

CANDIDATE PRIVACY NOTICE 2026

Version	1
Date	October 2026
Policy Owner	Louise Leyden-Ahmed
Organisation	Precision Resource Group
Status	Approved

Document control	Details
Organisation	Precision Resource Group Limited (PRG)
Version	1.0
Effective date	September 2026
Document owner	Data Protection Lead
Status	Approved
Classification	Public / Candidate-facing
Review cycle	At least annually and following material legal, technology or processing changes

This notice explains how PRG collects, uses, shares, protects and retains personal information about candidates and prospective candidates.



1. Who this notice applies to

Precision Resource Group Limited (PRG, we, our or us) is committed to handling personal information lawfully, fairly, transparently and securely. This notice applies to people who apply for work through PRG, register as candidates, are identified through sourcing or talent-search activity, are referred to us, or participate in recruitment, selection, placement or engagement processes.

It covers candidates for temporary, contract, permanent, consultancy and other work opportunities. If you become a PRG employee or worker, a separate employee privacy notice may also apply.

2. Who is responsible for your information

PRG is a controller of the candidate information described in this notice. Depending on the recruitment arrangement, a client, end hirer, umbrella company, payroll provider or group company may act as a separate controller for its own purposes. Those organisations should provide their own privacy information where required.

3. Data protection framework

PRG processes candidate information in accordance with the UK General Data Protection Regulation, the Data Protection Act 2018, the Data (Use and Access) Act 2025 and other applicable privacy and employment laws. Where local law imposes additional requirements, PRG may provide a supplementary notice.

4. Information we collect

Category	Examples
Identity and contact	Name, title, address, email, telephone number, date of birth, nationality, photograph and identifiers.
Professional profile	CV, work history, skills, qualifications, education, professional memberships, licences, certifications and portfolio information.



Application and selection	Roles applied for, availability, location, salary or rate expectations, interview notes, assessment results, communications, feedback and recruitment decisions.
Compliance and eligibility	Right-to-work evidence, visa or immigration information, references, identity checks and screening information where necessary and lawful.
Placement and assignment	Client submissions, role requirements, placement terms, timesheets, availability, onboarding and assignment information.
Special category information	Health, disability, diversity or equal-opportunity information where provided or lawfully required.
Criminal offence information	Conviction or background-check information only where authorised by law and necessary for a role or client requirement.
Systems and communications	Candidate portal activity, emails, calls, messages, interview scheduling, security logs and information generated through recruitment systems.
Recordings and transcripts	Audio, video, transcripts, summaries and notes where an approved tool is used and appropriate notice or consent is provided where required.
AI-assisted information	Search or matching results, skills extraction, summaries, suggested actions, workflow outputs, usage logs and reviewed outputs produced through approved AI-enabled tools.

5. Where information comes from

- You directly, including information supplied in applications, CVs, interviews and communications.
- Referees, former employers, recruitment agencies, employees and professional contacts.
- Job boards, professional networking sites and publicly available professional sources.
- Clients, end hirers, screening providers, qualification bodies and authorised service providers.
- Government, immigration, regulatory, law-enforcement or court sources where lawful.

- PRG systems, approved recruitment platforms, communications tools, security systems and approved AI-enabled services.

6. Why we use information and our lawful bases

Purpose	Typical lawful basis
Registering and communicating with candidates	Legitimate interests; steps requested before entering into a contract.
Searching, sourcing and matching candidates to work opportunities	Legitimate interests.
Managing applications, interviews, assessments and offers	Steps requested before entering into a contract; legitimate interests.
Submitting candidate information to an identified client or end hirer	Legitimate interests; steps requested before entering into a contract; consent where it is the appropriate basis.
Checking identity, eligibility, right to work, qualifications and references	Legal obligation; legitimate interests; steps before contract.
Managing placements, assignments, onboarding and related records	Contract; legal obligation; legitimate interests.
Maintaining talent pools and contacting candidates about relevant opportunities	Legitimate interests; consent where required.
Equality monitoring and workplace adjustments	Legal obligation; substantial public interest; employment and social-protection law; explicit consent where appropriate.
Security, fraud prevention, audit, complaints and legal claims	Legal obligation; legitimate interests; establishment, exercise or defence of legal claims.
Approved AI-assisted search, matching, transcription and workflow support	The lawful basis applicable to the underlying recruitment purpose, with additional safeguards where required.

Where PRG relies on legitimate interests, it considers the necessity and proportionality of the processing and balances those interests against your rights and reasonable expectations. Where consent is used, it will be specific

and capable of being withdrawn. Withdrawal does not affect processing already carried out lawfully.

7. Special category and criminal offence information

PRG only processes special category information where an Article 6 lawful basis and an applicable Article 9 condition are available. Depending on the purpose, this may include employment and social-protection law, occupational health, substantial public interest, legal claims, vital interests or explicit consent. Criminal offence information is processed only where authorised by law and subject to appropriate safeguards. Access is restricted and retention is limited to what is necessary.

8. Candidate submissions and sharing

PRG may share relevant candidate information with an identified prospective employer, client or end hirer for recruitment and placement purposes. PRG will limit disclosure to information reasonably needed for the opportunity and will use appropriate, authorised channels. Where practicable, PRG will tell you about the intended submission or keep you informed through the recruitment process.

- PRG group companies and authorised internal teams.
- Clients, prospective employers, end hirers and managed-service or recruitment-process partners.
- Payroll, umbrella, onboarding, benefits, screening, compliance and occupational-health providers where relevant.
- IT, cybersecurity, communications, recruitment, document-management, hosting and approved AI service providers.
- Professional advisers, auditors, insurers, regulators, courts, law enforcement and public authorities where required or permitted by law.

9. AI, matching and automated processing

PRG may use approved AI-enabled or automated features to help source candidates, extract skills, search and match profiles, summarise CVs or communications, create notes, support workflow and provide decision-

support. These tools may process information held in approved recruitment or business systems.

- Only approved tools, accounts, integrations and use cases may be used for candidate information.
- PRG applies data minimisation, access controls, supplier review, retention controls and human oversight.
- Outputs are checked for accuracy, relevance, bias, context and confidentiality before they are used or relied upon.
- PRG does not permit unapproved AI tools to make or communicate recruitment decisions.
- Where a decision produces legal or similarly significant effects and is made solely by automated means, PRG will only proceed where permitted by law and will provide applicable safeguards, including information, human intervention and a route to challenge the decision.

10. Recordings and transcription

Interviews, calls or meetings may be recorded or transcribed only through approved arrangements. PRG will provide appropriate notice before recording or transcription begins and will obtain consent where legally required. Recordings, transcripts, summaries and notes will be used only for an identified recruitment or business purpose, checked where necessary and retained in line with the applicable schedule.

11. International transfers

Some clients, group companies or service providers may be located outside the UK. Where a restricted transfer occurs, PRG will use an available lawful mechanism, such as UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to approved standard contractual clauses, binding corporate rules or another permitted safeguard. PRG will complete any required transfer risk assessment and apply supplementary measures where appropriate.

12. Security

PRG uses appropriate technical and organisational measures designed to protect candidate information against accidental or unlawful destruction,

loss, alteration, unauthorised disclosure or access. Measures may include role-based access, multi-factor authentication, secure transfer methods, encryption or password protection where appropriate, logging, monitoring, backups, supplier controls, staff training and incident response.

13. Retention and deletion

PRG retains candidate information only for as long as necessary for the relevant recruitment, placement, legal, regulatory or dispute-management purpose and in accordance with its Data Retention and Erasure Policy and Schedule. Unsuccessful application records are generally retained for up to six months unless a different period is justified and documented, or you agree to remain in a talent pool. Placement, compliance, right-to-work, contractual and financial records may be kept for longer where required by law or legitimate business needs.

PRG periodically reviews candidate records and will delete, anonymise or securely archive information when it is no longer required. Normal deletion may be suspended for a legal hold, complaint, rights request, regulatory enquiry, investigation or legal claim.

14. Your rights

Depending on the circumstances and applicable law, you may have the right to:

- Be informed about how your information is used.
- Request access to your personal information.
- Request correction of inaccurate or incomplete information.
- Request erasure where the legal conditions are met.
- Request restriction of processing.
- Object to processing based on legitimate interests or to direct marketing.
- Request portability of information you provided where the legal conditions are met.
- Withdraw consent where processing is based on consent.
- Request human intervention and challenge qualifying solely automated decisions.
- Complain to PRG and to the Information Commissioner's Office.

Rights are not absolute. PRG may verify identity, clarify a request, apply legal exemptions and protect the rights of other individuals. Rights requests are handled under PRG's Subject Access Request Procedure.

15. Complaints

If you have concerns about how PRG handles your personal information, please contact the Data Protection Lead. PRG will record and investigate data protection complaints through its complaints process. This does not affect your right to complain to the Information Commissioner's Office or seek a judicial remedy.

16. Contact details

Contact	Details
Controller	Precision Resource Group Limited
Data Protection Lead	Louise Leyden-Ahmed
Postal address	Data Protection Lead, Precision Resource Group Limited, St Bartholomew's House, Lewins Mead, Bristol, BS1 2NH
Telephone	0117 332 8080
Regulator	Information Commissioner's Office, the UK data protection regulator.

17. Changes to this notice

PRG may update this notice to reflect changes in law, guidance, technology, suppliers, systems or recruitment activities. Material changes will be communicated through an appropriate channel, and the current version will be made available through PRG's approved publication route.

18. Related documents

- PRG Data Retention and Erasure Policy and Schedule.
- PRG Subject Access Request Policy.
- PRG Information Security Policy.
- PRG Information Classification Policy.



- PRG AI Acceptable Use Policy.
- PRG Data Breach Procedure.
- Relevant recruitment, screening, complaints and records-management procedures.