GARDA
CAPITAL PARTNERS

Global Data Protection Privacy Notice for Candidates

Introduction

Garda Capital Partners LP (together with its affiliates, "**Garda**") values your privacy rights and is committed to protecting personal information about you that personally identifies you ("**Personal Data**"), which we may collect and store. This Global Data Protection Notice (the "**Notice**") is addressed to any Candidate, defined as any job applicant for full or part-time employment, temporary staff positions, intern positions, contractors, and consultant positions at Garda.

By interacting with Garda, you acknowledge Garda's disclosure and sharing within Garda of your Personal Data and disclosing such Personal Data to Garda's authorized service providers and relevant third parties in the manner outlined in this Notice. For the purposes of the relevant data protection laws, Garda is known as a "data controller." This means that Garda exercises overall control over the purposes and means of the processing of Personal Data relevant to this Notice. Garda's contact details are provided at the end of this Notice.

This Notice provides information regarding your Personal Data processed in connection with this Notice, our purposes for processing it, the lawful basis on which Garda processes such data, your rights under applicable privacy laws, and how we protect your Personal Data.

Depending on your location, your Personal Data may be subject to: (i) EU General Data Protection Law, UK General Data Protection Regulation, and any other EU Member State and UK data protection laws (collectively, the "**GDPR**"); or (ii) the data protection laws of any other country, including Switzerland, Singapore, the United States and India, but only to the extent such laws are applicable to our processing of your Personal Data (collectively, "**Data Protection Laws**").

Information Collected

We collect Personal Data when you apply for employment positions via our website by submitting resumes, sending us candidate information directly, or via recruitment companies. Personal Data may come from sources such as your resume, application documents, compliance pre-employment questionnaires, references, background checking agencies (if applicable), and other forms of verbal, written, or electronic communication.

The Personal Data we may collect includes:

- "**Identity Data**": including first name, middle names, maiden name, last name, marital status, title, date of birth, passport number/identification card or other official identity number or document, social security number, tax identification number, IP addresses, photographs and images;
- "**Contact Data**": including billing address, delivery address, e-mail address, and telephone and/or mobile phone numbers;
- "**Financial Data**": including bank account details, compensation and bonus expectations;
- "**Resume and Professional Information Data**": including your current and historic job titles, work email address, current work phone number and address, previous positions and professional experience,

professional memberships, education, educational achievements, diplomas, languages, computer skills and cover letter (if relevant);

- "**Other Recruitment Data**": including any other information you may provide to us as part of the recruitment process such as current notice period, non-compete provisions for existing employer, work arrangements; draw limits, profit and loss target and capital allocations for portfolio manager positions (if relevant), as well as references from previous employers, which may be provided by you or obtained by Garda, disability status and interview notes;
- "**Screening Test Data**": including computer geolocation data (i.e. the country you are located when you take the test), IP address you use to take the test, user name created, email used, test results, recruitment scorecard and information provided by third party providers/systems on your performance on screening or selection tools;
- "**Communication Data**": including communications connected to potential employment and interviews;
- "**Background Check Data**": where applicable and legally permissible, which will include civil and criminal offences, employment, education, and certification and licensure verification where applicable performed prior to employment;
- "**Physical Security Data**": including information about your use of firm premises such as a visitor log, which may contain the time, location, and purpose of your visit; and
- "**Relocation Data**": including relocation preferences of you and your family members.

How Information is Used

We will only process your Personal Data when the law allows us to, that is, when we have a legal basis for processing. The section headed "Purposes and legal basis for which we will use your Personal Data" below, sets out further information about the legal basis that we rely on to process your Personal Data. Your Personal Data is primarily processed to ensure that we hire appropriately qualified people and people well-suited to our company culture to work for us, as well as communicating with Candidates to facilitate our recruitment process.

Subject to applicable laws, we will use your Personal Data in the following circumstances:

- "**Contractual Necessity**": to determine whether Garda wishes to enter into a contract with a Candidate;
- "**Legal or Regulatory Obligation**": where we need to comply with a legal or regulatory obligation that we are subject to;
- "**Legitimate Interests**": where necessary for our interests (or those of a third party), provided that your fundamental rights do not override such interests; and
- "**Consent**": where you have given us permission (generally, we do not rely on consent as the legal basis for processing your personal data).

Purposes and legal basis for which we will use your Personal Data

We set out below, in a table format, a description of the ways in which we use your Personal Data and the legal basis we rely on to do so. Where appropriate (and to the extent relevant under applicable law), we have also identified our legitimate interests in processing your Personal Data. We may process your Personal Data for more than one legal basis depending on the specific purpose for which we are using your Personal Data.

Purpose and/or activity	Type of Data	Legal basis for processing
Recruitment Communications: Communicating with you about the recruitment process, including pre-employment travel and lodging requirements.	• Contact Data • Relocation Data • Communication Data • Identity Data	• Contractual Necessity • Legitimate Interests: it is in our legitimate interests (and all other parties concerned) to evaluate whether you have the necessary skills and qualities to perform the relevant role.
Recruitment Decision: Carrying out our obligation to find qualified candidates that meet necessary suitability requirements for the financial services industry. Garda assesses your skills, qualifications, and suitability for the role to decide whether Garda will enter into an employment contract with you.	• It is possible it could involve all Personal Data categories above.	• Contractual Necessity • Legitimate Interests: it is in our legitimate interests (and all other parties concerned) to evaluate whether you have the necessary skills and qualities to perform the relevant role.
Contract Administration (creating employment contracts, right to work checks (where relevant)	• Contact Data • Identity Data • Financial Data • Resume and Professional Information Data • Background Check Data • Other Recruitment Data • Relocation Data • Communication Data	• Legal or Regulatory Obligation • Legitimate Interests: it is in our interests to ensure that those who work for us have the right to work in the country that they will be employed in, as well as to establish the statutory excuse to avoid liability for the civil penalty for employing someone without the right to undertake the work for which they are employed. • Contractual Necessity
Background Checks: Carrying out background, education verification and reference checks, where applicable.	• Contact Data • Financial Data • Resume and Professional Information Data • Other Recruitment Data • Communication Data	• Legal and Regulatory Obligations • Legitimate Interests: it is in our interests as well as the interest of our candidates/ employees/ workers/ contractors to

		ensure candidates are suitable to work for Garda.
Fraud and Crime Prevention: Preventing fraud and maintaining security.	• It is possible it could involve all Personal Data categories above.	• Legal and Regulatory Obligations • Legitimate Interests: it is in our interests as well as the interest of our candidates/ employees/ workers/ contractors to ensure the prevention of fraud and crime is monitored. This will ensure a safe workplace for all.
To Deal with Legal Disputes: Exercising and supporting legal claims and defense of rights.	• It is possible it could involve all Personal Data categories above.	• Legitimate Interests: it is in our interests to process Personal Data to make and defend legal claims to ensure that our legal rights are protected. • Legal and Regulatory Obligations
Processing of Expenses	• Contact Data • Financial Data	• Legitimate interests: it is in our interests and the interests of our applicants to ensure that any expenses properly incurred are reimbursed.
Legal and Regulatory Compliance: such as pre-employment compliance questionnaires	• It is possible it could involve all Personal Data categories above.	• Legal and Regulatory Obligations • Legitimate Interests: it is in our interests as well as the interest of our candidates/ employees/ workers/ contractors to ensure compliance with all legal and regulatory requirements.

We will only use your Personal Data for the purposes for which we collected it as detailed in the section "Information Collected", "How Information is Used" and in the table above, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to receive an explanation as to how the processing for the new purpose is compatible with the original

purpose, please contact us using the contact information below. If we need to use your Personal Data for an unrelated purpose, we will notify you and we will explain the legal basis that allows us to do so. Please note that we may process your Personal Data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law. We reserve the right to rely on legal purposes for processing data not otherwise set forth above.

Having received your resume, cover letter, application, and/or the results from any tests you took, we will then process that data to decide whether you meet the basic requirements for the role. If you do, we will determine whether your application is suitable to invite you for an interview. If we decide to call you for an interview, we will use the data you provide to us at the interview to determine whether to offer you the role. If we offer you the role, we may take up references and/or any other check before confirming your appointment.

If you fail to provide Personal Data

If you fail to provide Personal Data when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we may not be able to process your application further. For example, if we require references for this role and you fail to provide us with relevant details, we will not be able to take your application further.

How we use sensitive data

We will use your sensitive Personal Data only as permitted by law. If we process your special category personal data within the meaning of applicable data protection laws, at least one or more of the additional conditions for processing this type of Personal Data will apply:

- **Employment condition**: if the processing is necessary for the purposes of your or our obligations and rights in relation to employment insofar as it is authorized by law;
- **Legal claims condition**: if the processing is necessary for the purpose of establishing, making, or defending legal claims;
- **Healthcare condition**: if the processing is necessary for assessment of your capability for the role or where necessary to protect your vital interests where you are physically incapable of giving consent (e.g. to arrange emergency medical care);
- **Explicit consent**: if the processing has been explicitly consented by you.

If we process your background check data, we will only do so where this is necessary for us because of the role you are applying for and only to the extent that this is legally permissible. In some circumstances, we are required or entitled to carry out a criminal records check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role.

Automated Decision Making

You will not be subject to decisions that will significantly impact you based solely on automated decision-making.

Disclosure of your Personal Data

Garda does not share your Personal Data with any third parties for the purposes of marketing. Garda may share your Personal Data with certain non-affiliated third parties for the above purposes. All such third parties are required to maintain the security of such information to the extent they receive it. In certain instances, Garda may be legally obligated to share your Personal Data (e.g., upon receipt of a court order or regulator

request or to comply with legal requirements). Any transfer of Personal Data by us or our duly authorized affiliates and/or processors shall be by the requirements of the relevant data protection laws.

For example, personal information (and, in some cases, sensitive personal information) will be shared with:

- Applicant tracking software and hiring platforms;
- Compliance and HR databases;
- Third parties who conduct criminal record searches and other background checks (where permissible and by applicable law);
- Third parties who assist in facilitating travel arrangements in the event you are required to travel as part of the recruitment process and who need personal information necessary for travel;
- Third-party software providers, IT providers, cloud storage companies and cyber and email protection companies;
- Those who facilitate expense reporting and process expense reimbursements in the event you incur reimbursable expenses during the recruitment process;
- Auditors, advisors, legal representatives, and similar agents in connection with the advisory services they provide to us for legitimate business purposes and under a contractual prohibition of using the personal information for any other purpose.

Transfer of your Personal Data

Due to the global nature of our business, your Personal Data will be transferred to jurisdictions outside of your home jurisdiction. The level of information protection in countries outside of your home jurisdiction may be less than or different from that offered in your home jurisdiction.

Where we transfer your Personal Data outside of your home jurisdiction, we will ensure, where required, that Personal Data is protected and transferred by applicable legal requirements, which will usually be achieved by the following:

- the country to which we send Personal Data may be approved in your home country (e.g., by the European Commission, the Swiss Federal Data Protection and Information Commissioner, the UK Information Commissioner's Office or other supervisory authority (as applicable)) as having adequate data protection laws; or
- the recipient may have signed a contract based on standard contractual clauses approved in your home jurisdiction (e.g., by the European Commission, the Swiss Federal Data Protection and Information Commissioner, the UK Information Commissioner's Office or other supervisory authority (as applicable)), obliging them to protect your Personal Data.

Should you wish to obtain a copy of the applicable international transfer mechanism Garda uses where it is required to do so under applicable data protection laws, please contact us using the details provided below.

Security

Garda maintains appropriate physical, electronic, and procedural safeguards to protect your Personal Data. These measures are designed to: (a) safeguard Personal Data against loss, theft, unauthorized use, disclosure, or modification; and (b) ensure the integrity of Personal Data. We seek to restrict access to your non-public personal information to only those Garda employees or third parties who need access to that information. All Garda employees and service providers must maintain the confidentiality of non-public Personal Data. However, while we will endeavor to protect the security and integrity of your Personal Data, due to the inherent nature of the internet as an open global communications vehicle, we cannot guarantee that any

information will be safe from intrusion by others, such as hackers, during transmission through the internet or while stored on our systems or otherwise in our care.

If you contact us via email, you should know that your transmission mechanism might not be secure. A third party could view the information you send by these methods in transit. We will have no liability for disclosure of your information due to errors or unauthorized acts of third parties during or after you transmit it.

Data Retention

Garda retains personal data for varying time periods to assist us in complying with legal and regulatory obligations, to enable compliance with any requests made by regulators or other relevant authorities and agencies, to enable us to establish, exercise and defend legal rights and claims, and for other legitimate business reasons.

Garda retains your personal data for the period of time required for the purposes for which it was collected (or where permitted by applicable data protection laws any compatible purposes which we subsequently establish), any new purposes to which you subsequently consent, or where permitted or required to comply with legal, regulatory, and Garda policy requirements.

Your rights

Depending on the jurisdiction in which you are based, and subject to the applicable privacy laws, you may have certain rights available, such as:

- **Access to information** – The right to ask us for copies of your Personal Data.
- **Rectification** – The right to ask us to rectify Personal Data you think is inaccurate or to ask us to complete information you think is incomplete.
- **Erasure** – The right to request that we erase your Personal Data in certain circumstances.
- **Restriction of processing** – The right to object to the processing of your Personal Data in certain circumstances.
- **Data Access Portability –** The right to ask that we transfer the Personal Data you gave us to another organization or to you in certain circumstances.
- **Objection to processing** – The right to object to the processing of your Personal Data in certain circumstances.

These rights are not absolute; they do not always apply, and exemptions may be applicable. Individuals may also have the right to complain about the processing of Personal Data with a data protection authority. If you make a request to Garda related to Personal Data about you, you may be required to supply a valid means of identification as a security precaution. We will process your request within the time provided by applicable law.

For Singapore Candidates

By interacting with Garda during the recruitment process, you agree and consent to us collecting, using, disclosing, and sharing within Garda your Personal Data and disclosing such Personal Data to Garda's authorized service providers and relevant third parties in the manner outlined in this Notice.

Garda collects some additional Personal Data for Singapore Candidates (where relevant), in addition to the above:

- Under the category Background Check Data, Garda will collect credit check data on you, if required under the Monetary Authority of Singapore regulations/guidelines, for the purpose and activity of "Background Checks".
- Under the category Physical Security Data, Garda will collect closed circuit television (CCTV) recordings for the purpose and/or activity of "Fraud and Crime Prevention".

Garda has appointed a Singapore Data Protection Officer to address all queries and feedback on Garda's data protection obligations. The Data Protection Officer may be contacted by email: Dpo.sgp@gardacp.com during office hours in Singapore, using "Privacy Policy" in the email subject line.

Contact Information

If you have any questions regarding this Notice or wish to exercise any rights regarding your Personal Data held by Garda, please contact:

Garda Capital Partners LP
Attn: General Counsel
305 Lake Street East
Wayzata, MN 55391
Telephone: +1-612-330-4900 or +1-800-917-3579
Email: privacy@gardacp.com

Garda would appreciate the chance to deal with your concerns before you approach the relevant supervisory authority, but you may also contact the data protection authority applicable to you.

Reviewed: June 2025

Privacy Notice for California Job Applicants

Effective date: June 2025

This notice supplements the above Notice. Under the California Consumer Privacy Act, as amended by the California Privacy Rights Act (together, the "**CCPA**"), this privacy notice ("**CCPA Notice**") explains our practices regarding the collection, use, and disclosure of "personal information" of job applicants who reside in California.

Information We Collect and Disclose

As defined by the CCPA, "personal information" includes any information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information does not include de-identified or aggregated consumer information, certain regulated information, or information made available to the general public.

In the past 12 months, Garda has collected the following categories of personal information from job applicants and disclosed such information to the following categories of third parties for the business or commercial purposes described below.

Categories of PI Collected	**Examples**	**Categories of Third Parties to whom Disclosed**
Identifiers	Real name, alias, postal or mailing address, email address, telephone number, IP address, job applicant portal username, Social Security number, driver's license, state identification card number, or passport.	• IT service providers, such as our email providers, business application providers, and IT managed service providers • Vendors that perform background checks and other Human Resources services • Professional advisors (e.g., lawyers) • Former employers and references of our job applicants
Personal information types listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e))	A name, signature, Social Security number, address, telephone number, driver's license or state identification card number, education, or employment information.	• IT service providers, such as our email providers, business application providers, and IT managed service providers

	Some personal information included in this category may overlap with other categories.	• Vendors that perform background checks and other Human Resources services • Professional advisors (e.g., lawyers) • Former employers and references of our job applicants
Personal Characteristics or traits	In some circumstances, we may collect personal information that is considered protected under U.S. law, such as disability status.	• IT service providers, such as our email providers, business application providers, and IT managed service providers • Professional advisors (e.g., lawyers)
Geolocation Data	If you use some of the systems we use, we may gain access to the approximate location of the device or equipment you are using, or the location from which you are accessing our systems.	• IT service providers, such as our email providers, business application providers, and IT managed service providers
Internet or other similar network activity	IP addresses	• Website hosting provider • Service providers performing necessary business functions
Sensory and video data	Voicemail, video or similar information	• IT service providers, such as our email providers, business application providers, and IT managed service providers
Professional or employment-related information	Information regarding prior job experience, positions held, names of prior supervisors	• IT service providers, such as our email providers, business application providers, and IT managed service providers

		• Vendors that perform background checks and other Human Resources services
Pre-hire information	Job application, resume, background check data (where applicable and legally permissible, which will include civil and criminal offenses, employment, education, and certification and licensure verification where applicable performed prior to employment), job interview notes, candidate evaluation records, and relocation data preferences of you and your family members.	• IT service providers, such as our email providers, business application providers, and IT managed service providers • Vendors that perform background checks and other Human Resources services
Consumer-Provided Education Information	Information from resumes regarding educational history; transcripts or records of degrees and vocational certifications obtained; grades or class results, disciplinary records, or other education records or information	• IT service providers, such as our email providers, business application providers, and IT managed service providers • Vendors that perform background checks and other Human Resources services

Please note that we may also use, disclose, or transfer your information concerning the sale, merger, dissolution, restructuring, divestiture, or acquisition of our firm or its assets. We may also disclose your personal information in response to a court order, subpoena, search warrant, law, or regulation.

How We Collect Your Information

Garda collects the above-identified categories of personal information from the following sources:

- **Direct collection:** We collect information directly from you when you choose to provide it by filling out applications, participating in an interview or other components of the applicant process, or otherwise directly providing the information to us.

- **Third Parties:** We collect information about you from third parties who support our Human Resources and job application process, including recruitment agencies, background check vendors, and other hiring technologies.

- **Indirect and technology-based collection:** We also indirectly collect certain information from you when you access our websites or job applicant portals.

Sensitive Personal Information

Garda does not collect "sensitive personal information" (as defined by the CCPA) to infer characteristics about California consumers. Accordingly, Garda treats any such information as "personal information" consistent with applicable provisions of the CCPA.

Sale or Sharing of Personal Information

In the past 12 months, Garda has not "sold" any categories of personal information or "shared" any such information for the purposes of cross-context behavioral advertising. Likewise, Garda does not have actual knowledge of any sales or sharing of personal information regarding minors under 16 years of age.

Your Rights Under the CCPA

The CCPA provides California residents with the rights discussed below. For convenience and as required by the CCPA, we explain how you can exercise those rights to the extent they are applicable.

1. **Right to Request Information.** You have the right to request that we disclose certain information about our collection and use of your personal information during the past twelve (12) months. Specifically, you may request that we disclose:

    - The categories of personal information we collected about you;
    - The categories of sources for the personal information we collected about you;
    - The business and commercial purposes for collecting your personal information;
    - The categories of third parties to whom we disclose your personal information;
    - The specific pieces of personal information we collected about you; and
    - If we disclosed your personal information for a business purpose, the categories of personal information received by each category of third party.

2. **Right to Data Portability.** You have the right to request that we provide copies of the personal information we collected about you. If a verifiable consumer request is made, and subject to any exceptions or limitations under the CCPA, we will take steps to deliver the personal information to you either by mail or electronically. If we provide the information to you electronically, it will be in a portable and readily useable format to the extent technically feasible. Consistent with the CCPA and our interest in the security of your personal information, we will describe but may not provide copies of certain personal information we may receive from you (e.g., driver's license number) in response to a CCPA request, to the extent any of those items are in our possession.

3. **Right to Request Deletion.** You have the right to request that we delete the personal information we collected from you, subject to any exceptions or limitations under the CCPA.

4. **Right to Correct Inaccurate Information.** If we maintain inaccurate personal information about you, you have the right to request that we correct that incorrect personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information.

5. **Right to Opt-Out.** Consumers in California have the right to opt out of (a) the sale of personal information or (b) the sharing of their personal information for the purposes of cross-context behavioral advertising (as defined in the CCPA). These rights are unavailable because Garda does not "sell" or "share" personal information.

Exercising Your Rights

To exercise the rights described above, you—or someone authorized to act on your behalf—must submit a verifiable consumer request to us by sending an e-mail to privacy@gardacp.com or calling us at 1-800-917-3579. Your request must include your name, e-mail address, mailing address, phone number, and the specific requests you are making. If you are an agent submitting a request on behalf of a consumer, we may request that you submit a signed permission from the consumer authorizing you to make the request. To protect the privacy and data security of consumers, the verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative of such consumer; and
- Describe your request with sufficient detail, allowing us to understand, evaluate, and respond appropriately.

As indicated above, please be aware that the CCPA provides certain limitations and exceptions to the foregoing rights, which may result in us denying or limiting our response to your request.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request. We may also request that you provide additional information to verify your identity or authority to make the request. We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you or the consumer on whose behalf you are making the request.

Response Timing and Format

The CCPA requires us to respond to a verifiable consumer request within forty-five (45) days of its receipt; however, we may extend that period by an additional 45 days. If we require more time, we will inform you of the reason and extension period in writing. We will deliver our written response via e-mail. Any disclosures we provide will only cover the 12-month period preceding the receipt of the verifiable consumer request, provided that you may request disclosure beyond the 12-month period as permitted by the CCPA. Our response will also explain why we cannot comply with a request, if applicable. For data portability requests, we will select the format of our response; the format will be readily usable and allow you to transmit the information from one entity to another. We will not charge a fee to process or respond to a verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide a cost estimate before completing the request.

Our Commitment Not to Discriminate

We will not discriminate or retaliate against a job applicant for exercising their rights under the CCPA.

Contact Information

Questions regarding this privacy Notice, our use and disclosure of your information, or the employment process should be directed to:

Garda Capital Partners LP
Attn: General Counsel
305 Lake Street East

Wayzata, MN 55391
Telephone: +1-612-330-4900 or +1-800-917-3579
Email: privacy@gardacp.com

Changes

Garda may update or revise this Notice from time to time.