

Via Match: Business Customer Privacy Notice

United Kingdom.

Version 3.5. Last updated: 20 August 2026. Prior versions available on request.

Who we are

We are Via Match Limited ("Via Match", "we", "us" or "our"), a company registered in England and Wales. Our company registration number is 16530334 and our registered office is at 3 Copthall Avenue, London, United Kingdom, EC2R 7BH.

Via Match is the controller of your personal data and responsible for it. This notice applies to the personal data of individuals connected with our business customers, meaning employers who subscribe to the Via Platform to access job slots and hire candidates. That includes anyone who registers a business account, accepts subscription or renewal terms, or is named as a hiring manager on a job posting. Where you accept terms on behalf of an organisation, references to "you" include you personally, including where an account has been created on your organisation's behalf by Via Match.

If you are a candidate using the Platform to find job opportunities, please see our separate Candidate Privacy Notice. Via Match is also the controller of candidate personal data, because candidates register directly with Via Match rather than being submitted to us by an employer. That relationship is governed by the Candidate Privacy Notice.

Some information described in this notice relates to your organisation

rather than to an identifiable individual (for example, company name, industry or logo) and is not "personal data" under UK GDPR. We describe it here for transparency, but it does not require a lawful basis in the way personal data does.

If you have any questions about this notice or our privacy practices, please contact us at privacy@viamatch.ai. You can also reach our customer service team at +44 (0)203 617 9746 or support@viamatch.ai.

Changes to this notice

We keep this notice under regular review. This version was last updated on 20 August 2026. Historic versions can be obtained by contacting us at privacy@viamatch.ai.

If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you. In this case, we may have to cancel a service you have with us but we will notify you if this is the case at the time.

The data we collect about you

Account and registration

- **Identity Data:** first and last name of the person who registered the account.
- **Contact Data:** email address.
- **Account Data:** password (hashed by our authentication provider)

Supabase and never visible to us in plain text), email confirmation timestamp, and last sign-in time.

Company profile

The following describes your organisation and is generally not personal data, except where it identifies an individual (for example, a sole trader operating under their own name):

- Company name, description, industry, size and year founded.
- Headquarters address and country.
- Website and social media profiles (LinkedIn, Facebook, Instagram, X).
- Logo (stored file).
- Registration email domain, used to verify and enforce one account per company.
- Marketing opt-in preference.

Hiring activity

This category includes personal data about your staff (such as a named hiring manager) and, where messages are exchanged, personal data about candidates. Candidate data referenced here is controlled by Via Match under our Candidate Privacy Notice and is described here only to explain what we hold on our customer side.

- Job postings: title, description, benefits, salary, location and coordinates, contract type, IR35 status, and hiring manager name.
- Hiring priorities and requirements extracted from each role.
- Records of which candidates were shortlisted, and when.
- Messages exchanged with candidates: content, sender, timestamps and read receipts.

Billing

- Subscription details: plan, status, term dates, renewal date, auto-renewal status.

- Payment details: amount, currency, dates, payment method, failure reasons, refunds.
- Stripe customer, subscription and payment identifiers.

We do not hold your card details. These are held by Stripe; we only see the card's last four digits and card brand via Stripe.

Consent and acceptance

- Which documents were accepted, the version and URL served, the exact plan and contract dates shown, the timestamp, and the IP address the acceptance was recorded from.

Behaviour and analytics

- First dashboard visit, last visit per job, and which pop-ups or notices were dismissed.
- Product analytics events, collected via PostHog (hosted in the EU).

How is your personal data collected?

- **Direct interactions:** when you or your organisation register, subscribe, post jobs, message candidates, or accept checkout, subscription or renewal terms.
- **Automated technologies:** Technical Data, Consent and Acceptance Data, and Behavioural Data collected automatically as you use the Platform, including via cookies.

Cookies and tracking technologies

When you visit the Platform, we use cookies and similar tracking technologies to collect Technical Data and Usage Data. A cookie is a small text file placed on your device by a website you visit.

When you first visit the Platform, you will be presented with a cookie consent banner allowing you to accept or reject non-essential cookies. Your choice is stored in a cookie called "via-cookie-consent" for 30 days, after which we will ask you again.

- **Strictly necessary cookies** (via-cookie-consent, via-user-data, via-user-firstname): essential to the Platform's operation and cannot be switched off. The last two hold your signed-in identity and expire after 7 days.
- **Analytics cookies** (PostHog, hosted in the EU): used with your consent to understand how the Platform is used. Anonymous and aggregated only if you reject cookies.
- **Marketing cookies** (LinkedIn Insight Tag): used with your consent for advertising conversion tracking and audience building.
- **Testing cookies** (via-ab-id, via-ab-flags): set only while we are running a test of different versions of a page, so that you continue to see the same version. via-ab-id lasts for one year. No such test is running at the time of writing.

How we use your personal data

We will only use your personal data when the law allows us to. The lawful bases we rely on most commonly are:

- **Performance of a contract:** where we need to perform the subscription contract we have with your organisation.
- **Legitimate interest:** where it is necessary for our legitimate interests, and your interests and fundamental rights do not override those interests. Examples include demonstrating what was agreed and by whom, defending against or resolving disputes, and preventing duplicate accounts.
- **Legal obligation:** where we need to comply with a legal or regulatory requirement.
- **Consent:** where you have provided your consent, for example to receive marketing communications.

The specific purposes for which we use your data, and the lawful basis relied on for each, are set out in the Schedule at the end of this notice.

Automated decision-making

We do not make decisions about you (as a business customer) using solely automated means that produce legal or similarly significant effects on you.

The Via Platform includes an automated candidate-matching engine that generates shortlists of candidates against a role. It scores each candidate against the criteria you (or your team) set for that role, using a combination of fixed rules and large language models supplied by OpenAI. The criteria for each role are set by you, and their weighting and the instructions given to the models are set by us and do not change unless we change them. No candidate data is used to train those models.

Scores are produced by generative models, so a re-run would not necessarily return identical figures. This is why each score is calculated once, at the point a match is generated, and then fixed. A shortlist does not change after it has been produced. Every shortlist is reviewed by a senior member of the Via Match operations team before it is delivered to you, and the matching engine does not make hiring decisions.

Candidate personal data processed in this way is handled by Via Match as controller under our Candidate Privacy Notice.

If you would like more information about how our matching works, or a copy of our Data Protection Impact Assessment on this activity, please contact us at privacy@viamatch.ai.

Who else processes your data

We share your data with the following categories of recipient and named service providers. Each of these processes data on our written instructions under an Article 28 UK GDPR data processing agreement and is contractually required to protect it.

Provider	Purpose	Data involved	Location
Supabase	Database hosting and authentication	Account, company, hiring and consent data	US (safeguards: UK IDTA)
Vercel	Application hosting	All data transmitted via the Platform	US (safeguards: UK IDTA)
Stripe	Payment processing	Billing data. Card details are held by Stripe, not by us	Ireland (EU adequacy)
Brevo	Transactional email	Contact Data, email content	France (EU adequacy)
PostHog	Product analytics	Behavioural and Usage Data	EU (Frankfurt)
OpenAI	Drafting and parsing job descriptions from your input, and scoring candidate profiles against your role criteria as part of the matching engine. No data is used to train OpenAI's models	Job description and intake conversation content, role requirements, and candidate CV and profile data	US (safeguards: UK IDTA)
Google (Maps / Address)	Address lookup and geocoding of job locations	Job location data	US (safeguards: UK IDTA)
Trustpilot	Review invitations to customers who have opted in	Contact Data	Denmark (EU adequacy)

LangSmith	Logging and debugging of the AI calls the Platform makes, including job description drafting and candidate matching	The content of those calls, including job description inputs and candidate CV data	US (safeguards: UK IDTA)
-----------	---	--	--------------------------

An up-to-date list of our sub-processors, and the safeguards in place for each, is available on request from privacy@viamatch.ai.

We may also share your personal data with:

- Professional advisers including lawyers, bankers, auditors and insurers.
- HM Revenue & Customs, regulators and other authorities, where required.
- Subsidiaries or holding companies of Via Match, for general business and shared systems and services.
- Third parties to whom we may sell, transfer or merge parts of our business.

Where your organisation's company profile or job postings are visible to candidates, this is shown as part of the Platform's core recruitment-matching function. We do not sell or share this data for any other purpose.

International transfers

Some of the service providers listed above are located outside the UK, including in the United States. Where we transfer personal data outside the UK, we ensure an appropriate safeguard is in place, such as the UK International Data Transfer Addendum to the EU Standard Contractual Clauses, or a UK adequacy finding. Please contact us at privacy@viamatch.ai if you want further information on the specific mechanism used for a particular transfer.

Data security

We have put in place appropriate technical and organisational security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and are subject to a duty of confidentiality.

We have procedures in place to deal with any suspected personal data breach. Where we are legally required to do so, we will notify the Information Commissioner's Office within 72 hours of becoming aware of a notifiable breach, and will notify you and other affected individuals without undue delay where the breach is likely to result in a high risk to your rights and freedoms.

Data retention

We only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect of our relationship with you.

The specific retention periods we apply are:

- **Account and Company Profile data:** for the duration of your subscription plus 6 years after account closure, reflecting the standard limitation period for claims under English law.
- **Hiring Activity data** (job postings, shortlist records, candidate messages sent from your account): for the duration of your subscription plus 6 years after account closure. The same period applies on the candidate side under our Candidate Privacy Notice, because a shortlist record or a message thread is a single record shared between both parties.

- **Billing data:** 7 years from the end of the tax year in which the transaction occurred, in line with HMRC record-keeping requirements.
- **Consent and Acceptance data** (including IP address, accepted document versions and timestamps): for the duration of the contract plus 6 years, reflecting the standard limitation period for contract claims under English law.
- **Behavioural and Analytics data:** 24 months from the date of collection, in aggregated form thereafter.
- **Marketing consent records:** for as long as you remain opted in, plus 3 years after opt-out for suppression purposes.

Your legal rights

Under UK GDPR you have the right to:

- **Request access** to your personal data (a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Request correction** of inaccurate or incomplete personal data that we hold about you.
- **Request erasure** of your personal data where there is no good reason for us continuing to process it. We may not always be able to comply with your request of erasure for specific legal reasons, which will be notified to you at the time of your request.
- **Object to processing** of your personal data where we are relying on a legitimate interest and you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes.
- **Request restriction of processing** of your personal data in certain circumstances, for example while we establish the accuracy of the data.
- **Request the transfer** of your personal data to you or to a third party in a structured, commonly used and machine-readable format.
- **Withdraw consent** at any time where we are relying on consent to process your personal data. This will not affect the lawfulness of

any processing carried out before you withdraw your consent.

You will not have to pay a fee to access your personal data or to exercise any of these rights. We may, however, charge a reasonable fee or refuse to comply with your request if it is clearly unfounded, repetitive or excessive.

To exercise any of these rights, please contact us at privacy@viamatch.ai. We may need to request specific information from you to help us confirm your identity and to ensure your right to access your personal data. We try to respond to all legitimate requests within one month; occasionally it could take us longer if your request is particularly complex or you have made a number of requests.

Complaints

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK regulator for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO, so please contact us in the first instance at privacy@viamatch.ai.

Schedule: Purposes and lawful basis

The table below sets out the specific purposes for which we process your personal data and the lawful basis we rely on for each.

Purpose / Activity	Type of Data	Lawful basis for processing
To register your organisation and its users on the Platform	Identity Data, Contact Data, Account Data	Performance of a contract; Legitimate Interest (registration and access)

To verify and enforce one account per company	Registration email domain	Legitimate Interest (to prevent duplicate accounts and platform abuse)
To manage your subscription, billing and renewals	Billing Data	Performance of a contract; Legal obligation (accounting)
To record and evidence acceptance of contract, subscription and renewal terms	Identity Data, Contact Data, Technical Data (IP address), Consent and Acceptance Data	Performance of a contract; Legitimate Interest (to demonstrate what was agreed, and to defend against or resolve disputes)
To create and display job postings, and to match candidates from our platform against them using our matching engine	Hiring Activity Data	Performance of a contract; Legitimate Interest (operation of the Platform's core recruitment function)
To score and rank candidates against your role criteria using large language model tools	Hiring Activity Data; candidate CV and profile data	Performance of a contract; Legitimate Interest (operation of the Platform's core recruitment function)
To enable messaging between you and candidates	Hiring Activity Data (messages)	Performance of a contract
To build and display a company profile to candidates matched to your job opportunities	Company Data, Identity Data	Performance of a contract; Legitimate Interest (Platform matching function)

To generate draft job description copy from your inputs using large language model tools	Job description drafting inputs (customer content only)	Performance of a contract; Legitimate Interest (to assist customers in producing role descriptions)
To ensure compliance with legal and regulatory requirements	Any category of data, as necessary	Compliance with legal obligation
To enforce compliance with our terms and conditions and applicable law	Any category of data, as necessary	Legitimate Interest (protection of legal rights and platform integrity)
To administer and protect our business and the Platform	Account Data, Behavioural Data	Legitimate Interest (business administration, IT and network security, fraud prevention); Legal obligation
To send marketing communications and review invitations, where you have opted in	Identity Data, Contact Data, Marketing opt-in	Consent
To collect analytics data about Platform usage via cookies and tracking technologies	Behavioural Data	Consent (non-essential cookies); Legitimate Interest (anonymous or aggregated data only)

Explanation of terms

Consent means processing your personal data where you have signified your agreement by a statement or clear opt-in to processing for

a specific purpose. Consent will only be valid if it is a freely given, specific, informed and unambiguous indication of what you want. You can withdraw your consent at any time by contacting us.

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. You can obtain further information about how we assess our legitimate interests against any potential impact on you by contacting us at privacy@viamatch.ai.

Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal obligation means processing your personal data where it is necessary for compliance with a legal obligation that we are subject to.