

PRIVACY NOTICE

How Papillon Talent Strategy Ltd handles your personal data

Controller	Papillon Talent Strategy Ltd, company number 11252560, registered in England and Wales
Registered address	1 Foxhill Crescent Camberley Surrey Gu15 1PR
ICO registration	ICO:00012249523
Data protection contact	emma@papillontalentstrategy.com

Papillon Talent Strategy Ltd ("Papillon", "we", "us") is a recruitment business. We introduce candidates to employers for permanent roles in the United Kingdom. Handling personal data is the core of what we do, so we take it seriously.

This notice explains what personal data we collect, why we use it, who we share it with, how long we keep it and what rights you have. We are the **controller** of the personal data described here, which means we decide why and how it is used.

If you only want to know one thing: we will never sell your data, and we will not send your details to an employer without telling you first.

1 WHO THIS NOTICE APPLIES TO

This notice applies to you if you are:

- a candidate or work-seeker whose details we hold, whether or not you have applied for a specific role;
- a referee nominated by a candidate;
- a contact at a client or prospective client company;
- a supplier, contractor or professional adviser to Papillon;
- someone who visits our website or contacts us by email, telephone or social media; or
- someone applying for a job at Papillon itself.

2 WHAT PERSONAL DATA WE COLLECT

2.1 For candidates and work-seekers, we typically hold:

- name, postal address, email address and telephone numbers;
- your curriculum vitae, employment history, qualifications, training and professional memberships;
- current and expected salary, notice period and availability;
- nationality and confirmation that you are entitled to work in the United Kingdom;
- interview notes, assessment results and feedback from clients;
- references and the details of your referees;
- correspondence between us; and
- details of roles you have been introduced to and the outcome.

- 2.2 For client contacts and suppliers, we typically hold name, job title, business contact details, correspondence and records of the assignments and invoices between us.
- 2.3 For website visitors, we collect technical data such as internet protocol address, browser type, pages viewed and the time of your visit. See Clause 12.

3 SPECIAL CATEGORY AND CRIMINAL OFFENCE DATA

- 3.1 Some data needs extra protection under Article 9 of the UK GDPR. We only collect it where we genuinely need to, and it is usually limited to:
- health information, where you tell us about a disability or condition so that reasonable adjustments can be made to a recruitment process under the Equality Act 2010;
 - racial or ethnic origin, religion, sex and sexual orientation, where a client asks us to gather anonymised equal opportunities monitoring data; and
 - trade union membership, where it is relevant to a role.
- 3.2 Our condition for processing this data is usually Article 9(2)(b) of the UK GDPR together with paragraph 1 of Schedule 1 to the Data Protection Act 2018, which covers employment obligations, or Article 9(2)(a) where you have given explicit consent. Where a client asks for equal opportunities monitoring, we rely on paragraph 8 of Schedule 1.
- 3.3 We do not routinely process criminal offence data. Where a role requires a check with the Disclosure and Barring Service, that check is arranged and held by the client as the employer, not by us.

4 WHERE WE GET YOUR DATA FROM

We collect personal data:

- directly from you, when you send us a curriculum vitae, register with us, speak to a consultant or complete a form;
- from job boards and application tracking systems you have chosen to use;
- from publicly accessible professional networking sites and company websites;
- from referrals and recommendations by colleagues, clients or other candidates; and
- from referees you have nominated.

Where we obtain your details from a public source or a referral rather than from you directly, we will tell you within one month of collecting them, or sooner if we contact you before then, as required by Article 14 of the UK GDPR.

5 WHY WE USE YOUR DATA AND OUR LAWFUL BASIS

We must have a lawful basis under Article 6 of the UK GDPR for everything we do with your data. Ours are set out below.

Purpose	Data used	Lawful basis
Finding you suitable roles	Contact details, curriculum vitae, work history, salary expectations	Legitimate interests: running a recruitment business and matching candidates to vacancies

Purpose	Data used	Lawful basis
Introducing you to a client	Curriculum vitae, interview availability, salary expectations	Legitimate interests, having first informed you and taken your agreement to the introduction
Taking up references	Referee details, employment history	Legitimate interests, or consent where you have given it
Keeping you on our database for future roles	All candidate data	Legitimate interests, subject to your right to object under Clause 13
Managing the client relationship	Client contact details, correspondence, assignment records	Performance of a contract, or legitimate interests
Invoicing and accounts	Client contact and payment details	Performance of a contract and legal obligation
Keeping recruitment records	Candidate and client records listed in Schedules 4 and 5 to the Conduct Regulations	Legal obligation under the Conduct of Employment Agencies and Employment Businesses Regulations 2003
Marketing by email	Name and email address	Consent, or the soft opt-in under the Privacy and Electronic Communications Regulations 2003 for existing clients
Defending legal claims	Any relevant record	Legitimate interests: establishing, exercising or defending legal claims

Where we rely on legitimate interests, we have carried out a balancing assessment weighing our interests against your rights. You can ask for a summary of that assessment using the contact details in Clause 16.

6 WHO WE SHARE YOUR DATA WITH

We share personal data with:

- clients and prospective employers, but only with your knowledge and only for the specific role discussed with you;
- referees you have nominated;
- our information technology, cloud hosting, applicant tracking and email providers, who act as our processors under a written contract;
- our accountants, auditors, insurers and legal advisers;
- background screening or referencing providers, where you have been told and a check is required for a role; and
- regulators, law enforcement and courts, where we are required to do so by law.

We do not sell your personal data, and we do not share it with third parties for their own marketing purposes.

When we introduce you to a client, that client becomes an independent controller of your data and decides for itself how it will use it. The client is responsible for its own privacy notice and for any right to work check it carries out. Our terms of business require clients to use your data only for the role you were introduced for.

7 SENDING DATA OUTSIDE THE UNITED KINGDOM

- 7.1 We store personal data in the United Kingdom and the European Economic Area wherever we can. Some of our technology suppliers process data outside those areas.
- 7.2 Where a transfer outside the United Kingdom takes place, we rely on one of the safeguards in Chapter 5 of the UK GDPR: adequacy regulations made by the Secretary of State, the International Data Transfer Agreement, or the United Kingdom addendum to the European Commission standard contractual clauses, supported by a transfer risk assessment.
- 7.3 If a client based outside the United Kingdom asks to see your details, we will tell you before we send them.
- 7.4 You can ask us for a copy of the safeguards we use, using the contact details in Clause 16.

8 HOW LONG WE KEEP YOUR DATA

Record	Retention period	Why
Candidate records where we have provided work-finding services	At least 1 year from the last service, then 2 years from last contact	Regulation 29 of the Conduct Regulations sets the statutory minimum. We then keep records so we can approach you about suitable roles
Candidate records where no service was provided	12 months from last contact	Speculative curriculum vitae that we do not act on are deleted sooner
Placement records and client contracts	6 years from the end of the assignment	Limitation Act 1980, for contractual claims
Invoices and accounting records	6 years from the end of the financial year	Companies Act 2006 and HM Revenue and Customs requirements
Equal opportunities monitoring data	Anonymised as soon as the process ends	No need to keep it in identifiable form
Website analytics	26 months	Standard analytics retention

We review our database periodically. If we have not heard from you and have had no reason to contact you within the retention period, your record is deleted or anonymised. You can ask us to delete your record sooner at any time, and we will do so unless we are required by law to keep it.

9 HOW WE KEEP YOUR DATA SECURE

We use access controls, encryption in transit and at rest, multi-factor authentication on business systems, regular backups and written contracts with our suppliers. Access to candidate records is limited to consultants who need it. We train our staff on data protection. No system is completely secure, but we take these obligations seriously and we will tell you and the Information Commissioner's Office about any breach that meets the reporting threshold.

10 AUTOMATED DECISION-MAKING

- 10.1 We do not make decisions about you based solely on automated processing that produce legal effects or similarly significant effects. A consultant reviews every shortlist and every decision not to progress a candidate.
- 10.2 Where we use software to sort, rank or search curricula vitae by keyword, that software supports a human decision rather than replacing it. Articles 22A to 22D of the UK GDPR, as amended by the Data (Use and Access) Act 2025, permit significant automated decisions only with safeguards including meaningful human review. If we ever change our approach, we will update this notice and tell you before it takes effect.

11 MARKETING

- 11.1 We send job alerts and market updates only where you have asked for them, or where you are an existing client contact and the message relates to services similar to those we have already provided.
- 11.2 Every marketing message contains an unsubscribe link. You can also ask us to stop at any time using the contact details in Clause 16. Opting out of marketing does not stop us contacting you about a live application.

12 COOKIES AND OUR WEBSITE

- 12.1 Our website uses cookies. Cookies that are strictly necessary for the site to work do not require your consent. Following section 112 of the Data (Use and Access) Act 2025, certain low risk analytics and functionality cookies also no longer require consent, provided you are given clear information and a way to object. All other cookies, including advertising cookies, are set only with your consent through the cookie banner.
- 12.2 You can change your cookie preferences at any time through the banner or your browser settings.
- 12.3 Our website may link to other sites. We are not responsible for their privacy practices, so please read their notices.

13 YOUR RIGHTS

Under the UK GDPR you have the right to:

- **be informed** about how we use your data, which is the purpose of this notice;
- **access** a copy of the personal data we hold about you;
- **rectification** of data that is inaccurate or incomplete;
- **erasure** of your data, where there is no good reason for us to keep it;
- **restrict processing** while a concern you have raised is resolved;
- **data portability** for data you gave us, in a machine readable format;
- **object** to processing based on legitimate interests, including profiling, and to direct marketing at any time; and
- **withdraw consent** at any time, where consent is the basis we rely on.

To exercise a right, contact us using the details in Clause 16. We respond within one month. Under Article 12A of the UK GDPR that period can be paused where we reasonably need to confirm your identity or clarify what you are asking for, and it restarts when you reply. We can extend it by up to two further months for complex requests, and we will tell you if we do.

When we deal with an access request, Article 15(1A) of the UK GDPR requires us to carry out a **reasonable and proportionate** search rather than an unlimited one. There is no charge unless a request is manifestly unfounded or excessive.

14 HOW TO COMPLAIN

Complain to us first. Since 19 June 2026, section 164A of the Data Protection Act 2018 gives you a statutory right to complain directly to us if you think we have breached data protection law, and requires you to raise it with us before going to the regulator.

- 14.1 You can complain by completing the form on our website at [INSERT URL], by email to [INSERT email address], or by post to our registered address.
- 14.2 We will acknowledge your complaint within 30 days of receiving it, investigate it without undue delay, keep you updated on progress and tell you the outcome.
- 14.3 If you are not satisfied with our response, or we do not respond, you can complain to the Information Commissioner’s Office:
 - Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
 - Helpline: 0303 123 1113
 - Website: ico.org.uk

We would rather hear from you first, so please give us the chance to put things right.

15 CHANGES TO THIS NOTICE

We review this notice at least once a year and whenever the law or our practices change. The version number and issue date are shown at the top. Where a change is significant, we will contact you directly rather than relying on you to check the website.

16 CONTACT US

Data protection contact	Emma McNamara
Email	emma@papillontalentstrategy.com

We are not required to appoint a Data Protection Officer, and we have not appointed one. The contact above is responsible for data protection at Papillon.