



Recruitment Privacy Policy

Pro2col Ltd

Managed File Transfer Specialists

Devonshire Suite, Saxon Centre, Christchurch. BH23 1PZ

0333 123 1240 | info@pro2colgroup.com

Company Registration No. 5038052 | VAT No. 831 2965 29

Recruitment Privacy Policy

Pro2col Limited is registered in England and Wales under company number 05038052, with the registered address Devonshire Suite, Saxon Centre, Christchurch, Dorset, BH23 1PZ.

Scope

This Recruitment Privacy Policy explains how we collect and use personal data during our recruitment and hiring process. It applies to:

- Job applicants and candidates (including those who apply directly via our website, job boards or third-party platforms or who are approached by us).
- Referees and contacts provided by candidates.
- Recruitment agencies supplying candidate information to us.

We are a data 'controller' for this information. This means that we are responsible for deciding how we hold and use personal data about you.

This policy does not cover existing employees, see our Employee Privacy Policy for more information.

Please make sure that you read this policy together with any other related information or policies/notices that we may provide to you from time to time so that you know how and why we are using such information.

We have appointed Richard Auger to be our Data Protection Officer to oversee compliance with this privacy policy. If you have any questions about this privacy policy, or how we handle your personal information, please contact that person at the address given below in Contact us.

The data we collect

Candidates

We may collect and process the following categories of data:

- Identification and contact information, such as, name, title, address, email, phone, LinkedIn/portfolio links, work authorisation/visa status.

- Application details, such as CV/resume, cover letter, application answers, salary expectations, notice period, desired working pattern, location preferences.
- Experience and qualifications, such as employment history, education history, certifications, professional memberships, skills, publications, awards.
- Assessment data, such as interview notes, task/technical test results, presentations (where applicable).
- Right to work screening, including documentation checks e.g. passport, visa, BRP (in line with legal obligations).
- Background checks, such as references, criminal record checks (where lawful and relevant for the role).
- Diversity and inclusion: information you choose to provide on characteristics such as ethnicity, disability, gender identity, sexual orientation, religion or belief (used for monitoring and equal opportunities).
- Other relevant information as applicable and as required by us in order to ensure that we fulfil our obligations as a prospective employer.

Referees and agency contacts

- Referees: information such as name, contact details and professional relationship to the candidate.
- Recruitment agencies: information such as consultant name, contact details, candidate submissions, communications and agreed terms.

Sources of personal data

- Directly from you (CV, interviews, emails, messages, calls).
- Third parties at your direction: recruitment agencies or platforms that you use or authorise.
- Public sources: professional networking sites, such as LinkedIn, publications, portfolios, conference talks, company websites.
- Verification and vetting partners: background-check providers, identity verification services, referees and former employers.
- Our systems: applicant tracking systems, email, scheduling tools and collaboration platforms used in the hiring process.

Purposes of processing and lawful basis

We process personal data only where we have a lawful basis. Depending on context, this may include:

Purposes of processing	Lawful basis
To manage recruitment and evaluate your application (reviewing CVs, scheduling interviews, assessing skills and suitability, communicating with you).	Legitimate interests (to recruit talent and manage our business) and/or steps prior to entering a contract with you.
To run assessments, technical tasks and interviews (including remote interviews).	Legitimate interests and/or steps prior to entering a contract.
Right to work checks and legal compliance (identity/immigration verification, regulated industry checks where required).	Legal obligation.
Background screening relevant to the role (e.g. references, criminal record checks where permitted).	Legitimate interests and where special category and/or criminal records data is involved: substantial public interest or other condition permitted by applicable law. We will only do this where lawful, proportionate and relevant.
Diversity and equal opportunities monitoring (voluntary).	Explicit consent or substantial public interest for equality of opportunity monitoring (as permitted by applicable law). We will present this clearly where used.
To maintain talent pools (considering you for future roles similar to those you applied for).	Legitimate interests. You may object at any time (see Your rights).
To defend legal claims and ensure security (audit trails of recruitment decisions, access logs, system integrity).	Legitimate interests and/or legal claims.
Corporate Purposes.	For corporate purposes such as finance or as transactions with third parties where information may be exchanged on a strictly confidential basis.

Please be aware that, if you do not provide us with certain information when requested, we may not be able to ensure that we are able to give full consideration to your potential employment by us, or we may be prevented from complying with our legal obligations. In some cases, you will be under a duty to supply us with certain personal data in order to satisfy your and our legal obligations.

We confirm that your personal data will only be used for the purposes for which it was collected, except in those circumstances where we reasonably consider that it needs to

be used for another reason, and that reason is compatible with the original purpose. Should we need to use your personal data for an unrelated purpose, we will notify you, and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Special category and criminal records data

We only collect special category data (e.g. health/disability adjustments for interviews) or criminal records data (where lawful and relevant) when necessary and subject to appropriate safeguards and legal conditions. We limit access, apply stricter retention, and typically aggregate/anonymise for reporting.

Who we share data with

It may be necessary for us to share your personal data with others so that we can carry out the recruitment process, or to comply with legal or regulatory obligations to you or that we are subject to.

We share personal data on a need to know basis with:

- Internal teams involved in hiring (HR team, recruiting managers, interviewers, executive approvers).
- Service providers (scheduling/video platforms, background check vendors, identity verification providers, cloud hosting and IT support).
- Referees and former employers (to obtain references and to obtain employment background checks from third-party providers, where applicable).
- Regulators or authorities (where required by law e.g. right to work compliance).
- Group companies for centralised recruitment or where a role may sit in another entity.

Where possible, we require our service providers to protect data under appropriate contractual terms.

International transfers

If personal data is transferred outside the UK/EEA, we will ensure an adequate transfer mechanism is in place (e.g. adequacy regulations/decisions, International Data Transfer

Agreement (IDTA), EU Standard Contractual Clauses (SCCs) with UK Addendum) and we will assess local laws and implement additional safeguards where appropriate. You can request details of relevant safeguards (see Contact us).

Retention periods

- Unsuccessful candidates: kept for six months after the hiring decision to evidence fair recruitment, manage queries or complaints made by you or on your behalf and consider you for similar roles (unless you object).
- Legal claims: to establish, exercise or defend a legal claim.
- Compliance: to comply with legal and regulatory requirements.
- Talent pool (if you consent and opt-in): two years or until you withdraw.
- Successful candidates: retained during employment and six years afterward.

Please note, however, that different periods for keeping your personal data will apply depending upon the type of data being retained and the purpose of its retention.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

How we store your data

We apply technical and organisational measures appropriate to the risks, including access controls, role-based access to HR systems, audit logging, staff confidentiality obligations and vendor due diligence.

Personal data that is processed by us will not be retained for any longer than is necessary for that processing, or for purposes relating to or arising from that processing, or under any timescale permitted under this policy. How long we retain your personal data will depend on whether your application is successful and you become employed by us, the nature of the information concerned, and the purposes for which it was acquired.

Recruitment information, including any notes made during your interview, will be kept for no longer than is reasonable, taking into account the limitation periods for potential claims, such as race or sex discrimination, after which they will be destroyed. Should there be a proper business reason for retaining recruitment records beyond the period of your recruitment, we may do so, but will always try and ensure that such data is retained in an anonymised form.

Your rights

Data protection legislation gives you, the data subject, various rights in relation to your personal data that we hold and process. These rights are subject to specific time limits in terms of how quickly we must respond to you. You have the following rights:

Access.	The right to obtain from us confirmation as to whether or not personal data concerning you is being processed, and, where that is the case, access to that personal data and various other information, including the purpose for the processing, with whom the data is shared, how long the data will be retained, and the existence of various other rights.
Rectification.	The right to obtain from us, without undue delay, the putting right of inaccurate personal data concerning you.
Erasure (also known as the right to be forgotten).	Sometimes referred to as the right to be forgotten, this is the right for you to request that, in certain circumstances, we delete data relating to you.
Restriction of processing.	The right to require us to restrict processing of your personal data in certain circumstances (particularly where we rely on legitimate interests or for direct outreach).
Data portability.	The right to receive the personal data you provided to us, in a structured, commonly used and machine readable format and/or transmit that data to a third party in certain circumstances.
To object.	The right to object to your personal data being processed in certain circumstances (particularly where we rely on legitimate interests or for direct outreach).
Not to be subject to automated individual decision making.	The right to not be subject to decisions based solely on automated processing,

	including profiling, that produce legal or similarly significant effects (we do not make purely automated hiring decisions, see Automated decision making).
The right to withdraw consent.	If you have provided us with a consent to use your personal data you have a right to withdraw that consent at any time. Withdrawing a consent will not affect the lawfulness of our use of your personal data in reliance on that consent before it was withdrawn.

Full details of these rights can be found in the UK GDPR or by reference to guidance produced by the Information Commissioner’s Office.

To exercise your rights, contact us using the details in Contact us. We will respond within applicable statutory timeframes. You may be asked to verify your identity.

Your responsibilities

- You must ensure that the information which you supply to us is correct and up to date.
- Where necessary, you must check that third parties mentioned by you, for example, referees, have agreed to be referred to.
- You need also to update us if there are any material changes to the information you supply.

Contact us

If you have any queries as to the acquisition, use, storage or disposal of any personal data relating to you please contact:

- Email: dpo@pro2colgroup.com
- Post: Devonshire Suite, Saxon Centre, Christchurch, Bournemouth, BH23 1PZ
- Our Data Protection Officer

Notwithstanding our best efforts, inevitably, sometimes things do go wrong. If you are not satisfied with our response or any aspect of the way in which we have used and/or protected your personal data, you have the right to make a complaint with the Information Commissioner’s Office (ICO), who may be contacted:

- In writing at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
- Online at www.ico.org.uk
- By telephone on 0303 123 1113

Automated decision making

We may use tools to assist screening e.g. structured scoring, but we do not make hiring decisions solely by automated means that have legal or similarly significant effects. Human review is always involved.

Recruitment agencies and referrals

- Agencies must have a current written agreement with us before submitting candidates. Unsolicited submissions may be treated as non-fee-bearing.
- By submitting candidate data, agencies confirm they have a lawful basis, required notices/consents and that the data is accurate, relevant and up to date.
- We may share limited feedback on submissions to improve candidate matching and fulfil contractual obligations.

Changes to this policy

This policy was published on 23rd February 2026 and last updated on 23rd February 2026.

The terms and provisions of this privacy policy may be changed, updated and amended from time to time. If we do so during the period of your recruitment, we will inform you of those changes, where appropriate.

If you would like this policy to be supplied to you in another format, please contact the Data Protection Officer.