COMPANY POLICY DOCUMENT

UK GDPR Compliance Statement

Our assurance to clients, recruitment agency partners and hirers on how People Group Services Limited meets its obligations under UK data protection law.

Policy owner	Data Compliance Team, People Group Services Limited
Approved by	The Board of Directors
Version	2026.8 (supersedes version 2, dated October 2019)
Effective date	21 August 2026
Next scheduled review	21 August 2027, or earlier on a material change in law or regulatory guidance
Purpose	Client-facing assurance statement. It sits alongside, and does not replace, our Data Protection and Privacy Policy and Data Retention Policy
Classification	Public — published on the Company policy portal

Why this statement has been rewritten

The previous version dated from October 2019. It was written around the introduction of the EU GDPR and no longer described the law that applies to us.

Since then the UK has left the EU data protection regime and adopted the **UK GDPR**; the **Data (Use and Access) Act 2025 (DUAA)** has amended the UK GDPR, the Data Protection Act 2018 and PECR, with its principal provisions in force from 5 February 2026 and a mandatory complaints duty from 19 June 2026; and the regulator is being reconstituted as the **Information Commission**.

This version is written to the law as it stands on the effective date and is aligned to our Data Protection and Privacy Policy, version 2026.8.

1. Purpose of this statement

Clients, recruitment agency partners and hirers routinely ask us to evidence our data protection compliance as part of their own due diligence. This statement is our standing answer. It summarises how People Group Services Limited ("People Group", "we", "our") collects, uses and protects personal data, and what assurance we can provide.

It is a summary written for a commercial audience. The operative documents are our **Data Protection and Privacy Policy**, our **Data Retention Policy** and the supporting policies referenced throughout, all published on our policy portal.

2. Our regulatory position

Our data processing activities exceed those of a processor as defined in the legislation. In relation to the workers we employ and pay, **we are a Data Controller** and we meet our obligations in that role. Our position varies by service, and we set it out clearly at the outset of each engagement:

Activity	Our role
Employment and payment of umbrella and PEO workers	Controller
Joint employment with a named recruitment agency	Controller, or joint controller with responsibilities allocated in writing
Payroll bureau or outsourced processing performed on a client's instructions	Processor, under a written Article 28 agreement
Portal access provided to agencies, hirers and MSPs	Controller, with role-based access limited to what each party needs

Where we act as a controller and an agency also acts as a controller in respect of the same worker, each party is responsible for its own processing. Where an agency wishes to transfer worker data outside the UK, it must satisfy itself of its own lawful basis and safeguards for doing so.

3. Legal framework

- **UK General Data Protection Regulation** (UK GDPR);
- **Data Protection Act 2018**, as amended by the Data (Use and Access) Act 2025;
- **Data (Use and Access) Act 2025**, principal data protection provisions in force from 5 February 2026 and the complaints duty from 19 June 2026;
- **Privacy and Electronic Communications Regulations 2003**, as amended, with penalties now aligned to UK GDPR maxima;
- sector obligations that shape our processing, including PAYE and Real Time Information reporting, National Minimum Wage record-keeping, pensions auto-enrolment, right to work checking, the Criminal Finances Act 2017 and the Economic Crime and Corporate Transparency Act 2023.

4. How we meet each principle

Lawfulness, fairness and transparency

We hold contracts of employment with our employees, and policies and privacy notices that describe what categories of personal data we collect and the lawful basis for each. Personal data held on the People Group platform is there to fulfil:

- our **contractual obligations** under the contract of employment or engagement with the worker;
- our **legal obligations** as an employer, in relation to HMRC, National Minimum Wage and National Living Wage compliance, pension obligations, gender pay gap reporting, right to work verification and the Criminal Finances Act 2017;
- our **legitimate interests**, and the **recognised legitimate interests** introduced by the DUAA, under our supply agreements with agencies and in relation to fraud prevention and the security of our network and information systems.

> **Recognised legitimate interests**
>
> The DUAA created a category of processing that carries a presumption of legitimacy and does not require a balancing test, although it must still be necessary for the purpose pursued. Where we rely on it — principally for network and information security, intra-group administration and direct marketing — we record that reliance and reflect it in the relevant privacy notice. The right to object continues to apply.

Purpose limitation

Data is collected for specified purposes set out in our privacy notices. Where we consider a new use, we assess compatibility with the original purpose using the framework the DUAA sets out, and we seek consent or identify a legal obligation where the new purpose is not compatible.

Data minimisation

Most personal data is captured in pre-determined fields that correspond to those defined in contract or required by statute. Where documents are uploaded, such as identity documents, this is to facilitate specific performance of a contractual obligation or to fulfil a legal obligation. We do not collect data speculatively.

Accuracy

Workers can correct much of their own personal data directly in their secure portal. Further access, correction or deletion requests are handled by the Data Compliance Team.

Storage limitation

Retention is governed by our Data Retention Policy. In summary, where a worker has been paid we must retain their personal data for **six complete tax years following the end of the tax year in which the last payment was made**, in order to satisfy HMRC and pension record-keeping requirements. Shorter periods apply where no placement or payment has been processed. That data cannot be deleted on request while the statutory period runs, and we explain this when a request is made.

Integrity and confidentiality

We adopt technical and organisational measures designed to prevent:

- accidental or unlawful destruction, loss or alteration of personal data;
- unauthorised disclosure, transmission or processing of personal data;
- cyber intrusion, penetration or unauthorised access.

Accountability

We maintain a record of processing activities, complete Data Protection Impact Assessments where processing is likely to result in a high risk, and can track processing through our secure systems in order to provide compliance confirmation to regulatory bodies or as required contractually.

5. Information security

Asset management

- assets are identified and documented in an asset register, reviewed at least annually;
- every asset has a designated owner or custodian recorded in the register;
- employees must use Company assets in accordance with the acceptable use procedures.

Access control

- controls operate across operating systems, applications, networks and mobile access to the platform;
- user registration and de-registration follow a formal authorisation process, with a unique user ID per person and an audit trail of every request to add, modify or delete an account;
- privileges are allocated on a need-to-have basis and privileged accounts are recorded and reviewed;
- access rights are revoked immediately when a person leaves;
- multi-factor authentication is required for portal and administrative access;
- password use, change and removal are controlled, and access rights are subject to management review;
- no system or application detail is displayed before log-in, log-in attempts are limited, password entry is masked, and use of system utility programs is restricted.

Network security

- network access is provided only to authorised users, with controls for remote access;
- equipment is uniquely identifiable and networks are segregated according to need;
- authentication mechanisms control remote user access and network access rights are allocated to business and security requirements;
- we carry out regular vulnerability testing of our systems.

> **Certification**
>
> Where the Company holds current information security certification or accreditation, copies of the certificates and their scope are available to clients on request from the Data Compliance Team.
>
> Certification status should be confirmed against the current certificate rather than against this statement, which is reviewed annually.

6. Individual rights

Right	How we meet it
To be informed	We notify the data subject when their information is received, whether from self-registration or from a third party, as soon as it is added to the platform.
Of access	Much of the data is available directly in the secure worker portal. Formal subject access requests are handled by the Data Compliance Team.
To rectification	Correctable directly in the portal, or on request to the Data Compliance Team.
To erasure	Applied in accordance with the retention rules. Where a statutory retention period applies, we explain why the data cannot yet be deleted.
To restriction and to object	Assessed on the merits, including objections to processing based on legitimate interests or recognised legitimate interests. Objection to direct marketing is always honoured.
To portability	We provide the data subject with their personal data in a structured, commonly used, machine-readable format.
Relating to automated decisions	The right to be informed, to make representations, to obtain human intervention and to contest the decision. See section 7.

How requests are handled. We respond without undue delay and within one month, extendable by up to two further months where a request is complex. Two clarifications introduced by the DUAA now apply:

- our search is limited to what is **reasonable and proportionate**, and we explain the scope of the search carried out;
- where we reasonably require clarification in order to respond, the response period is **paused** until we receive it. We do not seek clarification as a matter of routine.

7. Automated decision-making and AI

Article 22 of the UK GDPR has been replaced by Articles 22A to 22D. The former general prohibition on solely automated decisions with legal or similarly significant effects is now a safeguards regime. Where we deploy automated processing, profiling or AI-assisted tools:

- we complete a Data Protection Impact Assessment before deployment;
- we inform the individual and provide a route to meaningful human intervention by someone able to change the outcome;
- we do not make solely automated decisions with a legal or similarly significant effect using special category data except on explicit consent or a substantial public interest condition;
- we test for bias and record the testing;
- our Acceptable Use of AI Policy and OCR and Automated Data Extraction Policy apply.

8. Data protection complaints

Statutory duty in force from 19 June 2026

Section 103 of the DUAA inserted section 164A into the Data Protection Act 2018. Every controller must operate a process for receiving and responding to data protection complaints, with no exemptions.

Individuals are expected to raise the matter with the controller first, and the ICO may decline to act on a complaint that has not been put to us.

We provide an electronic complaint form on our portal and accept complaints by email, telephone and post. We acknowledge receipt within 30 days, investigate without undue delay, keep the complainant informed, communicate the outcome with enough detail to show how it was reached, and explain how to escalate to the ICO. Complaint volumes, themes and outcomes are reported to the Board. Full detail is in our Complaints Procedure.

9. Personal data breaches

- all incidents are assessed and recorded, whether or not they are reportable;
- where a breach is likely to result in a risk to individuals, we notify the ICO without undue delay and within 72 hours of becoming aware;
- where the risk is high, we notify affected individuals without undue delay;
- where we act as a processor, we notify the controller without undue delay;
- our Data Breach Notification Procedure and Data Incident Response Policy govern the process.

10. International transfers

Personal data is primarily processed in the UK. Where a transfer outside the UK is necessary, we rely on UK adequacy regulations, a data bridge, or an appropriate safeguard such as the International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses. The DUAA replaced the essential equivalence test with a **data protection test**, under which protection in the destination must not be materially lower than under UK law.

The European Commission renewed the UK's adequacy decision on 19 December 2025, with effect until 27 December 2031, which supports continued data flows from the EEA into the UK.

11. Special category and criminal offence data

As a default we do not handle special category data for the ordinary purpose of our service provision. Where we do — for example health information relating to sickness absence, statutory sick pay or workplace adjustments — we identify an Article 9 condition and, where required, a Schedule 1 Data Protection Act 2018 condition, and we maintain the appropriate policy document required by Schedule 1. Criminal offence data, such as DBS results required by a hirer, is processed on the same footing under Article 10.

Clients must tell us in advance if special category data will need to be processed as part of an engagement, so that the lawful basis, security measures and retention period can be agreed before any data is transferred.

12. Governance and contact

Day-to-day responsibility for data protection sits with the Data Compliance Team, which reports to the Board. The Board retains ultimate accountability. Every manager is responsible for compliance within their team, and all staff complete data protection training on induction and at least annually.

Data Compliance Team, People Group Services Limited

Email: compliance@peoplegroupservices.com

Telephone: 0345 034 1530

Post: Three Horseshoes Walk, Warminster, Wiltshire BA12 9BT

Supervisory authority: the Information Commissioner's Office, ico.org.uk, 0303 123 1113 — being reconstituted as the Information Commission under the DUAA.

13. Assurance for clients and agency partners

The following are available to clients, agencies and hirers on request from the Data Compliance Team, subject to a confidentiality undertaking where appropriate:

- our Data Protection and Privacy Policy, Data Retention Policy and Complaints Procedure;
- a summary of our record of processing activities relevant to the engagement;
- our standard Article 28 processing terms and sub-processor list;
- current information security certificates and their scope;
- confirmation of training completion and breach history;
- completed responses to standard security and data protection questionnaires.

Where you are carrying out labour supply chain due diligence following the introduction of PAYE joint and several liability on 6 April 2026, we will support that exercise. We provide aggregated or assurance-level evidence wherever it will answer the question, and release worker-level data only where there is a lawful basis and a genuine need.

14. Declaration

This Statement is approved by the Board of Directors of **People Group Services Limited**, Company Number 11570329.

Version: 2026.8 | **Effective:** 21 August 2026 | **Supersedes:** version 2, dated October 2019

Next scheduled review: 21 August 2027

Signed for and on behalf of the Board of Directors

Date
21 August 2026