

VERTAGE Global Privacy Notice

Last updated: [10th September 2026] **Effective from:** [DD Month YYYY]

1. About this notice

Vertage Group and the companies within the Vertage Group are committed to protecting your privacy and handling personal data fairly, transparently, and securely.

This notice explains how we collect, obtain, use, share, retain and otherwise process personal data in connection with our recruitment, staffing, workforce management, consulting, technology platform, and related services.

It applies where you are:

- a candidate, prospective candidate, or other work-seeker;
- a temporary worker, agency worker, contractor, consultant, independent professional or other person seeking or undertaking an assignment;
- an individual supplied by, or representing, a recruitment supplier or other workforce provider;
- a client, prospective client, or client representative;
- a supplier, service provider, or business partner;
- a referee, emergency contact, dependent, beneficiary, or representative;
- a user of our websites, applications, portals, or digital platforms;
- a recipient of our marketing, event, or business communications; or
- another individual whose personal data we process in connection with our services or business operations.

This notice should be read with any country-specific supplement, candidate notice, worker or employee notice, platform notice, cookie notice, collection statement, or other privacy information provided when we collect personal data.

2. Who is responsible for your personal data?

The Vertage company responsible for your personal data depends on the brand, website, or platform with which you interact, your location, the service provided, the company that recruits, employs, engages or places you, and the company that contracts with the relevant client or supplier.

Website controller

For the operation of this website, the controller is:

Vertage. Registered address: First Floor, Mulberry House, 750 Capability Green, Luton, Bedfordshire, LU1 3LU, England.

Other group companies and controller roles

Another Vertage Group company may act as an independent controller or, where the purposes and means of processing are determined together, as a joint controller. In other arrangements, including certain recruitment process outsourcing or managed service arrangements, a Vertage company may process personal data on a client's instructions as a processor.

Where required, we will make information about the essential features of any joint-controller arrangement available to you.

3. How to contact us

Questions about this notice or the way we use personal data may be sent to:

dpo@vertage.com.

Where appropriate, you may also contact the relevant local group company using the details shown [on our group companies page](#).

4. Personal data we collect

The personal data we collect depends on your relationship with us, the services you use, the role or assignment involved, applicable law and relevant client requirements.

4.1 Candidates

We only collect personal data that is necessary to provide recruitment, work-finding and related workforce services to candidates, prospective candidates and work-seekers. This may include information needed to assess your suitability, match you with relevant opportunities, progress applications, introduce you to clients and, where applicable, establish and administer any resulting employment, assignment, consultancy, contractor or other working relationship. If you do not provide information that is necessary for these purposes, we may be unable to consider you for roles, progress your application or continue providing recruitment or work-finding services to you.

Personal data you give us directly

This may include:

- your name, address and contact details;
- your CV or résumé, employment history, qualifications, education and training;
- information about your skills, experience, certifications, licences and professional memberships;
- your current and expected salary, pay rate, benefits, notice period, availability and working preferences;
- information you provide in applications, cover letters, forms, questionnaires, assessments or during registration;
- notes or records from interviews, meetings, telephone calls, video calls or other communications with us, including transcripts or recordings where these are used;
- bank account, tax, payroll or payment information where needed for an assignment, engagement or placement; and
- any other information you choose to provide, such as a photograph, date of birth, nationality, emergency contact or next-of-kin details.

Sensitive or special category information

Where lawful, relevant and appropriate, we may also collect and use more sensitive information, such as:

- health, disability or medical information where needed to consider workplace adjustments, support requirements or fitness for a particular role;

- equality, diversity and inclusion information, such as ethnicity, gender, sexual orientation, religion or other diversity data, where permitted by law and usually on a voluntary basis;
- vaccination, health screening or occupational health information where required for specific roles, client sites or legal obligations; and
- criminal record, background check or vetting information where this is lawful, proportionate and relevant to the role or assignment.

Personal data we receive from other sources

We may also obtain information about you from third parties or publicly available sources, including:

- referees, former employers, educational institutions or professional bodies;
- screening, identity verification, right-to-work, qualification-checking or background-check providers;
- clients or prospective clients who provide interview feedback, role-specific feedback or assignment-related information;
- publicly available professional sources, such as LinkedIn, job boards, professional directories or online profiles;
- other recruitment agencies, managed service providers, recruitment process outsourcing providers, umbrella companies or workforce suppliers; and
- other Vertage Group companies where this is relevant to recruitment, work-finding, assignment management or related services.
-

Personal data collected when you use our websites, platforms or systems

- When you interact with our websites, apps, portals, online recruitment systems or marketing communications, we may collect technical and usage information, such as:
- IP address, device identifiers and approximate location information;
- browser type, operating system, device details and network information;
- dates, times and records of your access to our websites, platforms or online services;
- cookie, tracking and consent information, where applicable;
- records of pages viewed, jobs searched for or viewed, applications started or submitted, links selected and interactions with our online services; and
- engagement information from emails or marketing communications, such as whether a message was delivered, opened or selected.

General note

The categories above are intended to describe the types of personal data we may process and are not exhaustive. The information we collect will depend on your relationship with us, the services you use, the role or assignment involved, applicable legal requirements, client requirements and the choices you make when interacting with us.

4.2 Workers, contractors, consultants and independent professionals

- employment, engagement, assignment and contract documentation;

- payroll, tax, pension, bank-account, payment and benefit information;
- timesheets, attendance, expenses, leave, availability and location information;
- performance, conduct, grievance, complaint and disciplinary information;
- health and safety, accident, incident and insurance information;
- equipment, access, account and security records;
- training, accreditation and compliance records;
- company, registration, tax and insurance information for independent professionals; and
- emergency contact, dependant and beneficiary information.

4.3 Client and prospective-client contacts

- name, and professional contact details;
- recruitment, resourcing and workforce requirements;
- purchasing, contracting, billing and account information;
- enquiries, meetings, communications, service history and feedback;
- marketing preferences, event participation and content interests;
- publicly available professional information; and
- website, email and campaign engagement information.

4.4 Suppliers, workforce providers and business partners

- business contact, role and organisation details;
- contracting, invoicing, payment and bank information;
- due diligence, tax, insurance and compliance information;
- details of supplied professionals and authorised users;
- service, meeting, communication and complaint records; and
- building, platform, account and system-access information.

4.5 Website, application and platform users

- IP address and approximate location derived from it;
- device, browser, operating-system and network information;
- pages viewed, links selected, searches, referring website, dates, times and visit duration;
- cookie, consent, advertising and device identifiers;
- form submissions, account registration and profile information;
- login, authentication, chat and support interactions; and
- security, diagnostic, event and audit records.

Further information about cookies and similar technologies is available in our Cookie Notice at [Cookie Notice | Vertage](#)

4.6 Referees, emergency contacts and other individuals

Where another person gives us your details, we may collect your name, contact details, relationship with that person, reference or emergency information, and other information reasonably necessary for the stated purpose. The person providing your details should tell you that they have done so.

5. Where we obtain personal data from

We may obtain personal data:

- directly from you;

- when you use our websites, applications, portals or platforms;
- from candidates, workers, referees, emergency contacts or representatives;
- from clients, prospective clients, suppliers and workforce providers;
- from job boards, professional networks, CV databases and recruitment sources;
- from publicly available sources and professional profiles;
- from former employers, educational establishments, referees and professional bodies;
- from screening, identity, right-to-work, assessment and verification providers;
- from government, tax, immigration, law-enforcement or regulatory authorities;
- from other Vertage companies;
- through business development and marketing platforms, including HubSpot;
- through recruitment and workforce platforms, including Strive; and
- from technology systems that generate usage, security, matching, workflow or audit information.

Where required by law, we will provide relevant privacy information after obtaining your personal data from another source, unless an exemption applies.

6. How and why we use personal data

The table below describes our principal purposes and the legal bases typically relied upon under UK and EEA data-protection law. Other lawful bases or local-law provisions may apply in other countries.

Purpose	Typical information	Typical UK/EEA legal basis
Candidate registration and applications	Identity, contact, CV, qualifications, preferences and application history	contract; legitimate interests
Candidate sourcing and initial contact	Professional profile, experience, public-source and contact information	contract; legitimate interests
Searching, matching and recommending	Skills, experience, availability, location, preferences and role criteria	Legitimate interests; steps before contract
Candidate presentation and selection	CV, role-related details, assessments and recruiter observations	Legitimate interests; contract
Talent pools and future opportunities	Contact, CV, skills, preferences and engagement history	Legitimate interests; consent where required
Worker or contractor administration	Contract, assignment, payroll, tax, time, attendance and payment information	Contract; legal obligation
Right-to-work, identity and screening	Identity, immigration, qualifications, integrity and screening results	Legal obligation; legitimate interests; applicable special-condition
Workplace adjustments and occupational support	Health, disability and adjustment information	Employment-law obligations; substantial public interest; explicit consent where appropriate
Platform and marketplace services	Account, profile, applications, bids, contracts and platform activity	Contract; legitimate interests
Client service and relationship management	Business contacts, communications, requirements and service records	Contract; legitimate interests
Supplier and workforce-provider management	Contacts, contracts, payments, due diligence and supplied-worker information	Contract; legal obligation; legitimate interests
Marketing, events and business development	Professional contacts, preferences, engagement and interests	Consent or legitimate interests, subject to direct-marketing law

Purpose	Typical information	Typical UK/EEA legal basis
Website operation, forms and security	Device, network, account, form, consent and audit information	Legitimate interests; legal obligation; consent where required
Analytics, reporting and service improvement	Usage, interaction, operational and aggregated information	Consent or legitimate interests, depending on technology and jurisdiction
Fraud prevention and information security	Identity, access, device, network and audit information	Legitimate interests; legal obligation
Legal claims, complaints and audits	Relevant operational, contractual and communication records	Legitimate interests; legal claims; legal obligation
Corporate transactions and restructuring	Relevant business, due diligence and operational records	Legitimate interests; legal obligation
AI-assisted recruitment and administration	Role criteria, candidate, communication and operational information	Legitimate interests, contract or another appropriate basis, subject to assessment

Where we rely on legitimate interests, these may include delivering and developing recruitment and workforce services, identifying suitable professionals, responding to client needs, maintaining business relationships, protecting systems, preventing fraud, improving services, managing the group and exercising or defending legal rights. We balance these interests against the rights, interests and reasonable expectations of affected individuals.

If information is required by law or contract, or is necessary to enter into a contract, we will explain the consequences of not providing it where these are not already apparent.

7. Special-category, criminal-record and other sensitive information

Depending on the jurisdiction, sensitive information may include racial or ethnic origin, religious or philosophical beliefs, political opinions, trade-union membership, health or disability information, sexual orientation, genetic or biometric information, criminal allegations or convictions, government identifiers and financial-account information.

We process such information only where an additional legal condition applies, for example where processing is necessary for employment and social-protection law, substantial public interest, occupational health, legal claims, or another condition permitted by law. We use explicit consent only where it is appropriate, freely given and genuinely withdrawable.

Criminal-record and background-screening information is processed only where lawful, relevant and proportionate to the role, assignment, client requirement or regulatory obligation.

8. Recruitment technology, matching and artificial intelligence

We use technology to help deliver recruitment, workforce and platform services. Depending on the service, technology may assist with searching candidate records, identifying potentially relevant experience, matching role criteria to profiles, organising applications, detecting duplicates, creating summaries, scheduling communications, identifying incomplete information, detecting fraud or security risks, transcribing approved interactions, cross-checking information and analysing service performance.

Where we use AI or automated tools, we apply proportionate governance, due diligence, access controls, testing, data-minimisation measures and human oversight. We assess material risks, including accuracy, bias, explainability, security, confidentiality and the effect on individuals.

Material decisions

We do not make decisions that produce legal or similarly significant effects about candidates or workers solely by automated means. Technology may support our personnel, but an appropriately authorised person remains involved in material recruitment, placement, engagement and screening decisions.

If we introduce solely automated decision-making that has legal or similarly significant effects, we will provide specific information about the decision, the main factors and logic involved, likely consequences, applicable legal basis, and the available rights to obtain human intervention, express a view and challenge the outcome.

9. HubSpot, Strive and other systems

9.1 HubSpot

We may use HubSpot to manage professional and business contacts, website forms and enquiries, client and prospective-client relationships, marketing communications, communication preferences, live chat, meeting bookings, events, content downloads, campaign reporting and website engagement.

Depending on our configuration, HubSpot may process names, professional contact details, organisation and role information, correspondence, form responses, marketing preferences, IP addresses, device information, website activity and cookie or tracking identifiers. Optional tracking technologies will be used only in accordance with applicable cookie and electronic-marketing requirements.

9.2 Other recruitment and workforce platforms

We may use other recruitment, work-finding and workforce management platforms to support candidate or professional registration, vacancy and assignment applications, profile management, matching, onboarding, contracting, assignment administration, timesheets, document handling, worker communications and related workforce processes.

Depending on the platform and how it is configured, these systems may process identity and contact information, account and login details, CVs or professional profiles, work history, experience, skills, qualifications, application information, role and assignment preferences, onboarding and right-to-work documentation, communications, placement and assignment records, timesheets, availability, platform activity, audit records, and information generated through matching, workflow or administration processes.

9.3 Other service providers and systems

We may use providers supporting applicant tracking, candidate relationship management, payroll, invoicing, identity and right-to-work checks, screening, assessments, video interviewing, electronic signatures, document management, cloud hosting, communications, job advertising, sourcing, web hosting, analytics, security, workforce and vendor management, business intelligence and AI-assisted productivity or administration.

We may identify key providers where this materially assists transparency.

10. Direct marketing and communications

We may send information about services, events, insights, vacancies or business opportunities where you have consented, where applicable law permits communication within an existing relationship, or where we rely on legitimate interests and electronic-marketing law permits that approach.

You can opt out at any time using the unsubscribe option in a marketing email, changing your preferences by contacting us [on our group companies page](#). Opting out of marketing will not prevent service, contractual, legal, security or administrative communications.

We may measure whether an email is delivered, opened or selected, and use campaign engagement information to improve communications, where permitted and subject to required choices or consent.

11. Who do we share personal data with?

We may share personal data with:

- Vertage Group companies;
- clients and prospective clients;
- managed service, recruitment process outsourcing and workforce partners;
- recruitment suppliers and other providers of professionals;
- payroll, pension, benefits and payment providers;
- screening, identity, right-to-work and assessment providers;
- technology, hosting, communications, analytics and cybersecurity providers;
- professional advisers, auditors, insurers, banks and financial institutions;
- government, tax, immigration, law-enforcement and regulatory authorities;
- courts, tribunals and legal representatives;
- parties involved in a merger, acquisition, financing, restructuring or sale; and
- other recipients where you direct or authorise us to share information or where law permits or requires it.

We require processors acting on our instructions to protect personal data and use it only for authorised purposes. Clients, employers, suppliers, insurers and other organisations may act as independent controllers where they determine their own purposes and means. Their own privacy notices will apply to that processing.

12. International transfers

Vertage operates internationally. Personal data may therefore be accessed from, transferred to or stored in countries outside the country in which it was collected.

Where transfer restrictions apply, we use an appropriate mechanism, such as an adequacy regulation or decision, the EU Standard Contractual Clauses, the UK International Data Transfer Agreement or UK Addendum, binding corporate rules, an approved certification framework, another approved mechanism or a legally permitted derogation.

Where appropriate, we assess the laws and practices of the destination and implement supplementary technical, contractual or organisational measures. Information about applicable safeguards may be requested using the contact details above, subject to legitimate confidentiality and security restrictions.

13. How long do we retain personal data for?

We keep personal data only for as long as necessary for the purposes described in this notice, including to provide recruitment, work-finding, workforce, platform and related services, and to meet legal, regulatory, tax, payroll, accounting, immigration, audit, insurance, contractual and dispute-resolution requirements.

Retention periods vary depending on the type of information, our relationship with you, the relevant service, applicable legal limitation periods, statutory obligations, client requirements and local laws. For example, candidate and work-seeker records are usually kept for a limited period after your last meaningful contact with us, while records relating to assignments, payroll, tax, right-to-work checks, screening, contracts, audits, complaints or legal claims may be kept for longer.

As we operate across multiple countries, retention periods may differ between jurisdictions, including Belgium, the Netherlands, the United Kingdom and other regions. Where local law, client requirements or a country-specific notice requires a different retention period, we will apply the relevant local requirement.

When personal data is no longer needed, we will delete it, anonymise it, restrict it or securely archive it in line with our retention standards and applicable law. We may keep limited information where needed to respect opt-out requests, maintain suppression lists, evidence compliance, manage disputes or prevent fraud.

14. Security

We use appropriate technical and organisational measures designed to protect personal data against unauthorised or unlawful access, accidental loss, misuse, alteration, destruction or unauthorised disclosure. Measures may include access controls, authentication, encryption, network protection, logging, monitoring, secure development, staff training, supplier due diligence, incident management, resilience and business-continuity arrangements.

No system is completely secure. You should take reasonable care when sending information electronically and when using online accounts.

15. Your privacy rights

Depending on the law that applies and subject to legal conditions or exemptions, you may have rights to:

- receive information about our processing;
- access personal data we hold about you;
- correct inaccurate or incomplete personal data;
- Request deletion (with lawful exceptions)
- Restrict certain processing
- object to processing based on legitimate interests;
- object at any time to direct marketing;
- withdraw consent, without affecting earlier lawful processing;
- receive certain information in a portable format;
- obtain human intervention and challenge certain automated decisions; and
- complain to our data protection team or a data-protection regulator.

To exercise a right, contact the Global Data Protection Officer at dpo@vertage.com.

We may request information that is reasonably necessary to verify identity, clarify the request and locate relevant records.

Where a Vertage company acts only as a processor for a client, we may refer or forward the request to the relevant controller as appropriate.

16. Complaints and supervisory authorities

We encourage you to contact us first so that we can investigate and respond to your concern. You may also complain to the data-protection authority responsible for your location or the relevant Vertage company.

United Kingdom: Information Commissioner's Office - <https://ico.org.uk>.

European Economic Area - [Contact | European Data Protection Board](#).

17. Children and younger applicants

Our services are not generally directed at children. Where we lawfully provide apprenticeships, work-experience opportunities or other services involving younger people, we will provide age-appropriate information and safeguards and involve a parent or guardian where required by law.

18. Third-party websites and services

Our websites and platforms may link to websites, platforms and services operated by other organisations. Those organisations control their own privacy practices. You should review their privacy information before providing personal data.

19. Changes to this notice

We may update this notice to reflect changes in our organisation, services, systems, technologies or legal obligations. The current version will be published on this page. Where a change is material, we may provide additional notice through our website, platform, email or another appropriate channel.

Annex A: Country and regional supplements

The following supplements should be developed and linked where relevant:

- United Kingdom;
- European Economic Area, including specific Netherlands and Belgium provisions where needed;
- United States, including applicable state privacy disclosures;
- Canada;
- Australia and New Zealand;
- India; and
- other countries in which Vertage actively recruits, supplies personnel, operates a platform or markets services.