COMPANY POLICY DOCUMENT

Data Protection and Privacy Policy

How People Group Services Limited collects, uses, stores, shares and protects personal data across its payroll, employment and workforce compliance services.

Policy owner	Data Compliance Team, People Group Services Limited
Approved by	The Board of Directors
Version	2026.8 (supersedes the version dated 12 June 2026)
Effective date	21 August 2026
Next scheduled review	21 August 2027, or earlier on a material change in law, regulatory guidance or business practice
Applies to	All directors, employees, workers, contractors and third parties processing personal data on behalf of the Company
Classification	Public — published on the Company policy portal

Legal and regulatory framework

This policy is written to the UK data protection framework as it stands on the effective date, including the **Data (Use and Access) Act 2025 (DUAA)**, whose principal data protection provisions took effect on 5 February 2026 and whose mandatory complaints duty took effect on 19 June 2026.

Primary legislation and rules: UK GDPR; Data Protection Act 2018 (as amended by the DUAA); Privacy and Electronic Communications Regulations 2003 (PECR, as amended); Data (Use and Access) Act 2025.

Sector context: Income Tax (Earnings and Pensions) Act 2003 (including the umbrella company PAYE joint and several liability rules in force from 6 April 2026); Employment Rights Act 2025 and the Fair Work Agency; Conduct of Employment Agencies and Employment Businesses Regulations 2003; Immigration, Asylum and Nationality Act 2006 (right to work); Pensions Act 2008.

Regulator: the Information Commissioner's Office (ICO), which is being reconstituted as the **Information Commission** under the DUAA. References in this policy to the ICO should be read as references to the Information Commission once that transition completes.

What has changed in this version

This version is a substantive rewrite rather than a light refresh. The changes below are the ones most likely to affect how individuals deal with us and how our teams operate.

Area	What is new
Complaints	A new statutory data protection complaints procedure (section 164A of the Data Protection Act 2018, inserted by section 103 of the DUAA), in force from 19 June 2026. There is no exemption for any controller. See section 13.
Lawful basis	Recognised legitimate interests introduced by the DUAA, which remove the need for a balancing test for defined activities. See section 8.
Automated decisions	Article 22 of the UK GDPR has been replaced by Articles 22A to 22D, moving from a general prohibition to a safeguards-based regime. A dedicated section on automated decision-making and AI has been added. See section 9.
Access requests	Searches are expressly limited to what is reasonable and proportionate, and the response clock can be paused where clarification is reasonably required. See section 12.
Cookies	Limited consent exemptions for low-risk statistical and functional cookies, with an opt-out still required, and PECR penalties now aligned to UK GDPR maxima. See section 14.
International transfers	The essential equivalence test has been replaced by the DUAA data protection test. The UK's EU adequacy decision was renewed on 19 December 2025 and runs to 27 December 2031. See section 16.
Digital identity	New section covering certified digital verification services used in right to work and identity checking. See section 17.
Supply chain	New sections on controller and processor roles across our umbrella, PEO sole and joint employment models, and on data shared for labour supply chain due diligence following the introduction of PAYE joint and several liability on 6 April 2026. See sections 4 and 10.

1. Introduction

This policy sets out how People Group Services Limited ("we", "our", "us", "the Company") collects, uses, stores, shares and protects personal data. It is written to the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025, the Privacy and Electronic Communications Regulations 2003 and other applicable privacy and data protection law.

We are committed to safeguarding the privacy and security of personal information about our employees, workers, contractors, candidates, clients, recruitment agency partners, suppliers and everyone else we deal with. Because we operate payroll and employment services, much of the data we hold is financial, identity-based or otherwise sensitive, and we treat it accordingly.

This policy is approved by the Board of Directors and is mandatory. Breach of it may result in disciplinary action, termination of a contract for services, or termination of a supplier relationship.

2. Scope

This policy applies to all personal data processed by the Company in connection with:

- employment, worker and contractor relationships, including umbrella employment, PEO sole employment and joint employment arrangements;

- recruitment, onboarding, right to work and compliance verification;
- payroll processing, statutory deductions, pensions, expenses and payment services;
- services provided to recruitment agencies, hirers and Managed Service Providers (MSPs), including portal access and reporting;
- commercial, operational, procurement and supplier activities;
- website usage, marketing communications and customer support.

It applies to personal data held in any form, whether structured or unstructured, electronic or on paper, and wherever it is held, including on Company systems, third-party platforms and devices used under our Bring Your Own Device (BYOD) Policy.

3. Data protection principles

We process personal data in accordance with the following principles:

1. **Lawfulness, fairness and transparency** — we process data lawfully, fairly and in a way people would reasonably expect, and we explain what we do.
2. **Purpose limitation** — we collect data for specified, explicit and legitimate purposes, and we only use it for a new purpose where that purpose is compatible with the original one, or where we have consent or a legal obligation.
3. **Data minimisation** — we collect only what is adequate, relevant and necessary.
4. **Accuracy** — we take reasonable steps to keep data accurate and up to date, and to correct or erase inaccurate data without delay.
5. **Storage limitation** — we keep data only for as long as necessary, in line with our Data Retention Policy.
6. **Integrity and confidentiality** — we apply appropriate technical and organisational security measures.
7. **Accountability** — we document our processing, can demonstrate compliance, and build data protection into new systems and processes by design and by default.

4. Our role: controller, processor and joint arrangements

Our role in law depends on the service being delivered. Getting this right matters, because it determines who is responsible for responding to individuals and to the regulator.

Activity	Our role	Notes
Employment of umbrella and PEO workers	Controller	We determine how we process employment, payroll and tax data for our own employees and workers.
Joint employment arrangements	Controller / joint controller	Where employment responsibilities are shared with a named recruitment agency, responsibilities are allocated in writing and a summary is made available to affected individuals.
Payroll bureau and outsourced processing for a client	Processor	We act on the client's documented instructions under a written Article 28 agreement.
Portal access provided to agencies, hirers and MSPs	Controller	Access is role-based and limited to the data that party needs for its own lawful purposes.
Marketing, website and supplier management	Controller	We determine the purposes and means of this processing.

Day-to-day responsibility for this policy sits with the Data Compliance Team, which reports to the Board. We are not currently required to appoint a statutory Data Protection Officer, but the Data Compliance Team performs an equivalent internal function, and the Board retains ultimate accountability. Every manager is responsible for compliance within their team.

5. What personal data we collect

Depending on the relationship, we may collect and process:

Ordinary personal data

- identity information, including name, date of birth, national insurance number, photograph and identity document details;
- contact details, including address, email addresses and telephone numbers;
- employment, assignment and engagement information, including agency, hirer, assignment rate, start and end dates, timesheets, working hours and holiday records;
- payroll and tax information, including tax code, student loan status, pension contributions, statutory payments and deductions;
- financial information for payment processing, including bank account details;
- next of kin and emergency contact details, where provided;
- training, qualification and performance records;
- correspondence, call recordings and support records;
- website usage, device and technical data collected through cookies and analytics.

Special category and criminal offence data

We process a limited amount of special category data (for example health information relating to sickness absence, statutory sick pay, workplace adjustments or occupational health, and information about trade union membership where relevant to deductions) and criminal offence data (for example the results of DBS or equivalent checks required by a hirer in the education, healthcare or social care sectors).

Additional conditions for sensitive data

Special category data is processed only where we identify an Article 9 UK GDPR condition and, where required, a Schedule 1 Data Protection Act 2018 condition. Most commonly this is employment, social security and social protection law.

Criminal offence data is processed only where we identify an Article 10 condition and a Schedule 1 condition, typically the safeguarding or regulatory requirements condition.

We maintain an appropriate policy document covering this processing, as required by Schedule 1, and review it alongside this policy.

The DUAA gives the Secretary of State power to designate further categories of sensitive data. We monitor for any such designation and will update our records of processing accordingly.

6. How we collect personal data

- **Directly from individuals**, during onboarding, through our portal, by email, telephone or completed forms;
- **From recruitment agencies, hirers and MSPs** that place or engage the worker;

- **From public and government bodies**, including HMRC, the Department for Work and Pensions, pension providers and the Home Office right to work checking service;
- **From certified digital verification service providers** used for identity and right to work checking (see section 17);
- **From screening and referencing providers**, including DBS umbrella bodies, where a role requires it;
- **Automatically**, through our website, portal and systems, using cookies, logs and analytics.

7. Why we process personal data

- to enter into and administer contracts of employment, engagement and supply;
- to operate payroll, calculate and remit PAYE income tax, National Insurance contributions and the Apprenticeship Levy, and to make payments;
- to administer holiday pay, statutory payments, pensions and auto-enrolment;
- to verify right to work, identity and eligibility, and to prevent illegal working;
- to meet statutory reporting and record-keeping obligations, including Real Time Information reporting to HMRC and intermediary reporting;
- to evidence compliance to hirers, agencies, MSPs, accreditation bodies and auditors, including supporting their labour supply chain due diligence;
- to prevent, detect and investigate payroll fraud, financial crime, tax evasion facilitation, modern slavery and labour exploitation;
- to secure our network, systems and information;
- to communicate with individuals about their engagement, pay, benefits and support requests;
- to handle complaints, disputes, grievances and legal claims;
- to improve our services and technology platforms;
- to send marketing communications where we are permitted to do so.

8. Lawful basis for processing

We rely on one or more of the following lawful bases under Article 6 UK GDPR:

- **Performance of a contract**, or steps taken at the individual's request before entering into one — for example paying wages and administering an assignment;
- **Compliance with a legal obligation** — for example PAYE, National Minimum Wage records, pensions auto-enrolment and right to work checks;
- **Legitimate interests** — for example fraud prevention, network security, service improvement and business administration, where a documented legitimate interests assessment shows the processing does not unduly affect the individual's rights;
- **Consent** — used sparingly, for example for certain marketing and for optional benefits. Consent can be withdrawn at any time;
- **Vital interests** or the **public interest**, in the limited circumstances where those apply.

Recognised legitimate interests (new under the DUAA)

The DUAA introduced a category of **recognised legitimate interests**. Where processing falls within that category, no balancing test is required, although the processing must still be necessary for the purpose pursued.

Activities relevant to us include direct marketing, transmitting personal data within a group of undertakings for internal administrative purposes, and ensuring the security of network and information systems. Crime prevention, safeguarding and emergency response are also recognised.

Where we rely on this basis we record it in our record of processing activities and reflect it in the relevant privacy notice. The right to object continues to apply, and we assess each objection on its merits.

9. Automated decision-making, profiling and AI

The DUAA replaced Article 22 UK GDPR with Articles 22A to 22D. The previous general prohibition on solely automated decisions with legal or similarly significant effects has been replaced by a safeguards regime. The change relaxes the lawful basis requirement but does not relax the safeguards, and it does not apply where special category data is used.

Where we use automated processing, we:

- identify and record whether a decision is solely automated and whether it has a legal or similarly significant effect;
- provide clear information to the individual before or as soon as reasonably practicable after the decision is made;
- allow the individual to make representations, to obtain meaningful human intervention from someone with the authority and competence to change the outcome, and to contest the decision;
- do not make solely automated decisions with a legal or similarly significant effect using special category data unless the individual has given explicit consent or a substantial public interest condition applies;
- complete a Data Protection Impact Assessment before deploying automated decision-making, profiling or AI-assisted tools in areas such as recruitment screening, compliance risk scoring or fraud detection;
- test for bias and unfair outcomes, and document the testing;
- operate our Acceptable Use of AI Policy and our OCR and Automated Data Extraction Policy alongside this policy.

The ICO has indicated it will prioritise enforcement where automated decision-making systems lack transparency or fail to deliver meaningful human intervention in practice. Our safeguards are therefore operational and tested, not documentary only.

10. Data sharing, disclosure and processors

Personal data may be shared by supplying electronic or hard copies, or by providing role-based portal access. We may share personal data with:

- **Government bodies and regulators**, including HMRC, the Department for Work and Pensions, The Pensions Regulator, the Home Office and the Fair Work Agency;
- **Recruitment agencies, hirers and MSPs** in the labour supply chain, limited to what each party needs, in line with our MSP Visibility and Data Access Policy;
- **Auditors appointed by agencies or hirers**, and industry accreditation and regulation bodies, for the purposes of assessing and monitoring our compliance;

- **Pension providers, insurers, benefits providers and payment institutions**;
- **Third-party service providers acting on our behalf**, including software, hosting, payroll technology, identity verification and archiving suppliers;
- **Professional advisers**, including lawyers, accountants and insurers, where necessary;
- **Other organisations where required or permitted by law**, including in response to lawful requests from law enforcement.

We do not sell personal data to third parties.

> **Labour supply chain due diligence**
>
> Since 6 April 2026, a recruitment agency, or in some cases an end client, can be jointly and severally liable for unpaid PAYE income tax and Class 1 National Insurance contributions where an umbrella company sits in the labour supply chain. As a result, agencies and hirers request more compliance evidence than they used to.
>
> We support that due diligence, but we do so proportionately. Wherever possible we provide aggregated, anonymised or assurance-level evidence rather than individual-level payroll data, and we release worker-level data only where there is a lawful basis and a genuine need.
>
> Requests for bulk worker data are reviewed by the Data Compliance Team before release.

Processors and supply chain assurance

- we appoint processors only where they can provide sufficient guarantees of appropriate technical and organisational measures;
- every processor is engaged under a written contract containing the terms required by Article 28 UK GDPR;
- sub-processors require our prior written authorisation;
- we carry out and record due diligence at onboarding and on a risk-based cycle thereafter, in line with our Supply Chain Due Diligence Policy;
- processor contracts require support for data subject rights, breach notification and the complaints duty described in section 12.

11. Data security

We implement appropriate administrative, technical and organisational measures to protect personal data against unauthorised or unlawful processing, accidental loss, destruction or damage. These include:

- role-based access control, least-privilege access and periodic access reviews;
- multi-factor authentication for portal and administrative access;
- encryption of personal data in transit and at rest;
- secure configuration, patching, vulnerability management and logging;
- verified controls around bank account changes, in line with our Bank Account Change and Verification Policy, which is a key defence against payroll diversion fraud;
- supplier and integration security controls, in line with our API and Integration Security Policy;
- device and remote working controls, in line with our BYOD and Remote and Hybrid Working Policies;
- mandatory data protection and information security training for all staff, refreshed at least annually and on joining;
- business continuity and disaster recovery arrangements, tested periodically.

Personal data breaches

Anyone who becomes aware of an actual or suspected personal data breach must report it immediately to the Data Compliance Team at compliance@peoplegroupservices.com. Do not attempt to investigate or resolve it alone, and do not delay reporting in order to establish the facts first.

- we assess every reported incident and record it, whether or not it is reportable;
- where a breach is likely to result in a risk to individuals, we notify the ICO without undue delay and in any event within 72 hours of becoming aware of it;
- where a breach is likely to result in a high risk to individuals, we notify the affected individuals without undue delay;
- where we act as a processor, we notify the controller without undue delay;
- PECR breach notification is now aligned with the UK GDPR framework, and we apply a single process;
- our Data Breach Notification Procedure and Data Incident Response Policy set out the detail.

12. Your rights

Under the UK GDPR and the Data Protection Act 2018 you may have the right to:

- be informed about how we use your personal data;
- request access to your personal data (a subject access request);
- request rectification of inaccurate or incomplete data;
- request erasure of your data in limited circumstances;
- request restriction of processing;
- object to processing, including processing based on legitimate interests or recognised legitimate interests, and to object to direct marketing at any time;
- request portability of data you provided to us, where processing is based on consent or contract and carried out by automated means;
- withdraw consent at any time, where processing is based on consent;
- obtain human intervention in relation to a solely automated decision with a legal or similarly significant effect (see section 9).

How we handle requests

- requests can be made in writing to the Data Compliance Team at compliance@peoplegroupservices.com, through the portal, or by post to our registered office. A request does not have to use any particular wording or mention data protection law;
- we may need to verify your identity, and we will do so proportionately;
- we respond without undue delay and within one month. We may extend this by up to a further two months where the request is complex or where a number of requests have been received, and we will tell you if we do;
- the DUAA confirms that our search must be **reasonable and proportionate**. We are not required to search every system without limit, and we will explain the scope of the search we have carried out;
- where we reasonably require clarification in order to respond, we may ask for it and the response period is paused until we receive it. We do not ask for clarification as a matter of routine, and we will explain why it is needed;
- we may refuse a request, or charge a reasonable fee, where it is manifestly unfounded or manifestly excessive. If we do, we will explain why and tell you how to challenge that decision;

- some information may be withheld where an exemption applies, for example legal professional privilege, or where disclosure would reveal information about another person who has not consented.

13. Data protection complaints procedure

> **Statutory requirement in force from 19 June 2026**
>
> Section 103 of the Data (Use and Access) Act 2025 inserted section 164A into the Data Protection Act 2018. Every controller must operate a process for receiving and responding to data protection complaints. There are no exemptions of any kind.
>
> Individuals are now expected to raise a concern with us **first**. The ICO may decline to act on a complaint that has not been put to the controller.

If you believe we have processed your personal data in a way that breaches data protection law, you can complain to us directly. You do not need to have made a subject access request first, and you do not need to use any particular form of words.

How to complain

- **Online** — using the data protection complaint form on our portal;
- **By email** — compliance@peoplegroupservices.com, marking the message "Data protection complaint";
- **By post** — Data Compliance Team, People Group Services Limited, Three Horseshoes Walk, Warminster, Wiltshire BA12 9BT;
- **By telephone** — 0345 034 1530, where we will record the complaint on your behalf and send you a written summary.

What we will do

Stage	Our commitment
Acknowledge	We acknowledge receipt of your complaint within 30 days. In practice we aim to acknowledge within five working days.
Investigate	We make appropriate enquiries into the subject matter of the complaint without undue delay, and we keep you informed of progress.
Respond	We tell you the outcome, with enough detail for you to understand how we reached it, and we explain any corrective action taken.
Escalate	If you are dissatisfied, we tell you how to escalate the matter to the ICO, and we give you its contact details.
Record and learn	Every complaint is logged. Volumes, themes and outcomes are reported to the Board so that recurring problems are fixed at source.

This procedure covers complaints about how we handle personal data. Complaints about pay, deductions, service quality or any other matter continue to be handled under our Complaints Handling Policy. Where a complaint raises both, we deal with the data protection element under this section and apply the shortest applicable deadline across the whole complaint.

14. Cookies and tracking technologies

We use cookies and similar technologies on our website and portal to:

- support login, session management and form functions;
- analyse usage and improve the user experience;
- administer marketing and analytics, where you have agreed to that.

Strictly necessary cookies do not require consent. The DUAA introduced limited further exemptions, including for cookies used only to collect statistical information in order to improve a service, and for certain appearance and functionality preferences. These exemptions are narrow, and they apply only where clear information is given and a straightforward opt-out is provided. Where any doubt exists, we ask for consent.

Non-essential cookies are not set before consent is given, consent is as easy to refuse as to give, and it can be withdrawn at any time through the cookie preference centre. Full details are in our Cookie Policy.

Note for the business: PECR penalties are now aligned with UK GDPR maxima, up to the higher of £17.5 million or 4% of global annual turnover. The ICO has signalled renewed enforcement focus on cookie compliance, particularly where opt-outs are not meaningful or where "statistical purposes" is used loosely.

15. Marketing communications

We send marketing communications only where we have consent, or where the soft opt-in under PECR applies to an existing customer relationship for similar products and services. Every marketing message identifies us and includes a simple, free means of opting out. Opt-outs are actioned promptly and recorded on a suppression list, which we do not delete.

16. International transfers

Personal data is primarily processed within the UK. We do not transfer personal data outside the UK unless appropriate safeguards are in place.

- we transfer data to countries covered by UK adequacy regulations or a "data bridge", or under 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 the standard of protection in the destination must not be materially lower than under UK law. We apply that test, supported by a transfer risk assessment where required;
- we follow current ICO guidance on when a restricted transfer arises, including the position that a UK processor returning data to its own overseas controller is not itself making a restricted transfer;
- we record transfers, safeguards and assessments in our record of processing activities.

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 to the UK.

17. Digital identity and verification services

We use digital identity verification technology to carry out right to work, identity and eligibility checks. This may involve processing identity document images, facial images and biometric data derived from them.

- we use providers certified against the UK digital identity and attributes trust framework, given statutory footing by Part 2 of the Data (Use and Access) Act 2025, and we check that certification remains current;
- biometric data derived from an identity check is special category data and is processed only where an Article 9 condition applies;

- we retain only the outputs and evidence required by Home Office guidance, not raw biometric templates, except where the provider retains them under its own certified controls;
- manual and Home Office online checks, including share code checks and eVisa checks, remain available where an individual cannot or does not wish to use digital verification, and no one is disadvantaged for choosing that route;
- our Right to Work Check Process (UK) sets out the operational detail.

18. Data retention

We retain personal data only for as long as necessary for the purposes for which it was collected, including any statutory retention period and any period needed to defend legal claims. Retention periods are set out in our Data Retention Policy. Illustrative examples include:

Record type	Indicative retention period
Payroll and PAYE records	At least 3 years after the end of the tax year to which they relate
National Minimum Wage records	At least 6 years
Working time and holiday records	At least 2 years
Right to work check evidence	2 years after employment or engagement ends, and for the duration of it
Pensions and auto-enrolment records	Generally 6 years
Personnel and engagement files	Generally 6 years after the relationship ends
Marketing consents and suppression records	Consent records for the duration of the relationship; suppression records indefinitely

At the end of the retention period, data is securely deleted or anonymised. Where deletion is not technically possible, for example within backups, the data is placed beyond use and deleted on the normal backup cycle.

19. Accountability, by design and impact assessments

- we maintain a record of processing activities and review it at least annually, and whenever a new processing activity, system or supplier is introduced;
- we apply data protection by design and by default when building or procuring systems, in line with current ICO guidance;
- we carry out a Data Protection Impact Assessment before any processing likely to result in a high risk to individuals, including new automated decision-making, large-scale processing of special category data, biometric processing and significant changes to portal data sharing;
- we maintain an appropriate policy document for special category and criminal offence data;
- we deliver mandatory training on induction and at least annually, with additional role-based training for payroll, compliance, onboarding and technology teams;
- we monitor compliance through internal review, supplier assurance, external accreditation assessment and audit.

20. Contact and regulator

For any question, request or concern about this policy or how we use your personal data, contact:

Data Compliance Team, People Group Services Limited

Email: compliance@peoplegroupservices.com

Telephone: 0345 034 1530

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

You also have the right to lodge a complaint with the Information Commissioner's Office, the UK supervisory authority for data protection, at ico.org.uk, by telephone on 0303 123 1113, or by post at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. We would ask you to raise the matter with us first, using the procedure in section 13, so that we have the opportunity to put things right.

Under the Data (Use and Access) Act 2025 the regulator is being reconstituted as the Information Commission. Its functions, powers and contact routes carry across, and this policy will be updated when that transition completes.

21. Changes to this policy

We review this policy at least annually, and sooner where there is a material change in legislation, regulatory guidance or our business practices. The current version is always published on our policy portal with a revised effective date. Material changes are notified to employees, workers and contractors directly.

22. Declaration

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

Version: 2026.8 | **Effective:** 21 August 2026 | **Supersedes:** version dated 12 June 2026

Next scheduled review: 21 August 2027

Signed for and on behalf of the Board of Directors

Date
21 August 2026