

1 What this policy covers

This policy outlines how we process personal data lawfully, fairly and transparently, in line with UK GDPR, the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations (PECR). It applies to recruitment operations, HR, marketing, compliance, and all business functions.

This policy applies to all personal data we process about candidates, temporary workers, employees, clients, suppliers, contractors, and website users.

This policy details your rights and obligations concerning your data and the personal data of third parties that you may encounter during your work.

"Personal data" is any information that relates to a living individual who can be identified from that information.

"Processing" is any use of personal 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 political beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" refers to information about an individual's criminal convictions and offences, as well as information related to criminal allegations and proceedings.

If you have access to the personal, special categories or criminal records data of staff or third parties, you must comply with this Policy. Failure to comply with the Policy and procedures may result in disciplinary action, including dismissal without notice.

Data Protection Principles

The Company processes HR-related personal data per 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 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 retains personal data only for the period necessary for the processing.
- The company adopts appropriate measures to ensure that personal data is secure and protected against unauthorised or unlawful processing and from accidental loss, destruction or damage.

2 Roles and Responsibilities

Data Controllers(s): Deploy Recruitment group (Inc Deploy Limited and Deploy Projects Limited)

Data Protection Officer (DPO): Robert Wands (dpo@deployrecruit.com)

3 Lawful Basis for Processing

- Recruitment: Legitimate interests, contract.
- Payroll/Tax/Right-to-work checks: Legal obligation.
- Marketing: Legitimate interests or consent under PECR.
- Special category data: Article 9(2)(b) and Schedule 1 (employment, equality).

4 Data Sharing

We share data only with authorised clients, suppliers, and processors under Article 28-compliant agreements.

5 Your entitlements

Data protection legislation prescribes how the Company may collect, retain and handle personal data. The Company will comply with the requirements of data protection legislation, and all individuals who handle personal data in the course of their work must also comply with these requirements.

The Company will inform individuals of the reasons for processing their data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data about individuals for other reasons.

Where the Company processes special categories of personal data or criminal record data to perform obligations or exercise rights under employment law, this is done in accordance with the rules relating to special categories of data and criminal record data.

The Company will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment or engagement of an employee, worker, contractor, volunteer, or intern is held in the individual's file (in hard copy, electronic format, or both) and on HR systems. The Company holds HR-related personal data for the periods given in its privacy notices.

Access to your data [subject access requests]

You have the right to make a subject access request. If you make such a request, the Company will tell you: whether or not your 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 you.

- to whom your data may be disclosed, including any recipients located outside the European Economic Area (EEA) and the safeguards that apply to any such transfers.
- for how long your data is stored, or how that period is decided.
- your rights to rectification or erasure of data, or to restrict or object to processing.
- your right to complain to the Information Commissioner if you think the Company has failed to comply with your data protection rights; and
- whether or not the Company carries out any automated decision-making and the logic involved.

The Company will also provide you with a copy of the personal data undergoing processing. This will typically be in electronic form if you have made the request electronically, unless you request otherwise.

If you require additional copies, the Company will charge a fee based on the administrative costs of providing the extra copies.

Other rights

You have several other rights concerning your data. You can require the Company to:

- rectify inaccurate data.
- stop processing or erase data if your interests override the Company's legitimate grounds for processing data (where the Company relies on its legitimate interests as a lawful basis for processing data).
- stop processing or erase data if it is unlawful; and
- stop processing data for a period if it is inaccurate or if there is a dispute about whether your interests override the Company's legitimate interests in processing the data.

6 Your responsibilities

You are responsible for ensuring the Company maintains accurate and up-to-date data. You should notify the Company if your personal data changes, for example, if you change your bank details or move house.

You may have access to the personal data of other individuals, as well as our customers or clients, during your employment, contract, volunteer period, internship, or apprenticeship. In such cases, the Company relies on you to assist in meeting its data protection obligations.

If you have access to personal data, you are required to:

- to access only data that you have the 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 personal devices used for work purposes.

Failure to observe these requirements may constitute a disciplinary offence, which will be addressed under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee, customer or client data without authorisation or a legitimate reason, may constitute gross misconduct and lead to your dismissal without notice.

Processing special categories and criminal records data

The Company will process special categories and criminal records data primarily where it is necessary to enable the Company to meet its legal obligations and to ensure adherence to health and safety legislation, vulnerable groups protection legislation, or for equal opportunities monitoring purposes.

Special category data processed for recruitment or employment (e.g., health data, ethnicity monitoring) is processed under GDPR Article 9(2)(b) and Schedule 1 DPA 2018—employment, equality and safeguarding obligations.

7 Procedure

The Company keeps a record of its processing activities in respect of HR-related personal data per the requirements of data protection legislation.

The Company may collect personal data relating to staff for:

- deciding on your recruitment or appointment.
- determining the terms on which you work for us.
- checking if you are legally entitled to work in the UK.
- paying you and, if you are an employee, deducting tax and National Insurance contributions.
- liaising with your pension provider.
- administering the contract we have entered into with you.
- business management and planning, including accounting and auditing.
- conducting performance reviews, managing performance and determining performance requirements.
- making decisions about salary reviews and compensation.
- assessing qualifications for a particular job or task, including decisions about promotions.
- gathering evidence for possible grievance or disciplinary hearings.
- making decisions about your continued employment or engagement.
- planning for the termination of our working relationship.
- education, training and development requirements.
- dealing with possible legal disputes involving you or other employees, workers and contractors, including accidents at work.
- ascertaining your fitness to work.
- managing sickness absence.
- complying with health and safety obligations.
- to prevent fraud.
- to monitor your use of our information and communication systems to ensure compliance with our policies.
- to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- to record digital meetings to allow replay or storage.
- to conduct data analytics studies to review and better understand employee retention and attrition rates, and
- equal opportunities monitoring

Some of the above grounds for processing will overlap, and several grounds may justify our use of your personal information.

How do we use special categories and criminal records data?

"Special categories" data and "criminal records" data require higher levels of protection. We need additional justification for collecting, storing, and processing this type of personal data. We may process special categories or criminal records data in the following circumstances:

- in limited circumstances, with your explicit written consent.
- where we need to carry out our legal obligations.
- where it is needed in the public interest, such as for equal opportunities monitoring or concerning our occupational pension scheme.
- Where it is needed to assess your working capacity on health grounds.

Less commonly, we may process this type of data when it is necessary to address legal claims, to protect your vital interests (or those of others), when you are unable to give your consent, or when you have already made the information public.

Accuracy of personal data

The Company will review personal data regularly to ensure that it is accurate, relevant and up to date.

To ensure the Company's files are accurate and up to date, so that the Company can contact you or, in the case of an emergency, another designated person, you must notify the Company as soon as possible of any change in your personal details (e.g. change of name, address, telephone number, loss of driving licence where relevant, next of kin details, etc).

Security of personal data

The Company will ensure that personal data is not processed unlawfully, lost or damaged. If you have access to personal data during your employment, you must also comply with this obligation. If you believe you have lost any personal data in the course of your work, you must report it to your manager immediately. Failure to do so may result in disciplinary action up to and including dismissal without notice.

Data breaches

The Company will record all data breaches regardless of their effect.

Suppose we discover that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals. In that case, we will report it to the Information Commissioner within 72 hours of becoming aware of the issue.

Suppose the breach is likely to result in a high risk to the rights and freedoms of individuals. In that case, we will inform affected individuals about the breach and provide them with information about the likely consequences and the mitigation measures we have taken.

The Company use various control measures to reduce the risk of a data breach, including MFA, encryption, access controls, staff training, device management, secure disposal, and breach monitoring.

Access to personal data ["subject access requests"]

To make a subject access request, you should send your request to the Company. Sometimes, the Company may require proof of identification before processing the request. We will inform you if we need to verify your identity and the required documents.

We will typically respond to a request within one month of receiving it. In some cases, such as when the Company processes large amounts of an individual's data, we may respond within three months of receiving the request. We will write to the individual within one month of receiving the original request to tell them if this is the case.

The Company is not obliged to comply with a subject access request if it is manifestly unfounded or excessive. Alternatively, we can agree to respond, but we will charge a fee based on the administrative costs of responding to the request. A subject access request is likely to be manifestly unfounded or excessive, where it repeats a request to which we have already responded. If you submit an unfounded or excessive request, we will notify you whether this is the case and whether we will respond.

Marketing and PECR

Emails/SMS comply with PECR. Opt-outs are honoured, and suppression lists are maintained.

Call Recording & Transcription

Telephone calls made to or from company devices, including those used by safety-critical workers, may be recorded and transcribed into our CRM/ATS. Recordings are processed to ensure accuracy of records, compliance, training, service quality, regulatory obligations, and to provide evidence in the event of an incident or dispute.

For safety-critical communications, recording is mandatory under industry regulations (e.g., Network Rail and safety-critical communication rules). Recording is used for competence management, incident investigation, and regulatory reporting. Access to recordings is strictly limited to authorised managers or investigators.

Individuals are informed of call recording via our published Privacy Notices.

The lawful bases for recording and transcribing calls are:

- Legitimate Interests (recruitment operations, compliance, accuracy of records);
- Contract (progressing a work-seeker relationship);
- Legal Obligation (safety-critical communication rules, incident reporting);
- Substantial Public Interest (Schedule 1 DPA 2018) for safety-critical roles.

Recordings are retained only as long as necessary for the stated purposes:

- Recruitment call recordings: 3–12 months
- Safety-critical communications: retained in line with industry regulations, competence review cycles, and incident investigation requirements.

A handwritten signature in blue ink, appearing to read 'PS', is located above the name Paul Smith.

Paul Smith, Managing Director
12TH January 2026