

GGK TECHNOLOGIES

Data Protection & UK GDPR Statement

Public-facing summary of how GGK protects personal information

PUBLIC DOCUMENT | Version 1.0 | Effective September 2026

Garden Gate Keeper (GGK) is an incident, accident and near-miss reporting and management platform for organisations. This statement explains GGK's approach to UK GDPR, including the different roles GGK and its customers have when personal information is processed through the service.

This document is intended for customers, prospective customers, procurement teams and other website visitors.

1. About this statement

This public statement describes GGK Technologies' data-protection approach at a practical, high level. It is designed to support customer due diligence and to explain how GGK applies the UK GDPR when operating the GGK service.

It complements GGK's Privacy Notice and Data Retention & Deletion Policy. It does not replace a customer organisation's own employee, contractor or workplace privacy information, and it does not disclose confidential security architecture or internal operational records.

The detailed Record of Processing Activities (ROPA), internal data map, supplier assessments, backup design and security-control records are maintained internally rather than published on the website.

2. Controller and processor roles

GGK may act in two different data-protection roles depending on why personal information is being processed.

Situation	Normal role	What this means
Customer incident, accident and near-miss records	Customer = Data Controller GGK = Data Processor	The customer determines why the information is collected, the applicable lawful basis, relevant special-category condition and appropriate retention requirements. GGK processes the information to provide the service and on the customer's instructions.
GGK's own business information	GGK = Data Controller	For website enquiries, prospective-customer information, customer contacts, account administration, service security and similar business records, GGK determines its own processing purposes and responsibilities.

3. Information that may be processed

Depending on how a customer configures and uses GGK, the platform may process information such as:

- Names, contact details, email addresses, employee or user information, departments and workplace/site information.
- Incident location, date and time, reporting-person details, impacted-person details and witness information.
- Incident descriptions, accident and near-miss information, investigation notes, findings, status history and attachments or evidence.

- Injury or harm information, affected body parts, medical treatment information and first-aider information.
- User-account information, roles, permissions, login/security information, IP address, session information, access records and audit logs.
- Website enquiry information, organisation details, correspondence, customer administration and support information.

4. Health and other special-category information

Incident-management records can contain information concerning an individual's health.

Examples include injuries, treatment, affected body parts, health consequences and other medical information included in an incident record. Health information is Special Category Personal Data under UK data-protection law.

Where GGK processes this information for a customer, the customer remains responsible for identifying the appropriate Article 6 lawful basis and Article 9 condition. GGK processes the information only as required to provide the service, in accordance with customer instructions and applicable contractual requirements.

GGK applies a data-minimisation approach to sensitive information. Access, reports, exports, support activity and notification content should contain only the information reasonably required for the relevant purpose.

5. UK GDPR principles

GGK's data-protection approach is based on the core UK GDPR principles:

- Lawfulness, fairness and transparency - personal data must be handled for an identified purpose and with an appropriate legal basis or valid processor instruction.
- Purpose limitation - information should not be reused for unrelated purposes without proper assessment and authority.
- Data minimisation - GGK aims to collect, display, transmit and retain only information reasonably necessary for the purpose.
- Accuracy - reasonable mechanisms and procedures are used to support correction of inaccurate information where appropriate.
- Storage limitation - information is not kept longer than necessary, subject to customer requirements and legal, regulatory, contractual or security needs.
- Integrity and confidentiality - appropriate technical and organisational measures are used to protect information against unauthorised access, loss, alteration, disclosure or misuse.
- Accountability - GGK maintains policies, registers, supplier assessments, contractual controls and review records to demonstrate its data-protection approach.

6. Why personal information is processed

- Enabling incidents, accidents and near misses to be reported and managed.
- Identifying affected persons, witnesses and relevant workplace locations.
- Recording injury, treatment and investigation information.
- Assigning and managing investigations, status updates and audit history.
- Producing reports and dashboards to support health and safety management and regulatory or legal reporting requirements.
- Administering user accounts, permissions and access.
- Maintaining the security and integrity of the service and investigating suspected misuse.
- Providing customer support and operating the service.
- Responding to website enquiries, arranging demonstrations and managing customer or prospective-customer relationships.

7. Lawful bases

When GGK acts as Data Controller, the lawful basis depends on the purpose. Relevant bases may include contract, legal obligation and legitimate interests. Consent may be used where it is appropriate and legally required.

When GGK acts solely as Data Processor for customer incident information, GGK does not determine the customer's lawful basis. The customer, as Data Controller, is responsible for that decision.

8. Security and access controls

GGK takes reasonable technical and organisational measures designed to protect personal information against unauthorised access, accidental loss, destruction, alteration, unauthorised disclosure and misuse.

- Customer information is restricted through user accounts, roles and permissions.
- GGK maintains security and audit information to help detect, investigate and respond to suspicious or unauthorised activity.
- Core application and database services are operated on GGK-controlled infrastructure in the United Kingdom.
- Backups are maintained for business continuity and disaster recovery and are subject to controlled retention and secure disposal arrangements.
- Access by GGK personnel to customer information is limited to circumstances where it is reasonably necessary for support, maintenance, security, service integrity or legal obligations.
- Security controls and architecture are reviewed internally and are not published in operational detail.

9. Retention and deletion

Retention of customer incident information is primarily determined by the customer and its legal, regulatory and operational requirements. GGK retains customer information for the period necessary to provide the contracted service and in accordance with customer instructions and agreed arrangements.

When a customer's service ends, GGK intends to provide a reasonable opportunity for the customer to export information it requires. Customer information held in active production systems is normally scheduled for deletion within 90 days of termination, unless another contractual arrangement, legal requirement or retention hold applies.

Deleted information may remain temporarily in historical backups until those backups reach the end of their normal retention cycle. Backups are not ordinarily modified record-by-record because doing so may affect backup integrity. Information retained solely for legal, regulatory, contractual or security purposes is not used for unrelated purposes.

10. Service providers, sub-processors and international transfers

GGK reviews external suppliers that may process personal information on its behalf and maintains an internal sub-processor register. Appropriate contractual and data-protection terms are used where required.

The core GGK application and SQL database are hosted on GGK-controlled infrastructure in the United Kingdom. Some supporting services, such as email delivery or business communications, may involve processing in other jurisdictions. Where an international transfer of personal data is relevant, GGK will use an appropriate mechanism or safeguard required by UK data-protection law, such as an adequacy arrangement or applicable contractual transfer safeguards.

GGK aims to minimise the personal and sensitive information passed through supporting services, particularly where notifications can be delivered without including full incident details.

11. Individual rights and requests

Depending on the circumstances, individuals may have rights under UK data-protection law including access, correction, deletion, restriction, data portability, objection and rights relating to automated decision-making and profiling. These rights are not absolute and depend on the circumstances and lawful basis.

If information has been entered into GGK by an employer or another organisation, that organisation will normally be the Data Controller. Individuals should therefore normally contact that organisation first. If GGK receives a request concerning customer-controlled information, GGK may refer it to the relevant customer and will provide reasonable assistance where required.

Where GGK is itself the Data Controller, requests will be handled in accordance with GGK's Privacy Notice and applicable UK data-protection law.

12. Personal data breaches

GGK maintains procedures for identifying, assessing and responding to suspected personal-data breaches. Where GGK is acting as a Data Processor and becomes aware of a relevant breach affecting customer data, GGK will notify the customer without undue delay in accordance with applicable law and contractual requirements and will provide reasonable information to support the customer's assessment and response.

Where GGK acts as Data Controller, GGK will assess whether notification to the Information Commissioner's Office or affected individuals is required under UK data-protection law.

13. Accountability, privacy by design and review

- GGK maintains internal records of processing activities and a data map covering its principal processing activities.
- New features and significant changes are considered from a data-minimisation and privacy-by-design perspective.
- New suppliers and material changes to processing, hosting, transfers or data categories are reviewed before or as part of implementation.
- High-risk processing or significant changes involving sensitive information are assessed to determine whether a Data Protection Impact Assessment is required.
- Policies and registers are reviewed periodically and following significant legal, technical, contractual or service changes.

14. Customer responsibilities

Customers using GGK remain responsible for their own compliance obligations where they are the Data Controller. This includes deciding:

- why personal information is collected and the lawful basis for processing;
- which Article 9 condition applies where special-category health information is processed;
- who should have access to incident and investigation information;
- how long incident, health and safety, personnel and investigation records should be retained;
- whether information is subject to legal, regulatory, insurance, investigation or litigation holds; and
- what privacy information should be provided to employees, contractors, clients and other affected individuals.

15. Questions, concerns and complaints

Questions about GGK's approach to data protection can be submitted through the contact form on the GGK Technologies website. Where a concern relates to information controlled by a GGK customer, the relevant customer organisation will normally be the appropriate first point of contact.

Individuals also have the right to raise concerns with the UK supervisory authority, the Information Commissioner's Office (ICO).

Website	https://ggktechnologies.net/
Contact form	https://ggktechnologies.net/#contact
UK supervisory authority	Information Commissioner's Office (ICO)
ICO website	https://ico.org.uk/

16. Changes to this statement

GGK may update this statement to reflect changes to the service, suppliers, legal requirements or the way personal information is processed. The latest public version should be made available through the GGK Technologies website.

Last updated: September 2026 | Version 1.0