Client and Business Contact Privacy Notice

How Venn Group uses your personal information

This notice explains how Venn Group collects, uses, stores and shares personal information, how long it is kept and the rights individuals have under UK data protection law.

Who we are

Venn Group Limited is the data controller for the personal information described in this notice. This means Venn Group decides why and how that information is used, stored and shared.

Registered office: 1 London Bridge, London, SE1 9BG

Company number: 04015584

Data Protection Officer: Paul Hayward, Associate Director – Finance Operations and IT

Email: phayward@venngroup.com

Who this notice applies to

This notice applies to individuals we deal with as part of a client relationship, including hiring managers, procurement, finance and HR contacts, directors, and other employees or representatives of client organisations and prospective clients. It also covers business contacts such as suppliers, introducers and other third parties we deal with in the course of providing recruitment services.

It does not apply to candidates, agency workers, contractors or consultants, who are covered by our Candidate and Agency Worker Privacy Notice, or to employees working directly within Venn Group's internal business, who are covered by the Employee Privacy Notice.

Personal information we collect and use

Depending on our relationship with you and your organisation, we may collect and use:

- identity and contact information, including name, job title, employer, work address, telephone number and email address;
- details of your role and responsibilities, and your authority to instruct us on behalf of your organisation;
- recruitment requirements, vacancy details, role specifications, rates and terms discussed with you;
- correspondence, meeting notes, telephone and video call records, and other communications with us;
- feedback on candidates, agency workers, assignments and the services we provide;
- contractual, billing, invoicing, purchase-order and payment information relating to your organisation;
- attendance at events, marketing preferences and responses to our communications;
- information about use of our website, portals, communications and systems where relevant; and
- information needed for audits, fraud prevention, legal claims, regulatory requirements and business continuity.

Special category information

We do not usually need to process special category information (such as health or racial or ethnic origin data) about client and business contacts. If this becomes necessary, for example in connection with a

workplace incident or a reasonable adjustment for a meeting, we will identify an appropriate lawful basis and additional legal condition before using it, and apply appropriate safeguards.

Where information comes from

We usually obtain your information directly from you or your organisation, for example when you engage our services, provide a business card, or communicate with our consultants. We may also obtain information from your organisation's website, professional networking sites such as LinkedIn, publicly available business sources, referrals from colleagues or other contacts, and candidates or agency workers who name you as a contact in connection with an assignment.

If we obtain your information from another source, we will provide the information required by law within the applicable timeframe, unless an exemption applies.

Credit reference and affordability checks

To help us assess applications, prevent fraud, and meet out legal and regulatory obligations, we may obtain information about you from credit reference agencies (CRAs). We obtain this information via Creditsafe, which uses its data partner, TransUnion to supply consumer credit and identity data.

- Creditsafe Business Solutions Limited is authorised and regulated by the Financial Conduct Authority. FCA Firm Reference Number: 742313.
- TransUnion International UK Limited is authorised and regulated by the Financial Conduct Authority. FCA Firm Reference Number: 737740.

The information we receive may include data relating to your identity, credit commitments, payment history and public record information. This data us used solely for legitimate business purposes, including creditworthiness assessment, identity verification and fraud prevention, in accordance with applicable data protection laws.

Further information about how Creditsafe and TransUnion process your personal data can be found on their respective privacy notices:

- Creditsafe Privacy / Transparency Notice (Customers & Suppliers): https://www.creditsafe.com/gb/en/legal/transparency-notice-customer-supplier.html
- TransUnion Credit Reference Agency Information Notice (CRAIN): https://www.transunion.co.uk/legal/privacy-centre/pc-credit-reference
- TransUnion Bureau Privacy Notice: https://www.transunion.co.uk/legal/privacy-centre/pc-bureau

Why we use personal information and our lawful bases

The lawful basis depends on the purpose and information involved. The main purposes and likely lawful bases are summarised below. Venn Group's internal processing records identify the basis used for each activity.

Purpose	Likely lawful basis
Identifying, engaging and communicating with clients and prospective clients	Legitimate interests; consent where required by electronic-marketing rules
Setting up and managing the client relationship and any contract for services	Contract; steps before contract; legitimate interests
Understanding recruitment needs, discussing vacancies and progressing placements	Legitimate interests; contract

Sharing relevant candidate information with you and receiving your feedback	Legitimate interests; contract
Invoicing, payments, credit checks and financial administration	Contract; legal obligation; legitimate interests
Managing assignments, health and safety, complaints and incidents on-site	Contract; legal obligation; legitimate interests
Marketing our services and keeping you informed about relevant opportunities	Legitimate interests; consent where required by electronic-marketing rules
Audit, fraud prevention, safeguarding, legal claims and regulators	Legal obligation; legitimate interests; legal claims

Legitimate interests

Where we rely on legitimate interests, these may include operating and improving our recruitment services, maintaining and developing our client relationships, understanding and meeting your organisation's recruitment needs, managing assignments, keeping appropriate business records, protecting people, systems and information, preventing fraud and dealing with legal claims. We will balance these interests against your rights, interests and reasonable expectations.

When providing information is required

Some information is required so we can set up and manage the client relationship, agree and perform a contract for services, progress a recruitment requirement, or invoice and administer payment correctly. If required information is not provided, we may be unable to act on an instruction, progress a placement, or provide our services to your organisation.

Who we share information with

Where relevant and lawful, we may share your personal information with:

- candidates, agency workers, contractors and consultants, where this is relevant to a placement or assignment;
- other individuals within your organisation, or its group companies, where relevant to the relationship;
- umbrella companies, payroll and payment providers, banks and finance providers where relevant to a placement;
- managed service providers, recruitment process outsourcing providers and recruitment partners;
- group companies, authorised staff, IT, hosting, communications and document-management providers;
- auditors, insurers, legal advisers, credit-reference agencies and other professional advisers; and
- HM Revenue & Customs, regulators, courts, tribunals, law-enforcement bodies and other public authorities where required or permitted by law.

Some recipients, including your own organisation, may act as an independent data controller for their own use of your information. Where an organisation processes information on our behalf, we require appropriate contractual, confidentiality and security protections.

International transfers

Where personal information is transferred outside the United Kingdom, Venn Group will use a lawful transfer mechanism and any required safeguards. These may include UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to approved standard contractual clauses, or another safeguard permitted by law. You may ask for information about the safeguards relevant to your information.

Security

Venn Group uses appropriate organisational and technical measures designed to protect personal information against accidental or unlawful loss, alteration, disclosure, access or destruction. Access is limited according to business need and is subject to confidentiality and security responsibilities.

Retention

We keep personal information only for as long as reasonably necessary to manage the client relationship, perform any contract, and meet our legal, tax, regulatory, audit and dispute-related obligations. Periods vary by record type and relationship and are set out in our approved retention schedule. We may retain relevant contact information so we can continue to provide services or contact you about relevant opportunities, where this remains lawful and reasonable. You may object to this use at any time. Information will then be securely deleted, destroyed or anonymised unless a lawful reason requires longer retention.

Automated decisions

We do not currently use your personal information to make decisions based solely on automated processing that produce legal or similarly significant effects. If this changes, we will provide the information and safeguards required by law, which may include the right to obtain human intervention, express your point of view and challenge the decision.

Your rights

Subject to legal limits and exemptions, you may have the right to:

- be informed about the use of your personal information;
- access your personal information and receive a copy;
- ask us to correct inaccurate or incomplete information;
- request erasure or restriction in certain circumstances;
- object to processing based on legitimate interests and to direct marketing;
- receive and transfer certain information where data portability applies; and
- withdraw consent where consent is the lawful basis.

These rights do not apply in every situation. We may verify your identity and ask for information to clarify a request. We will respond within the time required by law.

Complaints

You can raise a data protection complaint with the Compliance Team at dataprotection@venngroup.com. We will acknowledge the complaint within 30 days, take appropriate steps to investigate it without undue delay, keep you informed of progress and tell you the outcome.

You also have the right to complain to the Information Commissioner's Office, the UK supervisory authority. You do not have to complete Venn Group's internal complaints process before contacting the ICO.

Changes to this notice

We may update this notice when our services, processing activities, systems, suppliers or legal obligations change. The current version will be made available, and material changes will be brought to the attention of affected individuals where appropriate.

Sign off

Policy Owner:	Paul Hayward
Signature:	
Last review:	01/09/2026
Next review:	01/09/2027