

**California Consumer Privacy Rights Act Policy and Notice of Collection of Personal Information  
For California Employees, Applicants, and Individual Service Providers**

Cantor Fitzgerald, L.P., BGC Partners, Inc., and Newmark and their affiliated entities, subsidiaries, and strategic partners’ (collectively referred to herein as the “Company”) are committed to the proper handling of the personal information collected or processed in connection with your application for employment, employment relationship and/or engagement with the Company. This disclosure describes categories of personal information that the Company collects and the purposes for which the Company processes and uses that information, in accordance with the California Consumer Privacy Rights Act (the “CPRA”) in connection with the foregoing. For purposes of this privacy notice and policy (“Privacy Notice”), the term “personal information” shall have the meaning ascribed by the following definition given in the CPRA: “personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with you or your household. Personal information does not include publicly available information, information that is de-identified or aggregated information, or other information that is outside the scope of the CPRA. The Privacy Notice applies only to individuals residing in the State of California who are considered “Consumers” under the CPRA and from whom we collect “Personal Information” as described in the CPRA.

The categories of, and the purposes for use of, personal information described below reflect data collected across the Company. This table also sets out personal information we have collected over the last twelve (12) months:

	<b>Categories of Personal Information Collected</b>	<b>Retention Period<sup>1</sup></b>
Category A.	Identifiers, such as name, contact information, date of birth, online identifiers, Social Security numbers, and other ID numbers and licenses issued by the government or self-regulatory organizations (such as FINRA);	6 years; deleted per Policy
Category B.	Personal information, as defined in the California customer records law, such as name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account information, credit card number, debit card number, and other financial, medical, and health insurance information. Some personal information in this category may overlap with other categories;	6 years; deleted per Policy
Category C.	Characteristics of protected classifications under California or federal law;	6 years; deleted per Policy
Category D.	Commercial information, such as transaction information, purchase and reimbursement history, and financial details;	6 years; deleted per Policy
Category E.	Biometric information, such as fingerprints;	6 years; deleted per Policy
Category F.	Internet or network activity information, such as browsing history, search history, intranet activity, email communications, stored documents and emails, usernames and passwords, and other interactions with websites, applications or systems;	Retained and deleted subject to Policy

<sup>1</sup> Personal information is retained pursuant to the Company’s Records Retention Policy (the “Policy”). A copy of the Policy is available upon request via the contact information below.

Category G.	Audio, electronic, visual, and similar information, such as images and audio, voicemails, chat logs, text messages, video or call recordings created in connection with the Company's business activities;	Retained and deleted subject to Policy
Category H.	Professional or employment-related information, such as data submitted with employment applications, compensation, background check and criminal history (to the extent covered under the CPRA), work history and prior employers, work authorization, professional licenses, fitness for duty data and reports (upon return from a medical leave of absence), performance and disciplinary records, leave of absence information including religious and family obligations and physical and mental health data concerning employee and their family members, human resources data, and data necessary for benefits and related administrative services;	6 years; deleted per Policy
Category I.	Education information subject to the federal Family Educational Rights and Privacy Act, such as student records; and	6 years; deleted per Policy
Category J.	Inferences drawn from any of the personal information listed above to create a profile or summary about, for example, an individual's preferences, abilities, aptitudes and characteristics. We may accumulate your personal information to make decisions concerning your employment related qualifications consistent with applicable law.	6 years; deleted per Policy

Personal information is collected for the following purposes:

1. To comply with federal, state, and local law and regulations, the rules and regulations of self-regulatory organizations (such as FINRA), and contractual obligations;
2. To comply with and implement Company policies;
3. To process payroll and other payments, withholdings, deductions, and reimbursements;
4. To respond to employees' inquiries and claims and to otherwise communicate with employees and/or their emergency contacts and plan beneficiaries;
5. To track time and attendance;
6. Maintaining personnel records and complying with record retention requirements;
7. To administer and manage workers' compensation and short/long-term disability claims;
8. To administer and manage requests for leave;
9. To administer and maintain benefits, including group health insurance;
10. To administer and maintain the 401(k) plan;
11. To manage employee performance, including promotions, discipline, and/or termination;
12. Ensuring employee productivity and adherence to the Company's policies;
13. To conduct workplace investigations;
14. To accept job applications, evaluate job applicants and candidates for employment, and manage the Company's recruiting and hiring practices;
15. To obtain and verify background checks;
16. To grant and monitor employees' access to company facilities and systems;
17. To implement, monitor, and manage electronic security measures on devices that are used to access Company networks and systems (e.g., information security);
18. Preventing unauthorized access to or use of the Company's property, including the Company's information systems, electronic devices, network, and data;
19. Facilitate the efficient and secure use of the Company's information systems;
20. Ensure compliance with Firm information systems policies and procedures;

21. To review employee records in connection with potential corporate transactions, such as for evaluating potential mergers and acquisitions;
22. To maintain commercial insurance policies and coverages;
23. To anonymize and/or aggregate data to perform workforce analytics, data analytics, and benchmarking;
24. Business management;
25. Recruiting;
26. Design, implement, and promote the Company's diversity and inclusion programs;
27. To improve efficiency and productivity;
28. To prosecute or defend legal claims, and respond to court orders, subpoenas or governmental information requests; and
29. To perform call and chat monitoring and surveillance.

The Company collects personal information from the following categories of sources:

1. Directly from employees and applicants,
2. Service providers and contractors (including independent contractors and consultants) providing services on our behalf. We require our service providers and contractors who we provide your personal information to in order to provide services to maintain the privacy and security of your personal information;
3. Government agencies or self-regulatory organizations (e.g., FINRA);
4. The Company's internet and intranet networks and internal communications systems (e.g., the Company's telephonic systems, electronic mail and messaging platforms); and
5. Third-parties as necessary (e.g., recruiters, and state or federal governmental agencies, among other third-parties);

The Company does not: (i) share personal information with third parties for cross-contextual behavioral advertising purposes; or (ii) sell personal information to third parties. We have not shared with or sold any categories of your personal information (A-J) to third parties in the last twelve (12) months.

In the previous twelve (12) months, the Company has, or may, disclose the information collected in Categories A-J above to outside organizations or entities who are not service provider or contractors providing services on our behalf including to: state or federal governmental agencies or entities, self-regulatory organizations, among other third-parties, including but not limited to where required by law.

We do not collect sensitive personal information for the purposes of inferring characteristics.

### **NOTICE OF RIGHTS UNDER THE CPRA**

Under the CPRA, you have the following rights in the personal information held by the Company:

- You have the right to request that the Company disclose the personal information that the Company collects, uses and discloses about you. You may "request to know": (i) the categories of personal information that the Company has collected about you; (ii) the categories of sources from which the personal information is collected; (iii) the business or commercial purpose for collecting, selling or sharing your personal information; (iv) whether any categories of personal information were disclosed for a business purpose to third parties and the categories of third parties with whom the Company discloses your personal information; and (v) the specific pieces of personal information that the Company has collected about you. Your request may pertain to the personal information collected about you on or after January 1, 2022. If your request covers a time period beyond 12 months from the date of your request, the Company may deny your request as to that time period

where it would be impossible for the Company to provide you with the information or involve disproportionate effort. The Company may deny your request to search for certain information under certain circumstances (e.g., where the Company retains the information solely for legal and compliance purposes).

- You have the right under certain circumstances to receive specific pieces of your personal information in a format that is understandable, and to the extent technically feasible, in a structured, commonly used, machine readable format that allows you to transmit the information to another entity.
- You have the right to correct inaccurate personal information.
- You have the right to request deletion of personal information under certain circumstances. For example, the Company may not be required to delete personal information if the Company needs to retain the information to comply with a legal obligation or where the information is stored on an archived or backup system.
- You have the right to know what information is sold or shared to third parties, and to whom and to opt out of sale or sharing.
- You have the right not to receive discriminatory and non-retaliatory treatment for the exercise of any of these rights. The Company will not discriminate or retaliate against you because you have exercised your rights.

You may submit requests concerning any of your rights by contacting the Company by e-mail to [CCPA@cantor.com](mailto:CCPA@cantor.com), [CCPA@nmrk.com](mailto:CCPA@nmrk.com), or [CCPA@bgcpartners.com](mailto:CCPA@bgcpartners.com), or by telephoning the Company at 1-833-705-0543. The Company will use reasonable methods for verifying that the person making a request to know, data portability, request to correct or a request to delete is the individual about whom the Company has collected personal information.

This may involve, depending on the nature of the request, confirming that the email address provided corresponds with the Company's records concerning the individual. Additional reasonable measures may also be required to verify the identity of the person making the request depending on the circumstances. For requests to delete made electronically, you will be required to submit the request to delete, and then separately confirm that you want your personal information deleted. To the extent that you wish to use an authorized agent to make requests concerning the rights set forth above, you will need to provide the Company either with a power of attorney or, alternatively, with signed authorization to communicate with your authorized agent, and directly confirm that you provided the authorized agent with permission to submit the request.

The Company will (i) confirm receipt of requests to know, data portability, to correct inaccurate information or to delete within 10 business days of receiving the request and provide information concerning how the Company will process the request; and (ii) generally respond to requests to know, data portability or to delete within 45 calendar days of receiving the request. If the Company needs additional time to respond to your request beyond the 45 calendar days, the Company will provide you with notice explaining the reasons the Company needs more time, and will then take up to an additional 45 calendar days to respond to your request.

### **Changes to this Privacy Notice**

The Company may modify this Privacy Notice at any time in order to address the Company's business needs or changes in applicable laws and regulations.

### **Alternative Access to this Privacy Notice**

Persons with disabilities may contact the Company to receive this privacy notice in an alternative format by emailing the Company at by e-mail to [CCPA@cantor.com](mailto:CCPA@cantor.com), [CCPA@nmrk.com](mailto:CCPA@nmrk.com), or [CCPA@bgcpartners.com](mailto:CCPA@bgcpartners.com) or contacting the Human Resources Team.

### **Additional Questions**

Should you have questions about the collection and processing of your personal information or about the security of your personal information, please contact the the Company by e-mail to [CCPA@cantor.com](mailto:CCPA@cantor.com), [CCPA@nmrk.com](mailto:CCPA@nmrk.com), or [CCPA@bgcpartners.com](mailto:CCPA@bgcpartners.com) or contacting the Human Resources Team.

**Last updated:** December 2022