enhance
Financial Resources

Privacy Notice

1. Introduction

Enhance Financial referred to throughout this Privacy Notice as 'the Company', is a Data Controller and processes personal data for the purpose of recruitment and processing of temporary workers and permanent candidates for our clients as well as the recruitment and employment of permanent staff.

Enhance is committed to being transparent about how it collects and uses data and to meet its data protection obligations.

2. What information does the Company collect?

The Company collects and processes a range of information that may or may not relate to all employees, workers, candidates, or clients. This includes:

- name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of employment;
- details of qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the Company;
- information about remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of bank account and national insurance number;
- information about marital status, next of kin, dependants and emergency contacts;
- information about nationality and entitlement to work in the UK, including passport and visa information;
- details of working hours and attendance at work;
- details of periods of leave taken, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which the employee has been involved, including any warnings issued and related correspondence;
- assessments of performance, including appraisals, performance reviews and ratings, training participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not employees have a disability for which the Company needs to make reasonable adjustments;
- electronic information in relation to use of IT systems/swipe cards/telephone systems;
- images (whether captured on CCTV, by photograph or video);
- information relating to driving accidents / convictions; and
- any other category of personal data which we may notify you of from time to time.

3. How do we collect the information?

The Company collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes, obtained from a passport or other identity documents such as a driving licence, from forms completed at the start of or during employment, from correspondence such as emails, or through interviews, meetings or other assessments, notes, or conversations either via phone whether recorded or not, in person, by text or other messaging options or video recordings.

In some cases, the Company collects personal data about an employee from third parties, such as references supplied by former employers, Governments and information from employment background checks if applicable.

4. Why does the Company process personal data?

The Company needs to process data to deliver its recruitment services or/and enter into an employment contract with an employee to meet its obligations under an employees' employment contract. For example, it needs to process data to provide employees with an employment contract, to pay them in accordance with their employment contract and to administer benefit, pension and insurance entitlements.

In some cases, the Company needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, 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 employee data allows the Company to:

- run recruitment, recognition and promotion processes;
- meet it's obligations under any relevant licencing laws such as the GLAA;
- 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;
- communicate effectively with you;
- 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 it complies with duties in relation to individuals with disabilities, meet its 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 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;
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes.

Where the Company processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the Company uses for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

5. Who has access to personal data?

Personal information may be shared internally at enhance with members of the HR, Compliance and recruitment teams (including payroll), a line manager, account manager and senior managers of the business. Worker information will also be shared with clients of enhance where a worker may be employed. This may include third party processors of a client such as neutral vendors operating timesheet or system management, where agreements are in place. IT staff and other providers of services may only have access to data if it is necessary for performance of an employees' job.

Limited personal data, such as a telephone number, may be shared with other workers or employees, for the purpose of group communications. However, we will seek to gain explicit consent from you under these circumstances.

The Company may be required to transfer personal data to countries outside the European Economic Area where it is appropriate to do so.

The Company may also share data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

6. How does the Company protect data?

The Company takes the security of employees' data seriously. The Company has internal controls in place to try to ensure that data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by relevant personnel in the 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.

7. For how long does the Company keep data?

Personal data collected will be retained only for as long as necessary to fulfil the purposes for which it was collected, unless longer retention periods are required or permitted by law.

Retention periods will be defined in accordance with applicable legal and regulatory requirements.

We will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require. This includes requiring third parties to delete such data where applicable.

Employee Data: Employee personal data is deleted or discarded securely following a period of six years after termination of employment.
Client and Third-Party Data: Client and third-party data will be maintained securely and subjects contacted periodically to ensure data is current and appropriate. Client Data Subjects will be given the option to have their data removed at any time.
Candidate & Worker Data: Candidate data will be maintained securely and contacted periodically to ensure data is current and appropriate.

8. Call / Video Recording

To support compliance, service quality, and operational transparency, enhance record work-related telephone calls and / or video calls as applicable, that are made or received via company systems. This includes calls involving employees, candidates, workers, clients, and suppliers where recruitment activity or business services are discussed.
Recordings are used solely for legitimate business purposes, including:

- Verifying recruitment requirements, contractual and compliance information
- Supporting dispute resolution and safeguarding concerns
- Enhancing training, audit readiness, and service standards

All recordings are stored securely, with access restricted to authorised personnel. Call participants will be notified where required, and may request access to or deletion of recordings under applicable data protection laws.

Call recordings are not shared with third parties except:

- When required by law or regulatory bodies
- To investigate complaints or resolve disputes
- With trusted service providers under strict confidentiality agreements

9. Your Rights

An individual has the following rights under Data Protection Laws:

- The right to be informed of what information the Company holds on them – this is typically given to the individual in a privacy notice;
- The right of access to any personal data that the Company holds on them – this is usually referred to as a 'subject access request';
- The right to rectification of personal data that the individual believes is either inaccurate or incomplete;
- The right to erasure of their personal data in certain circumstances;
- The right to restrict processing of their personal data;
- The right to data portability of their personal data in specific circumstances;
- The right to object to the processing of their personal data where it is based on either a legitimate interest or a public interest;
- The right not to be subjected to automated decision making and profiling; and
- The right to withdraw consent where it was relied upon to process their personal data.

To Exercise any of these rights, please email privacy@ethero.co.uk

Further information on your rights or our obligations, can be request using the above email or alternatively, a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk).

10. Automated decision-making

Our recruitment processes are not based on automated decision-making.

11. What if you do not provide personal data?

Workers and Employees: Employees have some obligations under their employment contract to provide the Company with data. In particular, they 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 Company 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 an employee is unable to exercise their statutory rights.

Candidates: Candidates are under no statutory or contractual obligation to provide data to the Company during the recruitment process. However, if they do not provide the information required, enhance and its clients may not be able to process an application properly or at all.

12. Keeping your personal data current

It is important that our records are correct as inaccurate or out of date information may cause difficulties in situations where contact is required for processing information or in emergencies. All employees and workers must notify their enhance of all changes in the following personal information:

- Name
- Home address
- Personal email address
- Telephone number
- Bank account details
- Emergency contact
- Criminal charge, caution or conviction
- Conflict, or potential conflict of interest

13. Contact Information

For any questions, concerns, subject access requests or other requests related to data protection and privacy, data subjects should email privacy@ethero.co.uk

Please refer to our Data Protection Policy for further information.