Crowd Connected Ltd

Information Security Policy

v5.0, February 2026

1. Introduction

Crowd Connected provides indoor positioning, tag tracking, and occupancy counting services. We collect, process, and store data on behalf of our customers to deliver these location-based services. This document details the technical and organisational measures we maintain to protect that data.

This document is intended for customers and prospective customers conducting security due diligence. It should be read alongside our standard terms and conditions (specifically section 7), our Data Processing Addendum (where applicable), our Service Level Agreement, and our Console Privacy Policy.

We recognise that the security measures described here reflect our current operational scale and maturity. Where our practices differ from enterprise-grade frameworks such as ISO 27001 or SOC 2, we are transparent about this. Our approach is proportionate to the nature of the data we handle which is, by design, pseudonymised or anonymous.

2. Data we process

Understanding what data Crowd Connected handles is essential context for evaluating our security posture. We process several categories of data, each with different characteristics and sensitivity levels.

2.1 Location and place data

This is the core data our products generate. We collect it as processor on behalf of our customers (who act as controller). It falls into three distinct types:

Mobile app location data. Our SDK, embedded in a customer's mobile application, generates a random identifier for each app installation and transmits coordinates to our platform. No MAC addresses or IP addresses are stored. Customers may optionally pass their own identifiers ("aliases") but are contractually prohibited from sending directly identifiable personal data.

Device information. For each SDK installation, we collect basic information about the device, including hardware model and operating system version. This data is used for debugging and support purposes. It does not contain sufficient detail to fingerprint or uniquely identify a specific device.

Diagnostic data. We collect diagnostic data from the SDK for debugging and service improvement. This data supports the development and refinement of our positioning algorithms and is not capable of identifying individuals.

Tag tracking data. For hardware-based tracking (such as conference badges or asset tags), each tag is assigned a random identifier by Crowd Connected. The system records "place observations" based on proximity to sensors. Customers may assign aliases to tags. The same contractual prohibition on sending identifiable data applies.

Counting data. Our occupancy counting product detects devices using one-way hashed, rotating MAC addresses. The hashing occurs on the sensor itself before any data is transmitted. Crowd Connected never stores or transmits actual MAC addresses. This data is purely aggregate.

In all cases, Crowd Connected's architecture is designed so that we do not hold data that can identify individuals. Identifiers are random or hashed, and we cannot reverse them. Our contractual terms reinforce this by prohibiting customers from sending directly identifiable data to our platform.

2.2 Console user account data

People who use our web-based console have user accounts with email addresses, names, and login credentials. Crowd Connected acts as controller for this data, as we determine how it is collected and used. This data is covered by our Console Privacy Policy.

2.3 Customer-generated content

Customers create content within our console including map regions, zone names, geofences, floor plan references, and other configuration data. While typically not personal data, this content may be commercially sensitive or confidential. Crowd Connected processes it on behalf of the customer.

2.4 Operational data

We generate and retain system logs, API call records, and monitoring data for operational and security purposes. Crowd Connected acts as controller for this data.

2.5 Our privacy position

For location and place data, our position is that the data we process does not constitute personal data in most circumstances, because Crowd Connected cannot identify individuals from the random or hashed identifiers we hold. The customer, as controller, may be able to correlate identifiers with individuals using their own systems, but Crowd Connected cannot.

This distinction is important because it means that data subject access requests and similar rights under UK GDPR would typically be directed to the customer (as controller), not to Crowd Connected. We will, however, assist customers in responding to such requests in accordance with our contractual obligations.

3. Regulatory framework

Crowd Connected is a UK company and operates primarily under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Where we process data on behalf of customers in the European Economic Area, we also comply with the EU GDPR.

Our Data Processing Addendum sets out the contractual framework governing our role as processor, including obligations around data security, sub-processor management, international data transfers, and cooperation with data subject requests.

Crowd Connected is registered with the Information Commissioner’s Office as a data controller (registration number ZB426584). Our Data Protection Officer is Mark Maydon, contactable at datasecurity@crowdconnected.com.

4. Cloud infrastructure

Crowd Connected’s platform is deployed on Amazon Web Services (AWS), using services including Amazon EC2, Amazon API Gateway, Amazon Lambdas, Amazon S3, Amazon EFS, Amazon DynamoDB, and Amazon Kinesis.

AWS maintains an extensive compliance programme, including ISO 27001, SOC 2, and numerous other certifications. Full details of AWS’s security posture and certifications are available at aws.amazon.com/security and aws.amazon.com/compliance.

4.1 Data location

All customer data is currently hosted in AWS’s US region. This applies to all customers regardless of their geographic location.

For customers in the European Economic Area and the United Kingdom, international data transfers are governed by appropriate transfer mechanisms as set out in our Data Processing Addendum.

These may include the EU Standard Contractual Clauses, the UK International Data Transfer Agreement (IDTA), and reliance on AWS's own compliance certifications (including participation in data privacy frameworks).

4.2 Physical security

AWS data centres are managed by Amazon with comprehensive physical security controls including professional security staff, video surveillance, intrusion detection systems, multi-factor authentication for data centre access, and routine access auditing. Full details are published in AWS's compliance documentation.

Crowd Connected's office premises are secured with electronic pass-card access, 24/7 building security, and controlled visitor access. Staff are required to secure all devices with password-protected access.

5. Data security

5.1 Encryption

In transit: All data transmitted over the internet uses Transport Layer Security (TLS) encryption.

At rest: All data stored in S3, EC2, and DynamoDB is encrypted using AES-256-XTS.

5.2 Network security

AWS provides a comprehensive firewall solution. EC2 instances are configured with a default-deny inbound firewall, requiring explicit configuration to allow any inbound traffic. Traffic is restricted by protocol, port, and source IP address.

AWS's infrastructure includes protections against distributed denial of service (DDoS) attacks, man-in-the-middle (MITM) attacks, IP spoofing, port scanning, and packet sniffing between tenants.

5.3 Access control

Access to infrastructure and data is managed at multiple levels:

AWS infrastructure: Root credentials are restricted and always protected with multi-factor authentication. Other AWS credentials and keys are limited, monitored, and auditable.

Server access: SSH access to EC2 servers is disabled by default using AWS security groups. When temporarily required for testing or debugging, access is restricted by IP address to Crowd Connected's office, uses key-based authentication only (no passwords), and uses non-root logins.

API access: Access to Crowd Connected's APIs is authenticated via username/password or API key pair. Passwords and secret keys are stored encrypted and never exposed in plain text. All API activity is logged and auditable at user level. Minimum password standards are enforced.

Console access: The web console requires a minimum 12-character password. Customers can manage user accounts within their organisation. Two access levels are available: a privileged role (with the ability to create and manage other user accounts) and a standard role (full read/write access to data and configuration, without user management capabilities).

5.4 Backups

S3 data benefits from 99.99% durability, with versioning enabled where required to allow restoration in the event of accidental deletion. DynamoDB tables have point-in-time recovery enabled where required.

Our Business Continuity and Disaster Recovery Policy provides further detail on backup and recovery procedures. This document is available to customers on request.

6. Software security

6.1 Secure development

Crowd Connected maintains documented change control procedures for its codebase. Our development practices include code review, version control, and testing before deployment to production.

6.2 Application security

The web console is secured using AWS Cognito for user authentication. Once authenticated, Cognito authorises the web application to access backend APIs running on AWS API Gateway. Self-service password reset is available through Cognito.

6.3 Vulnerability management

We do not currently conduct formal penetration testing. We recognise that this is an area where our practices could be strengthened, and we are evaluating options for implementing regular vulnerability assessment and penetration testing.

We rely on AWS's infrastructure-level security scanning and patching, and we apply security updates to our application components as they become available.

7. Monitoring and logging

AWS CloudTrail is used to log every AWS API call, providing a complete audit trail of infrastructure activity.

All Crowd Connected API activity is logged and monitored. Logs are retained for operational and security purposes and may be used for forensic analysis in the event of a security incident.

8. People and organisation

8.1 Pre-employment screening

Crowd Connected applies pre-employment screening appropriate to the role and level of access.

8.2 Security awareness

All staff are provided with the employee handbook on joining, which covers data handling, security expectations, and acceptable use policies. Employee access to systems and customer data is limited to what is required for their role.

8.3 Internal access management

Access to customer data is granted on an as-needed basis for support purposes. Crowd Connected's directors have overall responsibility for data security and set the company's security policies.

9. Incident response

Data security is the responsibility of Crowd Connected's directors.

9.1 Notification

Should Crowd Connected become aware of any security incident that affects or is reasonably likely to affect a customer's data, we will notify the affected customer without undue delay and in any event within 24 hours of becoming aware of the incident.

The notification will include, to the extent available at the time:

- A description of the nature of the incident
- The categories and approximate volume of data affected
- The likely consequences of the incident
- The measures taken or proposed to address the incident and mitigate its effects

We will provide updates on any material developments as the investigation progresses.

9.2 Regulatory obligations

Where applicable, Crowd Connected will cooperate with customers in meeting their obligations to notify supervisory authorities (within 72 hours under UK GDPR) and affected data subjects. Any assistance beyond providing information reasonably available to Crowd Connected shall be provided on a reasonable time and materials basis.

9.3 Contact

To report a security incident or concern, contact datasecurity@crowdconnected.com. We will conduct a thorough review and provide findings to the reporting party.

10. Sub-processors

The following third parties process customer data on Crowd Connected's behalf:

Sub-processor	Purpose	Data processed	Location
Amazon Web Services (AWS)	Infrastructure, data processing and storage	Location data, tag data, counting data, device information, diagnostic data, console data	United States

Other tools used by Crowd Connected for internal operations (such as email, project management, and customer relationship management) do not process customer location or place data.

Changes to our sub-processor arrangements are governed by our Data Processing Addendum.

11. Business continuity and disaster recovery

Crowd Connected maintains a Business Continuity and Disaster Recovery Policy. Our platform is deployed in a single AWS availability zone, and we use AWS's built-in redundancy and recovery mechanisms (including S3 durability and DynamoDB point-in-time recovery) to protect against data loss.

We acknowledge that a single availability zone deployment carries inherent risk. Our BCDR policy documents our recovery procedures and is available to customers on request.

12. Compliance and certifications

Crowd Connected does not currently hold company-level security certifications such as ISO 27001 or SOC 2. We rely on AWS's extensive certification programme for infrastructure-level assurance.

We maintain the following:

- Compliance with UK GDPR and the Data Protection Act 2018
- Registration with the Information Commissioner's Office as a data controller (ZB426584)

- Professional Indemnity insurance
- Employers' Liability insurance
- Public Liability insurance
- Product Liability insurance

We recognise that company-level certifications are increasingly expected by larger customers and are evaluating the most appropriate path for our business.

13. Data retention and deletion

Customer location and place data is retained for the duration of the service agreement. Data is deleted on customer request.

Console user account data is retained for as long as the account is active and for a reasonable period afterwards in line with our Console Privacy Policy.

Operational logs are retained for a period appropriate to their operational and security purpose.

Specific retention and deletion obligations may be set out in individual customer contracts or Data Processing Addenda.

14. Related documents

This document should be read alongside:

- Crowd Connected Service Terms and Conditions (section 7 in particular)
- Crowd Connected Data Processing Addendum
- Crowd Connected Service Level Agreement
- Crowd Connected Console Privacy Policy
- Crowd Connected Business Continuity and Disaster Recovery Policy (available on request)

v5.0, February 2026

Crowd Connected Ltd | Surrey Technology Centre, Occam Road, Guildford, GU2 7YG, UK
datasecurity@crowdconnected.com