2024

KMP 009 Data Protection Policy

Published Feb 2024
Author: K Nichols
Review Date: Feb 2025
Version 16

Printed on 03 July 2024

DATA PROTECTION POLICY

Policy

Purpose

Group Horizon Ltd (GHL) is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out GHL's commitment to data protection, and individual rights and obligations in relation to personal data.

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 Karen Nichols as its data protection officer (DPO). The role is to inform and advise GHL on its data protection obligations. She can be contacted at karen.nichols@grouphorizon.co.uk. Questions about this policy, or requests for further information, should be directed to the data protection officer.

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.

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 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

Statutory retention period: 3 years for private companies, 6 years for public limited companies.

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

Coronavirus Job Retention Scheme - records of the furlough agreement including: the amount claimed, claim period for each employee, the claim reference number, and calculations in case HMRC need more information. For employees on flexible furlough - usual hours worked and the calculations required.

(See below for other types of COVID-19-related record keeping.)

Statutory retention period: 6 years for furlough records. (The guidance says employers should retain the written furlough agreement for 5 years. But HMRC can retrospectively audit all claims so GHL will keep a copy of all records for 6 years minimum.)

Statutory authority: The record keeping requirement appears to be in the statutory guidance 'Claim for wages through the Coronavirus Job Retention Scheme'.

First aid training

Statutory retention period: 6 years after employment.

Statutory authority: Health and Safety (First Aid) Regulations 1981.

Fire warden training

Statutory retention period: 6 years after employment.

Statutory authority: Fire Precautions (Workplace) Regulations 1997.

Health and Safety representatives and employees' training

Statutory retention period: 5 years after employment.

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

Income tax and 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, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631).

National minimum wage records

Statutory 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 (also overtime, bonuses, expenses)

Statutory 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 the Control of Substances Hazardous to Health Regulations (COSHH)

Statutory 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) (SIs 1999/437 and 2002/2677).

Records relating to children and young adults

Statutory retention period: until the child/young adult reaches the age of 21.

Statutory authority: Limitation Act 1980.

Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity

Statutory 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 shared parental, paternity and adoption pay records)

Statutory 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

Statutory retention period: 1 year following completion of the request.

Statutory authority: Data Protection Act 2018.

VAT deferral (COVID-19) – to support businesses through the COVID-19 pandemic, the government allowed VAT payments due between 20 March and 30 June 2020 to be deferred until 31 March 2021.

Statutory retention period: 6 years.

Statutory authority: HMRC VAT deferral guidance.

Whistleblowing documents

Statutory retention period: 6 months following the outcome (if a substantiated investigation). If unsubstantiated, personal data should be removed immediately.

Statutory authority: Public Interest Disclosure Act 1998 and recommended IAPP practice.

Working time records including overtime, annual holiday, jury service, time off for dependents, etc

Statutory retention period: 2 years from date on which they were made.

Statutory authority: The Working Time Regulations 1998 (SI 1998/1833).

Coronavirus Job Retention Scheme

Statutory retention period: 6 years for furlough records. The written furlough agreement should be retained for 5 years, but HMRC can retrospectively audit all claims, so GHL will keep a copy of all records for 6 years minimum. This will include the amount claimed, the claim period, claim reference number, calculations, usual hours worked (including any calculations for furloughed employees) and actual hours worked for flexibly furloughed employees.

Statutory authority: The statutory guidance 'Claim for wages through the Coronavirus Job Retention Scheme'

GHL adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

GHL tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. Where GHL relies on its legitimate interests as the basis for processing data, it will conduct an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where GHL processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

GHL will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's personnel file (in electronic format. The periods for which GHL holds HR-related personal data are contained in its privacy notices to individuals.

GHL keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Data Subject Rights

The GDPR lists eight data subject rights that the company will need to comply with, these are the rights of the data subject to:

- Be informed
- Subject access
- Erasure (to be forgotten)
- Rectification
- Portability
- Object
- Restrict processing
- Object to automated processing and profiling

Right to be informed

The right to be informed is complied with by issuing a privacy notice KMP 009A

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, GHL will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks GHL has failed to comply with his/her data protection rights; and
- whether or not GHL conducts automated decision-making and the logic involved in any such decision-making.

GHL will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically unless he/she agrees otherwise.

[If the individual wants additional copies, GHL will charge a fee, which will be based on the administrative cost to GHL of providing the additional copies.]

To make a subject access request, the individual should send the request to the DPO or use GHL's form for making a subject access request. In some cases, GHL may need to ask for proof of identification before the request can be processed. GHL will inform the individual if it needs to verify his/her identity and the documents it requires.

GHL will normally respond to a request within a period of one month from the date it is received. In some cases, such as where GHL processes substantial amounts of the individual's data, it may

respond within three months of the date the request is received. GHL will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, GHL is not obliged to comply with it. Alternatively, GHL can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which GHL has already responded. If an individual submits a request that is unfounded or excessive, GHL will notify him/her that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require GHL to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override GHL's legitimate grounds for processing data (where GHL relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override GHL's legitimate grounds for processing data.

To ask GHL to take any of these steps, the individual should send the request to the DPO

Data security

GHL takes the security of HR-related personal data seriously. GHL has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where GHL engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Data storage

These rules describe how and where data should be safely stored.

Data should only be stored on paper when essential or for legal purposes. It should be standard practise to only store data electronically (digital data).

Data printouts should be shredded or disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

Data must be protected by strong passwords that are changed regularly and never shared between team members.

Data should only be stored on designated drivers and servers and should only be uploaded to approved cloud computing services.

Servers containing personal data should be sited in a secure location, away from general office space..

All sensitive data such as customer data and personal identifiable information must be encrypted-at-rest using AES-256 or similar.

All sensitive data must be encrypted-in-transit during handling using TLS, SFTP, SSH or similar.

All employee devices should use full disk encryption.

Data should never be saved directly to laptops or other mobile devices like tablets or smartphones unless you have the full suite of security protection installed and configured.

All servers and computers containing data should be protected by approved security software and a security system.

Data use

Personal data is of no value to Group Horizon Ltd unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft.

When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

Personal data must not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

Personal data should never be transferred outside of the European Economic Area; however, data may be processed by a service provider based in countries outside of the EEA. Such countries do not always provide the same level of data protection as the UK; however, where such transfers of data occur, contracts are put in place that include security obligations on Group Horizon Ltd service providers to ensure that personal data is protected under UK standards.

Employees should not save copies of personal data to their computers. Always access and update the central copy of any data.

Data accuracy

The law requires Group Horizon Ltd to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Group Horizon Ltd should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Data will be held in as few places necessary. Team members should not create any unnecessary additional data sets.

Employees should take every opportunity to ensure data is updated. For instance, by confirming a customer’s details when they call.

Group Horizon Ltd will make it easy for data subjects to update the information Group Horizon Ltd holds about them. For instance, via the company page on our platform.

Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Impact assessments

Some of the processing that GHL conducts may result in risks to privacy. Where processing would result in an elevated risk to individual's rights and freedoms, GHL will conduct a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is conducted, the risks for individuals and the measures that can be put in place to mitigate those risks.

[Data breaches]

If GHL discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. GHL will record all data breaches regardless of their effect.

If the breach is likely to result in a substantial risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

GHL will not transfer HR-related personal data to countries outside the EEA.

Individual responsibilities

Individuals are responsible for helping GHL keep their personal data up to date. Individuals should let GHL know if data provided to GHL changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship, or apprenticeship. Where this is the case, GHL relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside GHL) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from GHL's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to [name of individual/the data protection officer] immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under GHL's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

GHL will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Disclosures required by law

There are circumstances where GHL is legally obliged to disclose information about an individual to a third party if this is required by law, enactment, or court order

Third Party	Authorisation for disclosure
UK Funding Councils e.g. HEFCE HEFCW, SFC and their agents e.g. QAA, HESA, HEFCE auditors	Further and Higher Education Act, 1992 s.79
Electoral registration officers	Representation of the People Act 2000; The Representation of the People (Scotland) & (England and Wales) Regulations 2001
Officers of the Department of Works and Pensions, and Local Authorities	Social Security Administration Act 1992: s.110A, s.109B and s.109C
Health and Safety Executive	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 1995 s.3
Audit Commission and related auditing bodies	Audit Commission Act 1998 s.6
Environmental Health Officers	Public Health (Control of Disease) Act 1984 and the Public Health (Infectious Diseases) Regulations 1988
Environment Agency	Agency Regulations – specific ones to be quoted
Inland Revenue	Taxes Management Act 1970
Other third parties	With a Court Order

Retention

The GDPR sets a clear requirement for the company to take its data retention responsibilities seriously. Generally, personal data should only be retained for as long as necessary. Just how long ‘necessary’ is, however, can differ based on the type of data processed, the purpose of processing or other factors.

Not only do we have to inform data subjects in the privacy notice how long we keep their personal data for, but we will also then have to ensure that these retention times are adhered to.

This means that data will need to be deleted, destroyed, or fully anonymised at the end of the retention time or archived appropriately in the company Archives.

It is important to note, in some circumstances personal data must be kept as destroying such data would be a data protection breach, for example learner records to verify a learner's qualifications.

Data retention is a personal responsibility for everybody in the company and it is important that all employees have an overview of where personal data is stored.

This may include:

- Own servers
- Third party servers
- Email accounts
- SharePoint sites
- Shared drives
- Backup storage
- Paper files

If in doubt, please ask your line manager for advice.

Learner/Student Privacy Policy

Group Horizon Ltd is committed to data security and the fair and transparent processing of personal data. This privacy policy (Policy) sets out how GHL, treats learner personal data.

If you are a learner enrolled with GHL to undertake learning, please read this Policy carefully as it contains important information on who we are, how and why we collect, store, use and share your personal data (process), your rights in relation to your personal data, how to contact us, and how to contact supervisory authorities in the event that you would like to report a concern about the way in which we process your personal data.

Who are we?

For the purposes of the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) and the UK Data Protection Act 2018 (DPA), GHL is the 'controller' of learner personal data.

If you have any queries about this Policy, the way in which we process personal data, or about exercising any of your rights, you may send an email to info@grouphorizon.co.uk or write to Group Horizon Ltd G24 The Avenues, Eleventh Avenue North, Team Valley, Gateshead, NE11 0NJ.

What personal data do we collect?

We collect your name, gender, and date of birth, and any other personal data which is necessary in relation to a specific qualification or programme. We may also collect personal data if required to administer our quality assurance processes, investigations, complaints, and appeals.

In exceptional circumstances, we may also collect and/or be provided with special category data, such as data about your physical or mental health or condition, to enable us to administer requests for reasonable adjustments, or in relation to an investigation, complaint, or appeal. Such data should only be collected and/or provided to us if you have provided your explicit consent or if we are otherwise permitted to receive and process it under the GDPR and/or DPA (including as set out below).

We assign a unique learner number to each learner at the point of enrolment or registration, which we also use in relation to your learning, training, assessment, and/or certification.

How do we process your personal data?

We may process your personal data where this is necessary to pursue our legitimate interests as a provider of learning, training, assessment, and/or certification products and/or services, including to:

- provide you with products and/or services for which you have enrolled or registered, or have been enrolled or registered;
- undertake administration in relation to products and/or services for which you are enrolled or registered;
- provide you with a certificate, credential, or other record of learning;
- contact you directly in relation to our quality assurance processes, investigations, complaints, and appeals;
- assess and provide reasonable adjustments in relation to your learning or assessment where requested; and
- prevent and detect crime and/or assist with the apprehension or prosecution of offenders.

We may also process your personal data if required by law.

With respect to special category data, we may process such data when we have obtained your explicit consent to do so. We may also process such data if necessary for reasons of substantial public interest, including for the prevention or detection of unlawful acts or in compliance with, or to assist third parties to comply with, any regulatory requirements relating to the investigation of unlawful acts, dishonesty, or malpractice.

Who do we share your personal data with?

We may share your personal data with relevant third parties, where necessary, in relation to your learning, assessment, certification, or the verification of your learning, assessment or certification, including:

- regulatory authorities, sector skills councils, professional bodies, and similar industry bodies;
- skills certification schemes and bodies;
- consortiums, authorised representatives, and partners; and
- centres, employers, providers, awarding bodies and similar third parties.

We may also share your personal data with trusted third-party service providers including:

- legal and other professional advisers, consultants, and professional experts;
- service providers contracted to us in connection with provision of learning, assessment, and training products and/or services such as markers, moderators, assessors, certification or credentialing providers, IT services and customer relationship management services; and
- analytics and search engine providers that assist us in the improvement and optimisation of our website.

We will ensure that there is a contract in place with such third-party service providers, which includes obligations in relation to the confidentiality, security, and lawful processing of any personal data shared with them, and which upholds your rights and freedoms with respect to personal data.

Where a third-party recipient is located outside the European Economic Area, we will ensure that the transfer of personal data is protected by appropriate safeguards, including by the use of standard data protection clauses adopted or approved by the European Commission where the Commission does not believe that the country has adequate data protection laws.

We may also share personal data (including any special category data) with law enforcement or other authorities or agencies if required by law or where we otherwise deem it necessary in pursuance of our legitimate interests. This may include, without being limited to, responding to requests for information from such authorities or agencies, or sharing information with them in connection with our quality assurance processes, investigations, complaints, or appeals.

You should be aware that, where personal data is shared with a public authority, it will become subject to the Freedom of Information Act 2000 (FOIA) and may potentially fall within the scope of any future FOIA request made to such public authority.

How long will we keep your personal data?

We will keep personal data relating to your learning, training, assessment, and/or certification in order to:

- provide information about your learning, training, assessment and/or certification;

- provide replacement certification;

- respond to any questions, complaints or claims made by you, on your behalf or about you;

- comply with any relevant third-party record retention requirements (e.g. those of a regulator); and

- comply with any contractual, legal, audit, and other regulatory requirements, or any orders from competent courts or authorities.

We will also keep personal data relating to our quality assurance processes, investigations, appeals and complaints, in order to comply with applicable contractual, legal, audit and other regulatory requirements, or any orders from competent courts or authorities.

GHL keeps personal data for no longer than as is necessary for the above purposes.

How do we protect your personal data?

We take all reasonable steps to ensure that we protect your personal data. This includes ensuring that our staff are aware of their information security obligations, providing training, and limiting access to your personal data to staff who have a genuine business need to know.

We also take reasonable steps to protect your personal data from loss or destruction and have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulatory of a suspected data security breach where we are legally required to do so.

Furthermore, our project management and change control process include structured assessment of information security and data privacy risks. This process aims to ensure that all proposed system changes of GHL from time to time fully align with the GDPR and good practice to uphold data subjects' rights and freedoms with respect to personal data.

Your rights

Under the GDPR, you have various rights with respect to our processing of your personal data:

Right to Access

You have the right to request a copy of the personal data that we hold about you by contacting us at the email or postal address given below. Please include with your request information that will enable us to verify your identity. We will respond within 1 month of request. Please note that there are exceptions to this right. We may be unable to make all data available to you if, for example, making the data available to you would reveal personal data about another person, if we are legally prevented from disclosing such data, if there is no basis for your request, or if your request is excessive.

Right to rectification

We aim to keep your personal data accurate, current, and complete. We encourage you to contact us using the contact details provided below to let us know if any of your personal data is not accurate or changes, so that we can keep your personal data up to date.

Right to erasure

You have the right to request the deletion of your personal data where, for example, the personal data is no longer necessary for the purposes for which it was collected, where you withdraw your consent to processing, where there is no overriding legitimate interest for us to continue to process your personal data, or your personal data has been unlawfully processed. If you would like to request that your personal data, be erased, please contact us using the contact details provided below.

Right to object

In certain circumstances, you have the right to object to the processing of your personal data where, for example, your personal data is being processed on the basis of legitimate interests and there is no overriding legitimate interest for us to continue to process your personal data, or if your data is being processed for direct marketing purposes. If you would like to object to the processing of your personal data, please contact us using the contact details provided below.

Right to restrict processing

In certain circumstances, you have the right to request that we restrict the further processing of your personal data. This right arises where, for example, you have queried the accuracy of the personal data we hold about you and we are verifying the personal data, you have objected to processing based on legitimate interests and we are considering whether there are any overriding legitimate interests, or the processing is unlawful, and you elect that processing is restricted rather than deleted.

Right to data portability

In certain circumstances, you have the right to request that some of your personal data is provided to you, or to another ‘controller,’ in a commonly used, machine-readable format. This right arises where you have provided your personal data to us, the processing is based on consent or the performance of a contract, and processing is conducted by automated means. If you would like to make such request, please contact us using the contact details provided below.

Please note that the GDPR sets out exceptions to these rights. If we are unable to comply with your request due to an exception, we will explain this to you in our response.

Complaints

If you believe that your data protection rights may have been breached, and we have been unable to resolve your concern, you may lodge a complaint with the applicable supervisory authority or seek a remedy through the courts. Please visit the UK Information Commissioner's Office website for more information on how to report a concern.

Changes to our Policy

Any changes we may make to our Policy in the future will be posted on this page and, where appropriate, notified to you by email. Please check back frequently to see any updates or changes to our Policy.