

GGK Technologies Data Retention & Deletion Policy

Version 1.0

Effective Date: September 2026

GGK Technologies Data Retention & Deletion Policy

Version 1.0

Effective Date: September 2026

1. Purpose

GGK Technologies is committed to ensuring that personal information and other customer data is retained only for as long as it is required.

This policy explains how GGK determines appropriate retention periods, how information is securely deleted when it is no longer required, and what happens to customer information when a customer stops using the GGK service.

GGK applies the principle that personal data should not be kept for longer than is necessary for the purpose for which it was collected, while recognising that certain information may need to be retained for legal, regulatory, contractual, security or evidential reasons.

2. Scope

This policy applies to information processed by GGK Technologies in connection with the provision and operation of the GGK platform.

This includes:

- Incident, accident and near-miss records
- User accounts
- Login and security records
- Audit history
- Customer and organisation records

- Support requests
- Emails and business correspondence
- System backups
- Records relating to former customers
- Prospect and marketing information

3. General Retention Principles

GGK follows these principles:

- Information is retained only while there is a legitimate business, contractual, legal, regulatory or security requirement.
- Retention periods must be proportionate to the reason the information is processed.
- Where the customer is responsible for determining a retention period, GGK will support the customer's requirements where technically and contractually applicable.
- Information no longer required will be deleted, anonymised or securely disposed of.
- Information subject to legal proceedings, regulatory investigation, dispute or another legal hold may be retained beyond its standard retention period.
- Data contained within backups will normally age out through the normal backup retention cycle rather than individual backup files being modified.

4. Incident, Accident and Near-Miss Records

Incident records are primarily controlled by the organisation using GGK.

Customers may need to retain health and safety records for different periods depending on the circumstances of the incident and applicable legislation.

GGK will retain active customer incident information for the duration of the customer's use of the service unless:

- the customer deletes the information;
- an agreed retention rule automatically deletes or anonymises the information; or

- another contractual arrangement applies.

Where GGK acts as a processor on behalf of a customer, the customer remains responsible for determining the appropriate legal retention period for its incident records.

5. User Accounts

User accounts are retained while the user requires access to GGK.

When an account is disabled or removed, information required for security, auditing or historical attribution may be retained where necessary.

Profile information that is no longer required should be deleted or anonymised.

6. Login and Security Logs

Login, authentication and security logs may be retained for the purposes of:

- investigating unauthorised access;
- identifying suspicious activity;
- diagnosing system problems;
- maintaining platform security; and
- providing evidence relating to security events.

The standard target retention period for routine login and security information is 12 months unless a longer period is necessary for an investigation, security incident or legal requirement.

High-volume operational logs may be retained for shorter periods.

7. Audit History

Audit information may include records of changes made to:

- incidents;

- accounts;
- permissions;
- investigations;
- statuses; and
- other significant information within GGK.

Audit history will generally be retained alongside the information to which it relates where it remains necessary to demonstrate accountability and the history of significant actions.

The standard target retention period for audit records is up to seven years, subject to customer requirements and applicable legal obligations.

8. Customer Records

Operational customer records are retained while the customer relationship remains active.

Certain financial, contractual and business records may be retained for up to seven years following termination where required for accounting, taxation, legal or contractual purposes.

9. Support Requests

Support requests and associated correspondence are normally retained for three years after closure.

Information may be retained longer where the request relates to:

- a security incident;
- a legal dispute;
- a significant software issue;
- contractual evidence; or
- another matter requiring continued retention.

10. Emails

Business correspondence is retained only while it remains relevant.

Emails connected with contracts, customer decisions, complaints, security incidents or other significant matters may be retained alongside the appropriate customer or business record.

Routine correspondence should be deleted when it is no longer required.

11. Backups

GGK maintains backups to support business continuity, disaster recovery and protection against accidental data loss.

Where information is deleted from the live GGK platform, copies may temporarily remain within historical backups.

GGK does not ordinarily modify individual historical backup files to remove specific records because doing so may affect the integrity of the backup.

Instead, backups containing deleted information are removed when they reach the end of their normal retention period.

Deleted data contained in backups must not be restored to active production systems except where necessary for legitimate disaster recovery or legal purposes.

12. Former and Deleted Customers

When a customer's GGK service ends:

- The customer should be given an opportunity to export information required for its records.
- Access to the live GGK service will be disabled following termination.
- Customer information held within production systems will normally be scheduled for deletion within 90 days of termination.
- Information may continue to exist temporarily within system backups until those backups reach the end of their retention period.
- Financial, contractual, security or other records that GGK is independently required to retain may be retained separately for the relevant legal period.
- Data retained solely for legal or regulatory purposes will not be used for unrelated purposes.

13. Prospect and Marketing Information

Information relating to prospective customers may be retained while there is a reasonable expectation of a business relationship or where the individual or organisation has requested communications from GGK.

Prospect information that has had no meaningful interaction for 24 months should normally be deleted or reviewed to determine whether continued retention is justified.

Individuals may opt out of direct marketing communications at any time.

Suppression information may be retained where necessary to ensure that an individual who has opted out is not inadvertently contacted again.

14. Customer Responsibilities

Customers using GGK may determine their own retention requirements for information entered into the system.

This is particularly relevant to:

- incident records;
- accident records;
- health and safety information;
- personnel information; and
- investigation records.

Customers remain responsible for determining:

- which laws and regulations apply to their organisation;
- how long their records should be retained;
- whether records need to be archived;
- whether data should be deleted or anonymised; and
- whether information is subject to litigation, investigation or another retention hold.

15. Authorisation of Deletion

Routine deletion carried out in accordance with an approved retention rule does not require individual approval for each record.

Deletion outside established retention rules must be authorised by an appropriately authorised person within GGK.

This may include:

- the owner or authorised senior representative of GGK Technologies;
- an authorised system administrator;
- the person responsible for data protection; or
- another formally delegated individual.

Customer-controlled information must not intentionally be permanently deleted outside established functionality or contractual procedures without appropriate customer authorisation, except where GGK is legally required to do so.

16. Legal and Regulatory Exceptions

Normal deletion may be suspended where information is required in connection with:

- legal proceedings;
- anticipated litigation;
- insurance claims;
- regulatory investigations;
- law-enforcement requests;
- contractual disputes;
- fraud or security investigations;
- taxation or accounting requirements; or
- another applicable legal obligation.

Once the requirement no longer applies, the information should return to the normal retention

and deletion process.

17. Secure Deletion

Where information is scheduled for permanent deletion, GGK will use methods appropriate to the system and storage technology involved.

Deletion procedures should ensure that information cannot normally be recovered or accessed through the live GGK platform following deletion.

Information contained within backups will be removed through normal backup expiry.

Storage devices that are retired or replaced should be securely erased or destroyed where necessary before disposal.

18. Data Subject Requests

Where GGK receives a request relating to personal information for which a GGK customer is the data controller, GGK may refer the request to the relevant customer.

GGK will provide reasonable assistance to customers where required to locate, export, correct or delete personal information in accordance with applicable data-protection legislation.

Where GGK is itself the data controller, requests will be handled in accordance with GGK's Privacy Notice and applicable data-protection legislation.

19. Policy Review

This policy will be reviewed at least annually.

It may also be reviewed following:

- changes to data-protection legislation;
- significant changes to the GGK platform;
- new categories of information being collected;
- changes to backup arrangements;

- changes to contractual requirements;
- security incidents; or
- recommendations arising from an audit or compliance review.

20. Contact

Questions relating to data retention, deletion or data protection within GGK can be submitted through the contact form on the GGK Technologies website.