Data Protection and Privacy Policy

Contents

Introduction

Quay HR Solutions Limited (the Company) is committed to meeting the requirements of the General Data Protection Regulation and compliance with current GDPR legislation is therefore regarded as the absolute minimum standard acceptable.

At Quay HR Solutions, we recognise the importance of looking after personal data consistent with our legal responsibilities and wider organisational values.

Proper management of personal data is seen as an integral part of the efficient management of the Company's activities, and critical to developing the professional culture of the business and establishing and maintaining a solid reputation with all parties connected with Quay HR Solutions.

The organisation and arrangements to meet the requirements of the GDPR legislation are detailed in the policy below.

The objectives of this policy are fundamental to our success and the Director is ultimately responsible for ensuring that the requirements of this policy are achieved.

Quay HR employees have a responsibility for implementing the specific arrangements made under this policy throughout the business. All employees are expected to read this policy in its entirety, familiarise themselves with the provisions contained in the policy and carry out their defined responsibilities. A copy of this policy will be held internally on the Quay HR Joint Working Documents and will be made available to all employees and externally on the Quay HR website.

Employees are expected and encouraged to be proactive on data protection and privacy issues as part of the continued development and focus on confidentiality and appropriate data handling, accuracy and security within the Company.

All employees are required to cooperate with the Company and their colleagues in implementing the policy and shall ensure that their own work follows best practice with regards to GDPR compliance as far as reasonably practicable.

The Company will provide any training necessary as and when appropriate, seek specialist advice when required, endeavour to adhere to recommendations made by the Information Commissioners Office (ICO) and commit adequate resources so that legal obligations can be met.

Purpose

The Company is committed to being transparent about how it collects and uses the personal data of its workforce, clients, client's employees and job applicants and to meeting its data protection obligations. This policy sets out the Company'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, Company employees, apprentices, and former employees, referred to as HR-related personal data. This policy also applies to the personal data of clients, any personal data processed on behalf of clients, including client employees, job applicants, apprentices and former employees and any other personal data processed for general business purposes.

Questions about this policy, or requests for further information, should be directed to enquiries@qhrs.net.

Definitions

“Data subject” means an individual who is the subject of personal data.

"Personal data" is any information that relates to an 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 principles

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

- The Company processes personal data lawfully, fairly and in a transparent manner.
- The Company collects personal data only for specified, explicit and legitimate purposes.
- The Company processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The Company keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The Company keeps personal data only for the period necessary for processing. Please refer to the Company’s separate Data Retention Policy for further information.
- The Company adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The Company tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in this policy. It will not process personal data of individuals for other reasons without express consent.

The Company will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate. It is the responsibility of the individual to ensure that we hold up-to-date records.

Personal data gathered during the employment, or apprenticeship is held in the individual's personnel file (in hard copy or electronic format, or both), and on the Company’s Joint Working Documents. Personal data gathered in order to provide HR consultancy services to the Company’s clients is held in client files (in hard copy or electronic format, or both), and on the Company’s Joint Working Documents. The periods for which the Company holds HR-related personal data are contained in the Company’s separate Data Retention Policy which is held internally on the Quay HR Joint Working Documents and externally on the Quay HR website.

The Company 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).

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, the Company 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, the Company will not be disclosing data to recipients located outside the European Economic Area (EEA);
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data ("right to be forgotten" request), or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the Company has failed to comply with his/her data protection rights; and
- whether or not the Company carries out automated decision-making and the logic involved in any such decision-making.

The Company will also provide the individual with a copy of any 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, the Company will charge a fee, which will be based on the administrative cost to the Company of providing the additional copies.

To make a subject access request, the individual should send the request to enquiries@qhrs.net. In some cases, the Company may need to ask for proof of identification before the request can be processed. The Company will inform the individual if it needs to verify his/her identity and the documents it requires.

The Company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Company processes large amounts of the individual's data, it may respond within three months of the date the request is received. The Company will write to the individual within one month of receiving the original request to tell him/her if this is the case and to explain why the extension is necessary.

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, the Company can agree to respond but will charge a reasonable 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 the Company has already responded. If an individual submits a request that is unfounded or excessive, the Company will notify him/her that this is the case and whether or not it will respond to it.

If the Company is not going to respond to the request, the individual will be informed of their right to make a complaint to the ICO or another supervisory authority and their ability to seek to enforce this right through a judicial remedy in accordance with legislative guidelines.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the Company 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 the Company's legitimate grounds for processing data (where the Company 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 the Company's legitimate grounds for processing data.

To ask the Company to take any of these steps, the individual should send the request to enquiries@qhrs.net.

If an individual believes that the Company has not complied with their data protection rights, they can complain to the Information Commissioner.

Impact assessments

On rare occasions, some of the processing that the Company carries out may result in high risks to privacy, where the processing would result in a high risk to individual's rights and freedoms, the Company will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

If the Company 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, and without undue delay. If the Information Commissioner decides to undertake an audit following this reporting, the Company will fully cooperate with this process and adhere to any recommendations subsequently made by the Information Commissioners Office. The Company will record all data breaches regardless of their effect and whether or not the Company is required to notify the Information Commissioner using the internal Data Protection Register saved in the Joint Working Documents.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals without undue delay that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Main parties

The Company is committed to being transparent about how it collects and uses data and to meeting its data protection obligations.

For the business to function effectively and to provide HR services to our clients, the Company processes personal data relating to four main parties:

1) Applicants

As part of any recruitment process, either recruiting directly for the Company, or recruiting on behalf of our clients, the Company collects and processes personal data relating to job applicants. From time to time the Company will also receive speculative job submissions.

2) Quay HR employees

The Company collects and processes personal data relating to its employees to manage the employment relationship.

3) Client employees

The Company collects and processes personal data relating to employees of our clients to support our clients when managing the employment relationship with their employees.

4) Clients

The Company collects and processes our client's personal data for the benefit of providing HR consultancy services to our clients.

What information does the Company collect?

Examples of the information that the Company collects in relation to the four main parties described above includes but is not limited to:

- name, address and contact details, including email address and telephone number;
- details of qualifications, skills, experience and employment history;
- information about current level of remuneration, including benefit entitlements;
- information about medical or health conditions, including whether or not an individual has a disability for which the Company needs to make reasonable adjustments;
- information about nationality and entitlement to work in the UK;
- the terms and conditions of an individual's employment;
- bank account details and national insurance number;
- information about marital status, next of kin, dependants and emergency contacts;
- information about an individual's criminal record where applicable;
- details of working hours and attendance at work;
- details of periods of leave taken by the individual, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which an individual has been involved, including any warnings issued to them and related correspondence;

- assessments of performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence; and
- equal opportunities monitoring information, to be used for that purpose only, including information about gender, age, ethnic origin, sexual orientation and religion or belief.

The Company may collect this information in a variety of ways or may be given this information through speculative submissions. For example, data might be collected/contained in application forms, CVs or resumes, obtained from passports or other identity documents, or collected through interviews, meetings or other forms of assessment.

In some cases, the Company may also collect personal data about individuals from third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law.

The Company will seek information from third parties only once a conditional job offer has been made and will inform the individual that it is doing so.

Data will be stored in a range of different places, including in client files, personnel files, application forms/records and on IT systems (including Joint Working Documents and email).

Why does the Company process personal data?

The Company needs to process data for a number of different reasons. For example, to process an individual's data before entering into a contract of employment directly with an individual at the Company. Alternatively, to take steps on behalf of a client before the client enters into a contract of employment with an individual.

In some cases, the Company or Company on behalf of a client, needs to process data to ensure that the Company or client is complying with legal obligations. For example, the Company is required to check a successful applicant's eligibility to work in the UK before employment starts, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

In other cases, the Company has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing personal data allows the Company, either directly or on behalf of our clients, to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;

- obtain occupational health advice, to ensure that the Company/client complies with duties in relation to individuals with disabilities, meets obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the Company/client complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- provide references on request for current or former employees of the Company/client; and
- respond to and defend against legal claims.

The Company may process special categories of data, such as information about ethnic origin, sexual orientation or religion or belief, to monitor recruitment statistics for the purposes of equal opportunities monitoring. The Company may also collect information about whether or not a person is disabled to make reasonable adjustments for individuals who have a disability. Information about health or medical conditions may be processed to carry out employment law obligations in relation to Company employees or our client's employees. For some roles, the Company is obliged to seek information about criminal convictions and offences. Where the Company seeks and processes this information either directly or on behalf of a client, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.

The Company uses a third party supplier to conduct criminal record checks and has written documentation from this supplier to confirm compliance with the General Data Protection Regulation and to ensure the security of the data.

If a job applicant is unsuccessful, the Company may keep the individual's personal data on file in case there are future employment opportunities for which the individual may be suited. The Company will ask for the individual's consent before it keeps personal data for this purpose and the individual is free to withdraw their consent at any time. It will be held in accordance with the Data Retention Policy.

The lawful bases for this processing include: Contractual, Consent, Legitimate Interests, and Legal Obligation.

Who has access to data?

Personal information may be shared internally within the Company with members of the Quay HR team and with third party suppliers as and when appropriate for example, if a client uses an external payroll provider it may be necessary to share information about remuneration to pay a client's employees in accordance with their employment contract and to administer benefit, pension and insurance entitlements. This also applies to Quay HR employees, as the Company uses an external payroll provider.

For the purposes of a recruitment exercise, when applicable, information will be shared with the client we are representing to further aid the recruitment process. However, the Company will not share personal data with third parties, unless an application for employment is successful and an offer of employment has been made. The Company will then share personal data with former employers to obtain references, employment background check providers to obtain necessary

background checks and the Disclosure and Barring Service or relevant umbrella body to obtain necessary criminal records checks.

The Company will not transfer personal data outside the European Economic Area.

How does the Company protect data?

Third parties

The Company takes the security of personal data seriously. It has internal policies and controls in place to ensure that personal data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties.

Where the Company engages third parties to process personal data on its behalf, they 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.

Quay HR employees' individual responsibilities and training

Quay HR employees are responsible for helping the Company keep their personal data up-to-date. Employees should let the Company know if data provided to the Company changes, for example if an employee moves house or changes his/her bank details.

Quay HR employees may have access to the personal data of other individuals and of our clients in the course of their employment or apprenticeship. Where this is the case, the Company relies on its employees to help meet its data protection obligations to other staff and clients.

Quay HR employees 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 the Company) 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 the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

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

The Company will provide training to all Quay HR employees about the data protection responsibilities relevant to their role as part of the induction process for any new starters and as and when appropriate for existing staff.

For how long does the Company keep data?

Job applicants, Quay HR employees and former employees, client employees and clients can refer to the Company's policy on Data Retention, where they will find full details on how long data is stored.

What if an individual does not provide personal data?

Job applicants are under no statutory or contractual obligation to provide data to the Company during the recruitment process. However, if an individual does not provide the information, the Company may not be able to process their application properly or at all.

Quay HR employees and client employees have some obligations under their employment contract to provide the employing organisation with data. In particular, employees are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. Employees may also have to provide the employing organisation with data in order to exercise their statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that employees are unable to exercise their statutory rights. Certain information, such as contact details, an employee's right to work in the UK and payment details, have to be provided to enable the employing organisation to enter a contract of employment with the employee. If the employee does not provide other information, this will hinder the employing organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Changes to this policy

Quay HR Solutions Limited reserves the right to update this Data Protection and Privacy Policy at any time and the updated Policy will be available internally on the Joint Working Documents and externally on the Quay HR website when any substantial updates are made. In the event of any legislative changes, these changes will prevail if there is any discrepancy with this policy. The Company may also notify relevant parties in other ways from time to time about the processing of their personal information as appropriate.