2025

KMP 009 Data Protection Policy

Published Feb 2025
Author: K Nichols
Review Date: Feb 2026
Version 17

Printed on 18 February 2025

DATA PROTECTION POLICY[1]

UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018,

Policy

Group Horizon Ltd (GHL) is committed to ensuring the security and protection of personal data that we process, and to providing a compliant and consistent approach to data protection. Our policies and procedures are designed to comply with the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices, and former employees, referred to as HR-related personal data. ***[This policy does not apply to the personal data of clients or other personal data processed for business purposes.]***

GHL has appointed Craig Roper as its data protection officer (DPO). The role is to inform and advise GHL on its data protection obligations. She can be contacted at craig.roper@grouphorizon.co.uk. Questions about this policy, or requests for further information, should be directed to the data protection officer. The designated DPO, operates independently and reports directly to the highest level of management. His responsibilities include monitoring compliance with data protection laws, providing advice on Data Protection Impact Assessments (DPIAs), and serving as the contact point for the Information Commissioner's Office (ICO

Definitions

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data Protection Law

The Data Protection Act 2018 describes how organisations must collect, handle and store personal information. These rules apply regardless of whether the data is stored electronically, on paper or other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

[1] In 2025, the United Kingdom is undergoing significant reforms to its data protection laws with the introduction of the Data (Use and Access) Bill (DUA Bill). This legislation aims to refine existing data protection frameworks, enhancing both innovation and compliance.

The UK General Data Protection Regulation is underpinned by six important principles which say that personal data must be;

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the implementation of the appropriate technical and organisational measures required by the GDPR to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organisational measures

Data protection principles

GHL processes HR-related personal data in accordance with the following data protection principles:

GHL processes personal data lawfully, fairly and in a transparent manner.

GHL collects personal data only for specified, explicit and legitimate purposes.

GHL processes personal data only where it is adequate, relevant, and limited to what is necessary for the purposes of processing.

GHL keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.

GHL keeps personal data only for the period necessary for processing.

General Guidelines

Access to data should be restricted to those who need it for their work.

Data should not be shared informally.

When access to CONFIDENTIAL or RESTRICTED data is required, employees can request it from the Managing Director.

Group Horizon Ltd will provide training to all employees to help them understand their responsibilities when handling data.

Keep all data secure, by taking sensible precautions and following the guidelines below.

All software the company provides or recommends is correctly licenced. This applies to software that has access to company or customer data.

Unless necessary, passwords should never be shared between users to maintain an audit trail.

Personal data should not be disclosed to unauthorised people, either within the company or externally.

Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it must be securely deleted or disposed of.

Statutory Retention Periods

The main UK legislation regulating statutory retention periods is summarised below. It is Group Horizon's policy to keep records for at least 6 years (5 in Scotland), to cover the time limit for bringing any civil legal action.

Record types

Accident Records:

Retention Period: At least 3 years from the date of the last entry.

Note: For accidents involving children or young adults, it's advisable to retain records until the individual reaches the age of 21, considering the Limitation Act 1980.

Accident books, accident records/reports (See below for accidents involving chemicals or asbestos)

Statutory retention period: 3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21).

Statutory authority: The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances (see below).

Accounting records

Retention Period: 6 years from the end of the financial year to which they relate.

Statutory authority: Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006.

The Coronavirus Job Retention Scheme (CJRS) concluded on 30 September 2021. However, HM Revenue & Customs (HMRC) mandates that employers retain all records pertaining to CJRS claims for a minimum of six years. This includes details such as the amounts claimed, claim periods for each employee, claim reference numbers, and calculations used to determine claim amounts. For employees who were flexibly furloughed, records should also document usual hours worked and actual hours worked, along with any related calculations.

First Aid Training Records

Statutory Retention Period: 6 years after employment ends.

Statutory Authority: Health and Safety (First-Aid) Regulations 1981**.**

Fire Warden Training Records

Statutory Retention Period: 6 years after employment ends.

Statutory Authority: Fire Precautions (Workplace) Regulations 1997.

Health and Safety Representatives and Employees' Training Records

Statutory Retention Period: 5 years after employment ends.

Statutory Authority: Health and Safety (Consultation with Employees) Regulations 1996; Health and Safety Information for Employees Regulations 1989.

Income Tax and National Insurance (NI) Returns, Income Tax Records, and Correspondence with HMRC

Statutory Retention Period: Not less than 3 years after the end of the financial year to which they relate.

Statutory Authority: The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended.

National Minimum Wage Records

- Retention Period: 3 years after the end of the pay reference period following the one that the records cover.
- Statutory Authority: National Minimum Wage Act 1998.

Payroll Wage/Salary Records (including overtime, bonuses, expenses)

- Retention Period: 6 years from the end of the tax year to which they relate.
- Statutory Authority: Taxes Management Act 1970.

Records of Tests and Examinations of Control Systems and Protective Equipment under COSHH

- Retention Period: 5 years from the date on which the tests were conducted.
- Statutory Authority: The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH).

Records Relating to Children and Young Adults

- Retention Period: Until the child/young adult reaches the age of 21.
- Statutory Authority: Limitation Act 1980.

Retirement Benefits Schemes – Records of Notifiable Events (e.g., relating to incapacity)

- Retention Period: 6 years from the end of the scheme year in which the event took place.
- Statutory Authority: The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103).

Statutory Maternity Pay Records, Calculations, Certificates (Mat B1s), or Other Medical Evidence (also applicable to Shared Parental, Paternity, and Adoption Pay Records)

- Retention Period: 3 years after the end of the tax year in which the maternity period ends.
- Statutory Authority: The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended, Maternity & Parental Leave Regulations 1999.

Subject Access Request Records

- Retention Period: While there is no specific statutory retention period mandated by the Data Protection Act 2018, it is considered best practice to retain records of subject access requests for a reasonable period to demonstrate compliance. A retention period of up to 6 years is advisable, aligning with the general limitation period for legal claims.
- Statutory Authority: Data Protection Act 2018.

VAT Deferral (COVID-19) Records

- Retention Period: 6 years.
- Statutory Authority: HMRC VAT deferral guidance.

Whistleblowing Documents

- Retention Period: For substantiated investigations, retain records for 6 years following the outcome, in line with practices observed by organizations such as the Housing Ombudsman. For unsubstantiated claims, personal data should be removed immediately.
- Statutory Authority: Public Interest Disclosure Act 1998.

Working Time Records

- Retention Period: 2 years from the date on which they were made.
- Statutory Authority: The Working Time Regulations 1998 (SI 1998/1833).

Coronavirus Job Retention Scheme Records

- Retention Period: 6 years.
- Statutory Authority: HMRC guidance on the Coronavirus Job Retention Scheme.

Data Protection Measures

- Policy Statement: GHL adopts appropriate measures to ensure that personal data is secure and protected against unauthorised or unlawful processing, as well as accidental loss, destruction, or damage.

Transparency and Legal Basis

- Policy Statement: GHL informs individuals of the reasons for processing their personal data, how such data is used, and the legal basis for processing in its privacy notices. Personal data will not be processed for other purposes. Where GHL relies on legitimate interests as the basis for processing data, an assessment will be conducted to ensure that those interests are not overridden by the rights and freedoms of individuals.

8. Processing Special Categories of Data

- Policy Statement: When processing special categories of personal data or criminal records data to perform obligations or exercise rights in employment law, GHL ensures this is done in accordance with its policy on special categories of data and criminal records data.

Data Accuracy

- Policy Statement: GHL promptly updates HR-related personal data if an individual advises that their information has changed or is inaccurate.

Personnel File Management

- Policy Statement: Personal data gathered during employment, work as a contractor or volunteer, apprenticeship, or internship is held in the individual's personnel file (in electronic format). The retention periods for HR-related personal data are specified in GHL's privacy notices to individuals.

Record of Processing Activities

- Policy Statement: GHL maintains a record of its processing activities concerning HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Data Subject Rights

Under the UK General Data Protection Regulation (UK GDPR), individuals are granted specific rights concerning their personal data. These rights are:

1. Right to be Informed: Individuals have the right to be informed about the collection and use of their personal data. This is achieved through clear and transparent privacy notices.
2. Right of Access: Individuals can request access to their personal data to understand how it is being processed.
3. Right to Rectification: Individuals can request correction of inaccurate or incomplete personal data.
4. Right to Erasure: Also known as the 'right to be forgotten', individuals can request the deletion of their personal data under certain circumstances.
5. Right to Restrict Processing: Individuals can request the limitation of their personal data processing under specific conditions.
6. Right to Data Portability: Individuals can request the transfer of their personal data to another organisation or directly to themselves.
7. Right to Object: Individuals can object to the processing of their personal data in certain situations.
8. Rights Related to Automated Decision-Making and Profiling: Individuals are protected against decisions made solely based on automated processing, including profiling, which have legal or significant effects.

Right to be Informed

GHL complies with the right to be informed by issuing a comprehensive privacy notice (KMP 009A) that details how personal data is collected, used, and managed.

Individual Rights

As data subjects, individuals have several rights regarding their personal data.

Subject Access Requests

Individuals have the right to access their personal data held by GHL. Upon receiving a subject access request, GHL will provide:

- Confirmation of whether personal data is being processed.
- Access to the personal data.
- Other supplementary information as outlined in Article 15 of the UK GDPR.

Requests should be directed to the Data Protection Officer (DPO) using GHL's designated form. GHL may require proof of identity before processing the request. Responses will be provided within one month of receipt. In cases of complex or numerous requests, this period may be extended by up to two additional months, with the individual informed of the extension and reasons within one month of the original request.

If a request is manifestly unfounded or excessive, GHL reserves the right to charge a reasonable fee or refuse to act on the request. In such cases, GHL will inform the individual of the decision and their right to complain to the Information Commissioner's Office (ICO).

Other Rights

Individuals may exercise the following rights concerning their personal data:

- Rectification: Request correction of inaccurate or incomplete data.
- Erasure: Request deletion of data when it is no longer necessary, consent is withdrawn, or processing is unlawful.
- Restriction: Request limitation of data processing under specific circumstances.
- Objection: Object to data processing based on legitimate interests or for direct marketing purposes.
- Data Portability: Request transfer of data to another controller in a structured, commonly used, and machine-readable format.

Requests should be directed to the DPO. GHL will assess and respond to such requests in accordance with the UK GDPR.

Data Security

GHL is committed to ensuring the security of personal data. Measures include:

- Implementing appropriate technical and organizational measures to protect data against unauthorised access, loss, or damage.
- Ensuring that third-party processors adhere to data protection standards through contractual agreements.

Data Storage

Personal data should primarily be stored electronically. Physical storage is permitted only when essential or legally required. Security measures include:

- Using strong, regularly updated passwords.
- Storing data on designated secure servers or approved cloud services.
- Encrypting sensitive data both at rest and in transit.
- Ensuring servers are located in secure areas.

- Prohibiting unauthorised storage of data on personal or unprotected devices.

Data Use

Access to personal data is limited to authorized personnel for legitimate business purposes. Precautions include:

- Locking computer screens when unattended.
- Avoiding informal sharing of personal data.
- Prohibiting unauthorised data transfers outside the European Economic Area (EEA).
- Accessing and updating only central copies of data to maintain accuracy.

Data Accuracy

GHL takes reasonable steps to ensure personal data is accurate and up-to-date by:

- Minimising duplicate data storage locations.
- Encouraging regular verification and updates of data.
- Providing mechanisms for individuals to update their information.

Impact Assessments

For processing activities that may pose high risks to individual rights and freedoms, GHL conducts Data Protection Impact Assessments (DPIAs) to evaluate and mitigate potential risks.

Data Breaches

In the event of a data breach posing a risk to individuals' rights and freedoms, GHL will:

- Report the breach to the ICO within 72 hours of becoming aware.
- Notify affected individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms.