PRIVACY NOTICE FOR EMPLOYEES/WORKERS

In accordance with the General Data Protection Regulation (GDPR), Peer Group PLC of The Peer Suite, The Hop Exchange, 24 Southwark Street, London, SE1 1TY has implemented this privacy notice to inform you, our employees, of the types of data we process about you. We also include within this notice the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data.

This notice applies to current and former employees and workers.

A) DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing is fair, lawful and transparent
b) data is collected for specific, explicit, and legitimate purposes
c) data collected is adequate, relevant and limited to what is necessary for the purposes of processing
d) data is kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) data is not kept for longer than is necessary for its given purpose
f) data is processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g) we comply with the relevant GDPR procedures for international transferring of personal data

B) TYPES OF DATA HELD

Personal data is any information about an individual from which that person can be identified. It does not include anonymous data which does not identify the individual.

We collect, store and use several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system. It is your responsibility to keep us up to date with any changes to your personal details so that we can make sure that your personal data is accurate. If your personal details change, you must notify your manager.

Specifically, we collect, store and use the following types of data, as appropriate to your status:

a) personal details such as name, previous names, title, address, phone numbers, email address, date of birth
b) name and contact details of your next of kin
c) your photograph
d) your gender, marital status, information of any disability you have or other medical information
e) right to work documentation
f) information on your race and religion for equality monitoring purposes
g) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter
h) references from former employers
i) details on your education and employment history etc

j) National Insurance numbers
k) bank account details
l) pension details
m) tax codes
n) driving licence
o) criminal convictions
p) information relating to your employment with us, including:

   i) job title and job descriptions
   ii) your salary
   iii) your wider terms and conditions of employment
   iv) details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
   v) internal and external training modules undertaken
   vi) information on time off from work including sickness absence, family related leave etc

q) CCTV footage
r) building access card records
s) IT equipment use including telephones and internet access

C) COLLECTING YOUR DATA

You provide several pieces of data to us directly during the recruitment period and subsequently upon the start of your employment.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies.

Personal data is kept in files or within the Company's HR and IT systems.

D) LAWFUL BASIS FOR PROCESSING

The law on data protection allows us to process your data for certain reasons only. In the main, we process your data in order to comply with a legal requirement or in order to effectively manage the employment contract we have with you, including ensuring you are paid correctly.

The information below categorises the types of data processing, appropriate to your status, we undertake and the lawful basis we rely on.

Activity requiring your data	Lawful basis
Carry out the employment contract that we have entered into with you e.g. using your name, contact details, education history, information on any disciplinary, grievance procedures involving you	Performance of the contract
Ensuring you are paid	Performance of the contract
Ensuring tax and National Insurance is paid	Legal obligation
Carrying out checks in relation to your right to work in the UK	Legal obligation
Making reasonable adjustments for disabled employees	Legal obligation
Making recruitment decisions in relation to both initial and subsequent employment e.g. promotion	Our legitimate interests which are to ensure that we recruit, promote, and retain the most suitable talent for our business needs.
Making decisions about salary and other benefits	Our legitimate interests which are to ensure competitive, fair, and sustainable

	remuneration structures across the organisation.
Ensuring efficient administration of contractual benefits to you	Our legitimate interests which are to maintain smooth internal operations and provide a seamless benefits experience for our workforce.
Enrolling you in our pension scheme and administering the scheme	Legal obligation
Effectively monitoring both your conduct, including timekeeping and attendance, and your performance and to undertake procedures where necessary	Our legitimate interests which are to ensure workforce productivity, maintain operational standards, and uphold our workplace policies.
Maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained	Our legitimate interests which are to facilitate effective internal communication and ensure employee health and safety during workplace emergencies.
Implementing grievance procedures	Our legitimate interests which are to ensure a fair, transparent, and legally compliant framework for resolving workplace disputes.
Assessing training needs	Our legitimate interests which are to support employee career development and ensure our workforce possesses the skills necessary for our business operations.
Implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments	Our legitimate interests which are to manage operational staffing levels, support employee well-being, and minimise the impact of absence on the business.
Gaining expert medical opinion when making decisions about your fitness for work	Our legitimate interests which are to ensure a safe working environment, verify employee fitness for duty, and fulfil our duty of care.
Managing statutory leave and pay systems such as maternity leave and pay etc	Our legitimate interests which are to ensure fair, structured, and consistent management of family-related and statutory leave across the business.
Business planning and restructuring exercises	Our legitimate interests which are to ensure the long-term commercial viability, agility, and strategic growth of the company.
Dealing with legal claims made against us	Our legitimate interests which are to defend our legal rights, seek legal advice, and protect the financial and reputational standing of the business.
Preventing fraud	Our legitimate interests which are to protect company assets, safeguard financial integrity, and prevent criminal activity within the business.
Ensuring our administrative and IT systems are secure and robust against unauthorised access	Our legitimate interests which are to protect company and client data, prevent cyber threats, and maintain business continuity.
Providing employment references to prospective employers, when our name has been put forward by the employee/ex-employee, to assist with their effective recruitment decisions	Legitimate interest of the prospective employer

E) SPECIAL CATEGORIES OF DATA

Special categories of data are data relating to your:

a) health
b) sex life
c) sexual orientation
d) race
e) ethnic origin
f) political opinion
g) religion
h) trade union membership
i) genetic and biometric data.

We carry out processing activities using special category data:

a) for the purposes of equal opportunities monitoring
b) in our sickness absence management procedures
c) to determine reasonable adjustments

Most commonly, we will process special categories of data when the following applies:

a) you have given explicit consent to the processing
b) we must process the data in order to carry out our legal obligations
c) we must process data for reasons of substantial public interest
d) you have already made the data public.

F) FAILURE TO PROVIDE DATA

Your failure to provide us with data may mean that we are unable to fulfil our requirements for entering into a contract of employment with you. This could include being unable to offer you employment or administer contractual benefits.

G) CRIMINAL CONVICTION DATA

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your employment. We use criminal conviction data to determine your suitability, or your continued suitability for the role. We rely on the lawful basis of our legitimate interests to process this data.

H) WHO WE SHARE YOUR DATA WITH

Employees within our company who have responsibility for recruitment, administration of payment and contractual benefits and the carrying out of performance related procedures will have access to your data which is relevant to their function. All employees with such responsibility have been trained in ensuring data is processed in line with GDPR.

Data is shared with third parties for the following reasons: for the administration of payroll. The third parties who will process your personal data for this purpose are Sage Group PLC, and Peninsula Business Services Limited.

We will share your data with third parties for the purposes of administering any pension arrangement you are participating in, such as the trustees or scheme managers of the arrangement.

We may also share your data with third parties as part of a Company sale or restructure, or for other reasons to comply with a legal obligation upon us.

We have a data processing agreement in place with such third parties to ensure data is not compromised. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

We do not share your data with bodies outside of the European Economic Area.

I) PROTECTING YOUR DATA

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such.

J) RETENTION PERIODS

We only keep your data for as long as we need it for, which will be at least for the duration of your employment with us though in some cases we will keep your data for a period after your employment has ended. Some data retention periods are set by the law. Our retention periods are listed at peergroup.co.uk/legal.

K) AUTOMATED DECISION MAKING

Automated decision making means making decisions about you using no human involvement e.g. using computerised filtering equipment. No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

L) EMPLOYEE RIGHTS

You have the following rights in relation to the personal data we hold on you:

a) the right to be informed about the data we hold on you and what we do with it;
b) the right of access to the data we hold on you. More information on this can be found in our separate policy on Subject Access Requests;
c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
d) the right to have data deleted in certain circumstances. This is also known as 'erasure';
e) the right to restrict the processing of the data;
f) the right to transfer the data we hold on you to another party. This is also known as 'portability';
g) the right to object to the inclusion of any information;
h) the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate policy on employee rights under GDPR.

M) CONSENT

Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

N) MAKING A COMPLAINT

If you consider your data rights have been breached, you can make a complaint to us at any time using any of the following methods:

- Email: legal@peergroup.co.uk
- Post: The Peer Suite, The Hop Exchange, 24 Southwark Street, London, SE1 1TY
- Telephone: 020 7940 8900

More information is available in our separate policy on Data Protection Complaints available at peergroup.co.uk/legal.

You can also raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

O) DATA PROTECTION COMPLIANCE

Our Data Protection Officer is:

Michael Breeze
mdb@peergroup.co.uk