GARDA
CAPITAL PARTNERS

Privacy Notice

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 Data Protection Privacy Notice (the "**Notice**") is addressed to:

- website, social media users, and other individuals who contact Garda;
- service providers and vendors; and
- office visitors, event attendees, and speakers; all together the "**Data Subjects**".

If you are a job candidate applying for a job at Garda, we will process your details in accordance with our Global Data Protection Privacy Notice for Candidates, which is located here https://www.gardacp.com/candidate-privacy-notice/.

If you are an investor or employee of an investor using the Investor Portal, we will process your details in accordance with the Global Privacy Notice for Investors, which will have been provided to you. If you would like an additional copy, please reach out using the contact information located in this notice.

If you are a California resident, please see the Privacy Notice for California Residents section below, which supplements this Notice.

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. This Notice also includes additional information required under California law about our collection, use, and disclosure of the personal information of California residents, along with other required information such as rights that may be available to California residents.

Depending on your location, your Personal Data may be subject to: (i) EU General Data Protection Regulation, 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 and the United States, but in each case, only to the extent such laws are applicable to our processing of your Personal Data (collectively, "**Data Protection Laws**").

Information Collected

We may collect Personal Data when you interact with Garda. The information Garda holds and processes will be used to: (i) keep our systems and information safe; (ii) improve our website and social media experience; and (iii) for management, compliance, and administrative use. This includes using information to enable Garda to: (a) comply with any legal requirements; (b) pursue legitimate interests of Garda; and (c) protect Garda's legal position in the event of any proceedings.

For website, social media users and other individuals who contact Garda:

- "**Identity Data**": including first name, middle name, maiden name, last name, title, IP addresses (where relevant);
- "**Contact Data**": including contact information you provide to us (such as postal address, e-mail address, telephone and/or mobile phone numbers);
- "**Communication Data**": including any further data you enclose in your communications (such as email), the processing and the storage of your communications; and
- "**Social Media Information**": including your social media ID and content of postings on Garda's pages/accounts, including photos (where relevant).

For Service Providers and Vendors:

- "**Identity Data**", "**Contact Data**" and "**Communication Data**" listed above;
- "**Service Provider Data**": includes your services contract; correspondence with you or about you (for example, communication with you regarding your engagement); contract details; citizenship; copies of identification cards (such as passport); credit checks performed prior to or during your engagement, billing/financial information;
- "**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 if you are visiting the Singapore office, Garda will collect closed circuit television (CCTV) recordings for the purpose and/or activity of "workplace operations" and "fraud and crime prevention";
- "**Internal Documents and Records**": including documents and records that are produced in the course of carrying out your services for Garda (e.g., documentation pertaining to services performed and correspondence); and
- **"Virtual Meetings and Audioconferencing Data"**: including name; screen name; email address; date; location; IP address; device information and audio, video, and chat during the call (if recorded).

For Office Visitors, event attendees and event speakers:

- "**Identity Data**", "**Contact Data**", "**Communication Data**", "**Physical Security Data**", "**Social Media Information**" and "**Virtual Meeting and Audioconferencing Data"** listed above;
- "**Health-related information**" such as dietary preferences/food allergies, etc.
- "**Travel or expense information**", such as flight details, hotel reservations, itineraries, expense requests, etc.

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.

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

- "**Contractual Necessity**": to establish, execute, and fulfill the obligations of an agreement;
- "**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).

Garda does not knowingly collect or maintain Personal Data from anyone known to be under the age of 18. If Garda is made aware that it has collected Personal Data from a child that is not provided by a parent or guardian in the course of its services or in a manner that is inconsistent with applicable laws, Garda will delete this information as soon as possible.

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	Data Subject	Type of Data	Legal basis for processing
Operating Website and social media	Website and social media users	Identity Data	• Legitimate Interests: to ensure the proper functioning, optimization, security of Garda's website and social media channels, including fraud prevention, as well as providing information on Garda.
Administration (to contact you or respond to your requests or enquires and maintain our internal records)	All Data Subjects	Identity Data, Contact Data, Communication Data and Virtual Meeting and Audioconferencing Data	• Legitimate Interests: to develop and improve our technology platforms and keep our systems safe; to contact you or respond to your requests or inquires; and maintain our internal records.
Legal and Regulatory Compliance and dealing with legal disputes (including all uses and disclosures of Personal Data	All Data Subjects	It is possible it could involve all Personal Data categories above.	• Legitimate Interests: to ensure compliance with all legal and regulatory requirements, as well as

that are required by law or reasonably needed for compliance with company policies and procedures)			supporting legal claims and defense of rights. • Legal or Regulatory Obligation.
Facilitating any proposed or confirmed merger, acquisition or business asset transaction	All Data Subjects	It is possible it could involve all Personal Data categories above.	• Legitimate Interests: to ensure the ability by Garda to change ownership and fulfil its legal obligations.
Hiring, Managing and Terminating Service Providers (evaluating suitability, to make payments, maintaining a business relationship)	Service Providers and Vendors	Identity Data, Contact Data, Communication Data, Service Provider Data, Physical Security Data, Internal Documents and Records, Virtual Meetings and Audioconferencing Data.	• Legal and Regulatory Obligations. • Legitimate Interests of hiring and retaining appropriate service providers. • Contractual Necessity.
Fraud and Crime Prevention: preventing fraud and maintaining security.	All Data Subjects	It is possible it could involve all Personal Data categories above.	• Legal and Regulatory Obligations. • Legitimate Interests of preventing fraud and maintaining security. • Contractual Necessity.
Workplace Operations (facility access, scheduling, and data back-up copies.)	All Data Subjects	It is possible it could involve all Personal Data categories above.	• Legitimate Interests: of security, fraud prevention, compliance with laws and regulations, and the smooth running of the business.
Facilitating Events (including organizing an event and to communicate or publish your involvement with an event (for hosts and speakers)	Event attendees and event speakers	Identity Data, Contact Data, Communication Data, Social Media Information, Physical Security Data, Health-related information, Travel and expense information, and Virtual Meetings and Audioconferencing Data	• Legitimate Interests of maintaining the security and smooth running of events. • Additional basis of processing for health-related information: for reasons of substantial public interest (to ensure health and safety within our premises and, where relevant, to protect your vital interests).

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.

The purposes listed in the above table may continue to apply even in situations where your relationship with us (for example, pursuant to a contract) has been terminated or altered in any way, for a reasonable period thereafter (including, where applicable, a period to enable us to enforce our rights under any contract with you).

If you fail to provide Personal Data

If you fail to provide Personal Data when requested, Garda will be unable in some circumstances to comply with its obligations. Garda will inform you about the implications of your decision not to provide the requested data.

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. When you visit our offices, we may ask you to provide limited information relating to your health, such as details of allergies or dietary requirements. This helps us to ensure your comfort and safety while on our premises. Providing this information is voluntary, but it may be necessary for us to make suitable arrangements for your visit.

We process this information to comply with our legal obligations relating to workplace health and safety. The additional legal basis under Article 9 of the GDPR is that processing is necessary for reasons of substantial public interest, specifically to ensure health and safety within our premises and, where relevant, to protect your vital interests.

Personal data, including sensitive personal data is not sold to or shared with third parties. Additionally, Garda does not use or disclose sensitive personal data for the purpose of inferring characteristics about Data Subjects.

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 Data may be shared with:

- Compliance providers, personal safety and business continuity providers, and HR databases;
- Third-party software providers, IT providers, cloud storage companies, and cyber and email protection companies;
- Third-party work messaging and scheduling systems, work information sharing platforms, and task management systems;
- Event management organisers and travel specialists; and
- 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 Data 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 Data 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.

Cookies and Related Technologies

What are cookies?
A "cookie" is a small amount of information that a web server sends to your browser that stores information about your use of a website. Some cookies are temporary, whereas others may be configured to last longer.

First and third-party cookies
Whether a cookie is 'first' or 'third' party refers to the website or domain placing the cookie. First-party cookies in basic terms are cookies set by a website visited by the user, the website displayed in the URL window. Third-party cookies are cookies that are set by a domain other than the one being visited by the user. If a user visits a website and a separate company sets a cookie through that website this would be a third-party cookie.

We do not use cookies that track activity
Garda does not use first- or third-party cookies. Garda collects your IP address for a short period of time for cybersecurity purposes.

The website links to third-party websites. These sites may use cookies, and Garda has no control over the cookies placed on your browser when using these services. Please review each third party's cookie policy located on their website.

Privacy Policies of Third-Party Websites

This Notice only addresses the use and disclosure of Personal Data we collect from you. Other third-party websites that may be accessible or linked through our website have their own privacy policies and data collection, use, and disclosure practices. If you access any such website, we urge you to review its privacy policy. We are not responsible for the policies or practices of third parties, including those of any sites or services not owned by us.

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.

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 has appointed a Singapore Data Protection Officer to address all queries and feedback on Garda's data protection obligations as they pertain to the Garda Singapore office. 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.

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.

Changes to this Notice

We may update this Notice from time to time. Any changes will be posted to this page with an updated revision date. We encourage you to review it periodically.

Reviewed November 2025

Privacy Notice for California Residents

Effective date: November 21, 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 the Data Subjects, listed in the above Notice, who are California residents.

This CCPA Notice does not apply to personal information collected from California resident job candidates, which is subject to the Global Privacy Notice for Candidates, located here https://www.gardacp.com/candidate-privacy-notice/.

If you are a California resident employee of an investor using the Investor Portal, we will process your details in accordance with the Global Privacy Notice for Investors, which has been provided to you. If you would like an additional copy, please reach out using the contact information located in this CCPA Notice.

Information We Collect and Disclose

As defined by the CCPA, "personal information" includes any information that identifies, relates to, describes, 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.

Depending on how you interacted with us, we may have collected the following categories of personal information from you in the last 12 months, which we may also share with third parties for the purposes outlined in this CCPA Notice. Please note that we do not collect every type of personal information identified below from every consumer. The types of personal information we have collected depends on how you interacted with us.

Categories of PI Collected	Examples	Categories of Third Parties to whom Disclosed
Identifiers	Name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name	IT service providers, such as our email provider, business application providers, and managed service providers
Personal information types listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e))	Name, signature, address, and telephone number. Some personal information included in this category may overlap with other categories.	IT service providers, such as our email provider, business application providers, and managed service providers
Protected classification characteristics under California or federal law	None	N/A
Commercial information	None	N/A
Biometric information	None	N/A
Internet or other similar network activity	IP addresses, social media activity and engagement, transcripts of video conferences	IT service providers, such as our email provider, business application

		providers, and managed service providers
Geolocation data	None	N/A
Sensory data (audio, electronic, thermal, olfactory or similar information)	Voicemail or similar audio recordings	IT service providers, such as our email provider, business application providers, and managed service providers
Professional or employment information	None	N/A
Non-public education information as defined under the Family Educational Rights and Privacy Act	None	N/A
Inferences drawn from other personal information	None	N/A
Sensitive Personal Information	None	N/A

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, regulation, or to ensure compliance with legal and regulatory requirements, as well as to support legal claims.

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.

Use and Disclosure of Personal Information

We may use or disclose the personal information described above for the following business purposes:

- Preventing and detecting fraud, hacking activities, security breaches, and other unlawful activities in connection with our website, LinkedIn page, or use of our services;
- Informing individuals about Garda through our LinkedIn page;
- Communicating with you and responding to your requests, including providing you with information you request from us, and maintaining our internal records;
- Managing our business relationships, including carrying out our obligations and enforcing our rights arising from any agreements;
- Hiring, managing, and terminating service providers;
- Workplace operations, including facility access and scheduling;
- Facilitating events, including organizing the event and publishing or communicating involvement with the event;
- Protecting the safety, security, and integrity of Garda, our rights or property (including website and other technology assets), to protect someone's health, safety, or welfare;
- Complying with a law or regulation, court order, our ethical obligations, or other legal process; and

- Performing other functions as otherwise described to you at the time of collection.

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 directly to us by communicating with us, visiting our offices, attending an event, webinar, or presentation, or otherwise directly providing the information to us.
- **Indirect collection:** We also indirectly collect certain information from you when you visit our website, such as IP addresses for cybersecurity purposes.
- **Collection via LinkedIn:** We may also collect personal information through LinkedIn if you interact with Garda's LinkedIn page.

Data Retention

Garda retains personal information 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 information 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 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 Know.** You have the right to request that we disclose certain information about our collection and use of your personal information. Specifically, you may request that we disclose:

    - The personal information we collected on you, including the categories of personal information;
    - The categories of sources for the personal information we collected about you;
    - The business or commercial purposes for collecting or sharing your personal information;
    - The categories of third parties to whom we disclosed or shared your personal information; and
    - The categories of personal information that we disclosed or shared for business purposes about you.

2. **Right to Delete.** 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.

3. **Right to Correct.** 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.

4. **Right to Opt-Out of Sale and Sharing.** 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.

5. **Right to Limit Use and Disclosure of Sensitive Personal Information.** You have the right to limit our use and disclosure of your sensitive personal information to purposes necessary to perform services or provide goods reasonably expected by you. This right is currently unavailable because Garda does not collect sensitive personal information.

6. **Right to Opt-Out of Automated Decision-Making Technology (ADMT) and Right to Access ADMT.** You have the right to opt out of the use of ADMT that produces legal or similarly significant effects and to access information about such technology. However, both rights are currently unavailable because Garda does not currently use ADMT for decisions that produce legal or similarly significant effects concerning you.

7. **Right of No Retaliation or Discrimination following Exercise of CCPA rights.** We will not discriminate or retaliate against you for exercising your rights under the CCPA.

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. 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 confirm receipt of the request and provide information about how we will process the request within 10 business days. It also requires us to respond to a verifiable consumer request within 45 calendar days of its receipt; however, we may extend that period by an additional 45 calendar days. If we require more time, we will inform you of the reason and extension period in writing. Our response will also explain why we cannot comply with a request, if applicable. When you request specific pieces of personal information we have collected about you, we will provide this information in a readily usable format that allows you to transmit the information from one entity to another. 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 in response to a CCPA request, to the extent any of those items are in our possession.

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.

Contact Information

Questions regarding this CCPA Notice, our use and disclosure of your information, 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

If we make material changes to this CCPA Notice, we will post an updated version on our website and indicate the date of the most recent revision.