Crowd Connected
Console Privacy Policy

Version 2.0
April 2026

1. Introduction

The CC Console is a web application owned and operated by Crowd Connected Ltd ("**Crowd Connected**", "**we**", "**us**", or "**our**"), a company registered in England (number 08417106) with offices at Surrey Technology Centre, Guildford, GU2 7YG, United Kingdom.

Crowd Connected is committed to protecting and respecting your privacy. We accept the responsibility that comes with processing personal data, including communicating transparently with you and adhering to good industry practice in relation to data security.

In this privacy policy ("**Policy**") we set out how we collect and use your personal data through your use of the CC Console, and the rights you have in relation to your personal data.

By "personal data" we mean identifiable information about you, like your name, company, email, address, telephone number, support queries, and so on. If we cannot identify you (for example, when your personal data has been aggregated and anonymised) then this Policy does not apply.

For UK and European Union data protection purposes, Crowd Connected acts as a controller in relation to your personal data collected through the CC Console. This is distinct from our role as a data processor when processing certain data on behalf of our customers collected via mobile applications or sensors. This processing is separately covered, as applicable, by our Mobile App Privacy Policy and the Data Processing Addendum agreed with each customer.

2. How we collect your data

This Policy applies to the CC Console (web application) only. We collect personal data as follows:

Provided directly by you

Your company or you may provide personal data to us, for example when a user login is created for you for the CC Console, when contacting us, or when requesting support. If this personal data is not provided, it will mean you cannot use certain features – for example, each user of the CC Console needs to be identifiable.

Collected automatically

We use industry-standard technologies to collect certain information automatically when you access the CC Console, including your IP address, device type, web browser, operating system, pages visited, session durations, and links you click. This information helps us provide the functionality in the Console, and to record what is being used so we can continue to improve it.

Some of this information is collected using cookies (small text files stored on your device) and similar tracking technologies.

We only use strictly necessary cookies: These are essential to the operation of the CC Console, including the authentication cookies set by AWS Cognito to manage your login session. These cookies do not require your consent as they are necessary for the delivery of a service you have requested.

From third parties

On occasions we may obtain personal data about you from other sources, such as publicly available materials or trusted third parties. We may use this information combined with other data in order to better inform, personalise and improve our services, and/or to validate the personal data you provide.

3. Legal basis for processing

We only process your personal data where we have a lawful basis for doing so. The table below sets out each processing activity, the categories of personal data involved, our lawful basis under UK GDPR Article 6, and (where we rely on legitimate interests) identifies those interests.

We do not use your personal data to make automated decisions that produce legal or similarly significant effects concerning you. We do not engage in profiling of CC Console users for the purposes of Art. 22 UK GDPR.

Processing activity	Categories of personal data	Legal basis	Legitimate interests (where applicable)
Creating and managing your user account on the CC Console	Name, work email address, employer, job title, password (hashed)	Art. 6(1)(b) — necessary for performance of our contract with you or your company	—
Providing the CC Console and associated support	Name, email, usage data, support query content	Art. 6(1)(b) — necessary for performance of our contract	—
User access logs and audit trails	IP address, login timestamps, session identifiers, actions taken within the Console	Art. 6(1)(f) — legitimate interests	Maintaining the security and integrity of the CC Console; detecting and investigating unauthorised access; complying with enterprise security obligations to our customers
Analytics and performance monitoring (non-essential cookies and usage tracking)	IP address (truncated), device/browser type, pages visited, session duration, feature usage	Art. 6(1)(a) — consent (where using analytics cookies) or Art. 6(1)(f) — legitimate interests (where using server-side analytics without cookies)	Improving the functionality and user experience of the CC Console; understanding how features are used
Sending service communications (account notices, technical alerts, product updates)	Name, work email address	Art. 6(1)(b) — necessary for performance of our contract, or Art. 6(1)(f) — legitimate interests	Keeping users informed of changes that affect their use of the CC Console
Sending marketing communications about Crowd Connected products and services	Name, work email address	Art. 6(1)(a) — consent; or Art. 6(1)(f) — legitimate interests	Promoting our products and services to existing and prospective customers

Processing activity	Categories of personal data	Legal basis	Legitimate interests (where applicable)
Fraud and abuse detection; security monitoring	IP address, login metadata, usage patterns	Art. 6(1)(f) — legitimate interests	Protecting the security and integrity of the CC Console and the data of our customers; preventing misuse of our services
Compliance with legal obligations (e.g., responding to lawful requests from authorities)	As required by the relevant legal obligation	Art. 6(1)(c) — legal obligation	—
Business transfers (sharing data with a buyer in a merger or acquisition)	All categories held at the time	Art. 6(1)(f) — legitimate interests	Enabling lawful corporate transactions

Where we rely on legitimate interests as our legal basis, we have carried out a legitimate interests assessment to ensure that our interests are not overridden by your rights and freedoms. You have the right to object to processing based on legitimate interests at any time — see section 8.

4. How and why we share your data

We share your personal data only to the extent necessary for the purposes set out in section 3. Our third-party recipients are set out in the table below. All processors are bound by data processing agreements that require them to process your data only on our instructions and in compliance with applicable data protection law.

Recipient	Role	Data shared	Location	Transfer safeguard
Amazon Web Services	Cloud infrastructure and hosting provider (AWS Cognito for authentication; AWS infrastructure for hosting the CC Console and associated databases)	All Console user data including account details, session data, access logs	USA	UK International Data Transfer Agreement (IDTA) / EU Standard Contractual Clauses; AWS also participates in the UK-US Data Bridge where applicable
Heap	Usage analytics and performance monitoring	IP address (truncated or hashed), session metadata, feature interaction data	USA	SCCs / IDTA / adequacy decision as applicable

Recipient	Role	Data shared	Location	Transfer safeguard
Atlassian HubSpot	Customer support, marketing automation, and CRM	Name, work email, support query content, email interaction data	USA	SCCs / IDTA / UK-US Data Bridge as applicable
Google, HubSpot	Transactional and marketing email delivery	Name, work email address	USA	SCCs / IDTA as applicable
Professional advisors (lawyers, accountants, auditors)	Legal, financial and compliance services	As required on a case-by-case basis	UK	No transfer outside UK
Regulatory authorities, law enforcement, courts	Compliance with legal obligations	As required by the applicable legal obligation	Variable	Relies on Art. 6(1)(c) legal obligation basis; transfer safeguards applied where required
Actual or prospective acquirers of Crowd Connected's business	Business transfer	All categories held at the time	Variable	Contractual protections; SCCs / IDTA as required

We do not sell, rent or otherwise make your personal data available to third parties for their own marketing purposes.

5. International data transfers

When we share data with authorised third parties, this may entail a transfer of your personal data from the United Kingdom or European Economic Area ("EEA") to a country outside these territories.

Where your personal data is transferred outside the UK or EEA, it will only be transferred to:

(a) countries that have been identified as providing an adequate level of protection for personal data; or

(b) a third party where we have approved transfer mechanisms in place to protect your personal data, such as the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or the EU Standard Contractual Clauses (as applicable).

The principal international transfers arising from our use of the third-party services listed in section 4 are transfers to the United States of America. These transfers are protected by the UK International Data Transfer Agreement (IDTA) and/or the UK Addendum to the EU Standard Contractual Clauses entered into with the relevant service providers. Where a provider participates in the UK-US Data Bridge (established under the UK Extension to the

EU-US Data Privacy Framework), we may rely on that mechanism instead. Copies of the relevant transfer safeguards are available on request.

For further information about international transfers, please contact us using the details in section 9.

6. How we protect your data

We take data security seriously. We implement reasonable administrative, technical and physical measures to protect your personal information against the loss, misuse and alteration of your personal data.

Our technical and organisational security measures are described in detail in the Crowd Connected Information Security Policy (a copy is available on request).

We do not sell, rent, distribute or otherwise make your personal data commercially available to any third party, except for sharing with our service providers strictly for the purposes set out in section 4.

7. How long we retain your data

We will retain your personal data for as long as we have a relationship with you (for example, because your company is a current customer) and for a period of time afterwards where we have an ongoing business need to retain it, in accordance with our data retention policies and practices.

Following termination of your account, we will delete or anonymise your personal data within 90 days, unless we are required by law to retain it for a longer period.

8. Your rights

Under UK and EU data protection law, you have the following rights in relation to your personal data:

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

(b) Right to rectification: you have the right to have any inaccurate personal data corrected and any incomplete personal data completed.

(c) Right to erasure: you have the right to request that we delete your personal data in certain circumstances.

(d) Right to restrict processing: you have the right to request that we restrict the processing of your personal data in certain circumstances.

(e) Right to data portability: you have the right to receive your personal data in a structured, commonly used and machine-readable format in certain circumstances.

(f) Right to object: you have the right to object to the processing of your personal data in certain circumstances, including where we process it for direct marketing purposes.

(g) Right to withdraw consent: where we rely on your consent to process your personal data, you have the right to withdraw that consent at any time.

If you receive marketing materials from us, you may withdraw your consent at any time and free of charge by following the unsubscribe instructions in the communication or by contacting us using the details in section 9.

To exercise any of your rights, please contact us using the details in section 9. We may require further information from you to verify your identity before disclosing any personal data. We will respond to your request within one month, as required by law.

You also have the right to lodge a complaint with the Information Commissioner's Office (ICO) if you believe that we have not complied with data protection law. The ICO can be contacted at https://ico.org.uk.

9. Changes to this Policy and contact information

From time to time, we may update this Policy. Changes are effective as of the date given at the start of this Policy. If there are material changes to this Policy or in how Crowd Connected will use your personal data, we will notify you either by prominently posting an announcement before the changes take effect, or by directly sending you a notification.

If you have any questions about this Policy, or if you would like to exercise your rights as described in section 8, you may contact us at:

Crowd Connected Ltd

FAO: Data Protection Officer

Surrey Technology Centre, Guildford, GU2 7YG, United Kingdom

Email: legal@crowdconnected.com