

Candidate Privacy Notice

This notice describes how we collect, store, use, and share your personal information when you apply for a job with VikingCloud. It explains your rights regarding the personal information we hold about you.

This notice is applicable to all candidates globally.

Please note that we have layered this notice to simplify the content, which is in accordance with good practice guidance issued by the EU Data Protection Regulators. This means we have embedded links to further information at the appropriate point, to ensure this is easily accessible. We have checked these links to be authentic prior to publication.

Who we are

When we say 'we' or 'us' in this notice, we are referring to VikingCloud Group, on behalf of itself and its affiliates. Within VikingCloud Group, there are several entities which are employers and as such, would process your personal information as 'Data Controllers.' Please see your contract for the applicable entity, which will be one of:

- Australia – Viking Cloud (Australia) Pty Ltd
- Canada – Viking Cloud Canada, Inc.
- India – Sysnet Global Solutions India Private Limited
- Ireland – Sysxnet Limited
- Germany – Viking Cloud (Germany) GmbH
- Poland – Sysxnet Limited Spółka z ograniczoną odpowiedzialnością Oddział w Polsce
- South Africa – Sysxnet Limited
- Sweden – Viking Cloud Sweden AB
- U.K. – Sysnet Global Solutions (UK) Limited
- U.S. – Sysnet North America, Inc. and Viking Cloud, Inc.

What kinds of information do we collect about you?

As we are subject to a variety of legal regimes, the personal information we collect will vary depending on the country you are in. We have summarized the types of personal data below and highlighted the variances as applicable.

- Personal – your title, full name, home phone number, home email address and home address. In the United States, we record your racial/ethnic origin and if you're a veteran (for EEOC reporting, see **here** for further information).
- Education and Training – qualifications, training records and professional certifications where relevant to your job.
- Employment-related – CVs, work history/experience, references, salary expectations, employment dates.
- Government Identification Documents – your passport, driver's license or other government issued documentation (as permitted, based on your working country's requirements) to verify your identity and / or your right to work in the country. Such documentation usually includes your citizenship status and identification number(s).
- Reasonable adjustments – information regarding your health / disability and any changes to your work, which may be helpful for you considering your condition (it is your choice as to whether to share this information with us).
- Facilities Management – CCTV footage and building access logs. If you attend one of our office locations, we will record your name and the date/time of your visit in the visitor log. We also need to keep health and safety records in our offices. If you experience an accident on our premises, we will record your details and details of the accident.
- Monitoring – we monitor the use of our email system and retain system/application logs of access and / or changes to systems / data.
- Criminal Convictions – Where legally permissible in your country, we will process information relating to criminal convictions as part of our vetting procedures.

Where do we get your information?

The personal information we process we obtain directly from you, or your referees.

Depending on the practices applicable to your country, we will collect additional information about you from other sources:

- Screening – we use third-party services who provide us with the outcome of your background screening. They will request that you complete a consent form which details what information will be collected and processed (this is country specific).

How do we use your personal information, and what are our legal grounds?

In the European Economic Area (EEA), U.K., Philippines, and South African data protection / privacy laws require organizations to process personal information only where they have a 'legal basis' (i.e., our use of personal information must match one of the 'good reasons' mandated in the relevant law).

In the table below, you can see more details on these legal bases. However, please make sure you read the 'Use of your Information' column regardless of your location, as we explain the use of your information relating to all colleagues within this section.

In Australia, we need your express consent to collect sensitive information about you; to facilitate any reasonable adjustments you may require throughout the application process. We will ask you to provide details of any reasonable adjustments along with a statement that you consent to us processing this for the purposes of facilitating a fair recruitment process.

In Canada and India, we require your consent. This is different from consent under the GDPR. We will imply your consent by providing you with this Privacy Notice when you provide your information to us.

Legitimate Interests

Where we use legitimate interests as specified below, this means that we process your personal information for the interests of VikingCloud, or those of a third party such as our clients.

Whenever we use legitimate interests, we assess each process to ensure that we only process what is necessary. We'll also assess our interest against the rights and freedoms you have under the law, to ensure that we aren't doing anything which is unreasonable, unexpected, or overly intrusive.

You have the right to object to any processing that is done under legitimate interests, and, if you object, we will reassess our interests against your rights. If we have a compelling interest, then we may continue to process your information.

Reason for using your personal information	Legal basis
Recruitment Our HR team and hiring managers collect and review CVs to assess your suitability for the role you have applied for. Please remember that the candidate's CV stays stored in our database for an appropriate length of time, even if we do not decide to offer you a job within VikingCloud. If you would like us to remove the document, you can do this by contacting DataProtectionPrivacy@Vikingcloud.com .	Contract Your personal information is processed for the purpose of entering an employment contract with us.
Pre-employment / Continuous Screening We will request your permission to process information relating to criminal convictions, where your local law requires us to collect your consent as part of the vetting procedure. Note this is not the same as consent under the GDPR; we instead use legitimate interests as our legal grounds under the GDPR.	Legitimate Interests We need to meet client security requirements to sell and provide our services. In Ireland, there is no formal regime to access criminal records. If such checks are

In the following countries, we use a third-party screening service to conduct our vetting which verifies: Canada Address Education Employment Self-adjudication India Address Criminal history Education Employment Sanctions and enforcements Self-adjudication Ireland Education Employment Sanctions and enforcements Poland Education Employment Self-adjudication Sweden Criminal history Sanctions and enforcements Self-adjudication United Kingdom Criminal history Education	relevant to your role, we will request this information from you directly if you provide your explicit consent; you will receive a consent form explaining the process, your options and your rights.
--	--

Employment Sanctions and enforcements United States SSN SSN Trace Education Employment Criminal felony & Misdemeanor history Sanctions and enforcements National sex offender status Credit report In other countries, we do not conduct any checks other than checking you have a right to work in the country you're employed in.	
Monitoring We process information collected automatically through systems and applications that you use within the corporate network to maintain our security posture.	Legitimate Interests We need to prevent and detect events, incidents, and breaches along with maintaining our information security standards and certifications.
Facilities Management We process information collected through our CCTV (images) and building access systems (logs) to ensure the physical security of our premises is maintained. Where you visit an office location you are not primarily based in, we maintain visitor logs for building access.	Legitimate Interests We need to protect the security of our people, premises, and assets.
Health and Safety We process information relating to health and safety incidents to comply with our legal	Legal Obligation We have a legal requirement to manage health and safety in the workplace.

obligations. In Poland we conduct period OHS training where we will process the training you have attended and when you attended it.	
--	--

Online Tracking / Minors

Where permitted, we may set tracking technologies in accordance with the rules applicable to your jurisdiction for the websites that we operate. Please see our website [privacy notice](#) for further details.

We do not collect information relating to minors. Therefore, we do not sell or share personal information of consumers under 16 years of age.

Who do we share your personal information with?

We share your personal information with other organizations. The organizations we share personal information with will depend on your role, the systems you have access to, and the benefits provided to you. The organizations we share personal information with are as follows:

- Systems and technology providers:
- Recruitment – Jobvite Inc.
- Productivity tools – Microsoft Corporation (for Office 365, Teams, Purview and Intune)
- Endpoint Detection – SentinelOne
- Email Content Monitoring – Mimecast North America, Inc.
- Security Incident/Event Management – Rapid7, Inc.
- Screening providers.
- Professional services providers and consultants, such as contractors, external auditors, and lawyers.
- Insurance companies and brokers.
- Office services providers such as landlords.

We only share personal information where it is proportionate to do so, and where appropriate technical, organizational, and where necessary, contractual measures are in place to ensure its protection.

Overseas transfers

The information that we process about you will be primarily stored in the United States (where Jobvite is hosted), Ireland / the U.K. (where our Microsoft instances are hosted) and Germany (where many of our security tools are hosted from). It may also be stored or accessed by authorized individuals who operate in a variety of countries, or who work for us or for one of our suppliers.

If you are based in the EEA or U.K., we need to have specific protections in place to transfer your information to another country. We also need to let you know which methods we use:

- Some countries have been assessed by the relevant authorities as being 'adequate', which means their legal system offers a level of protection for your information which is equal to the level of protection in your country. This applies to some of our suppliers, as well as some of the transfers of information within VikingCloud (e.g. EU data stored in the U.K.).
- The EU Commissioner and the U.K. have also approved Binding Corporate Rules (BCRs) to protect information shared within a group of companies. This requires the group to commit to meeting European standards across all regions. These rules need to be approved by all the EU supervisory authorities or (for the U.K., the U.K. regulator) and require extensive monitoring and oversight they are authorized. Some of our suppliers have BCRs including ADP.
- Where the country or mechanism hasn't been assessed as 'adequate', the method we use most frequently is Standard Contractual Clauses (SCCs). These contract terms place EU standards onto companies in other jurisdictions. The European Commission approved standard contractual clauses are available via the link below, or let us know if you'd like more information; https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en
- We have SCCs in place to allow sharing between VikingCloud entities globally.

- We use SCCs for most of our service providers – we make sure we have contract terms and make checks of their practices / agree additional controls to ensure that your information is treated securely and in accordance with this Privacy Notice.

If you're based in a country outside of the EEA / UK, there may be local obligations with regards to the transfer. See below for details of the additional controls which we will apply to satisfy these:

- Canada – clear privacy notices explaining the transfer. We also need to tell you who to contact for more information. Please contact the Data Protection Team using details in the 'Contact' section below.
- India – at present, no restrictions are in place unless sensitive personal information is involved.
- South Africa – we must ensure a binding agreement is in place which ensures POPIA's principles are upheld including when further transferring personal information. South Africa has yet to issue approved contract terms, so we have extended the EU SCCs to cover your information.

How long do we keep personal information for?

Unless otherwise set out in this Privacy Notice, any information we process about you will be retained by us until we no longer need it for the purposes for which it was collected, as set out in this Privacy Notice. We will base that decision on criteria, including:

- Any legal or regulatory requirements to delete or retain the information for a specific period,
- Our legitimate business reasons for keeping the information, such as to analyze and assess our activities,
- The likelihood of a claim arising where we'd need to defend our conduct, and
- Whether the information is likely to remain up to date.

We will review and delete or destroy personal information on a regular basis. If we are unable, using reasonable endeavors, to delete or destroy personal information we will ensure that the

personal information is encrypted or protected by security measures so that it is not readily available or accessible by us.

We retain information processed by our CCTV systems for 90 days on a rolling basis.

Automated decisions / profiling

Automated decisions are decisions made by a computer or AI system without a human being directly involved. Profiling is the use of information about you to analyze or predict certain aspects, such as your likely reactions, preferences, or behavior.

We conduct profiling using Security Incident and Event Monitoring (SIEM) software to support security monitoring. This helps us understand what normal activity looks like so that unusual behavior, potentially indicating a security compromise, can be identified quickly.

All SIEM alerts are triaged by a person, and the insights from conversation intelligence are used solely for real-time coaching and support and will never be used for formal performance evaluation.

Security

We align to the International Standard for Information Security, ISO27001, as well as that relating to Privacy, ISO27701. This involves setting up a system to manage risk around both information security and data protection / privacy, as well as putting in place measures and objectives to keep improving.

An example of a measure we take is to enforce TLS1.2 when transferring information externally / to our suppliers; TLS1.2 is a network protocol for encrypting information in transit.

Access to your information is only provided to our people who have a need to know. We implement role-based access control so only those with a relevant role are given permission. We audit access on a regular basis.

Your rights

There are several rights available under global data protection and privacy laws. These do not usually require any fee, and we must respond within one (1) calendar month in most circumstances.

Not all rights apply in all situations, and some regions have different timeframes. If you require further details of timeframes and what applies in your jurisdiction, please contact our Global Data Protection Manager using the Contact details below.

The easiest way to exercise any of your rights is to enquire if a right is applicable in a specific circumstance or to check what timescales apply would be to contact our Data Protection Team as set out below.

If we need further information to comply with your request, including any identification, we will let you know. However, wherever possible, we will seek to identify you by way of information we already have; for example, if you contact us via the email address that you have registered with us, we will not normally need anything further (except if the data or the nature of the request is sensitive).

Right of access / right to know

You have the right to ask for access to and receive copies of your personal information. You can also ask us to provide a range of information relating to how we collect/use your information.

Right to rectification / right to correct

If you believe the personal information we hold about you is inaccurate or incomplete, you can ask us to correct that information.

Right of erasure / right to be forgotten / right to delete / right to anonymization

In some circumstances, you have the right to ask us to delete and/or anonymize personal information we hold about you.

Right to restrict processing / right to have information preserved

In some circumstances, you are entitled to ask us to restrict the processing of your personal information. This means we will stop using your personal information, but we will not delete it. Or you could ask us not to delete your information.

Data portability

You have the right to ask us to provide your personal information in a format that allows you to share your personal information with another provider.

Right to object

You are entitled to object to us processing your personal information if the processing is based on legitimate interests. You also always have the right to object to our use of your information for marketing purposes.

Right to non-discrimination

If you exercise your privacy rights, we will never discriminate against you for making a request. Under the CCPA, we are legally obliged to not discriminate in response to requests.

Changes to this Privacy Notice

This Privacy Notice Was last updated in July 2026.

Any changes we may make to the Privacy Notice in the future will be posted on this page and, where appropriate, notified to you by email. Please check back frequently to see any updates or changes.

Contact

Our Data Protection Team can be contacted using the following email address: dataprotectionprivacy@vikingcloud.com or alternatively by writing to 1st Floor Block 71A, The Plaza, Park West Business Park, Dublin 12.

Questions, comments, and requests regarding the Privacy Notice are welcomed and should be addressed to **dataprotectionprivacy@vikingcloud.com**.

If you have any concerns about the ways in which we process your personal information, in many countries you have a right to complain to the relevant supervisory authority in your jurisdiction. We'd encourage you to contact us first, so we can address your concerns (some regulators require this before they accept a complaint).

Please see below for details of the relevant regulators;

- Canada
 - Office of the Privacy Commissioner of Canada
<https://www.priv.gc.ca/en/report-a-concern/>
Telephone: 1-800-282-1376
- European Economic Area
 - EU regulators, plus those from Iceland, Liechtenstein and Norway
https://edpb.europa.eu/about-edpb/about-edpb/members_en
Telephone: See details in the link above.
- India
 - There is no regulator as such, the current law is overseen by the Ministry of Communication & Information Technology (Department of Technology)
- South Africa

- Information Regulator (South Africa)
<https://inforegulator.org.za/complaints/>
Telephone: 010 023 5200

- United Kingdom
 - Information Commissioner's Office (ICO)
<https://ico.org.uk/global/contact-us/contact-us-public/>
Telephone: 0303 123 1113