Last update: April 2025

NORTH AMERICA EMPLOYEE PRIVACY STATEMENT (US / Canada)

This Employee Privacy Statement (this "**Privacy Statement**") explains when and what personally identifiable information relating to you as individual ("**Personal Data**") we collect, use, disclose, store, and in general process about you in the context of your employment relationship with Gen II, what we use your Personal Data for, and who we may share it with, as well as your rights in relation to your Personal Data, and whom you can contact for more information or in case you have any queries.

If you are a candidate seeking employment at Gen II, please instead refer to our Candidate Privacy Statement here.

"**Gen II**" or the "**Employer**," or "**we**" refer to the Gen II entity that has a contractual relationship with you (for example, a contract of employment, a traineeship agreement, or a consultancy agreement), which shall be in charge of processing your Personal Data in the context of this Privacy Statement:

- Gen II Fund Services, LLC1675 Broadway, New York, NY 10019
- Gen II Compliance Services, LLC, 1675 Broadway, New York, NY 10019
- Sensr Solutions, LLC 1675 Broadway, New York, NY 10019
- Gen II Management, LLC, 1675 Broadway, New York, NY 10019
- Gen II Tax Services, LLC1675 Broadway, New York, NY 10019
- Gen II Fund Services (California), LLC, 505 Sansome Street, Ste 875, San Francisco, CA 94111
- Gen II Fund Services (Connecticut), LLC, 201 Broad Street, Stamford, CT 06901
- Gen ll Fund Services (Texas), LLC, 4131 N. Central Expressway, Suite 800, Dallas, TX 75204
- Gen ll Fund Services (Colorado), LLC, 6900 E Layton Avenue, Denver, CO 80237
- Gen II Fund Services (Florida), LLC, 120 East Palmetto Park Road, #510, Boca Raton, FL 33432
- Gen II Fund Services (New Jersey), LLC, 60 Columbia Road, Building B, Suite 200, Morristown, NJ 07960
- Sensr Solutions (Canada), Inc., Suite 2500, Park Place, 666 Burrard Street, Vancouver, BC V6C2X8, Canada

Any Personal Data provided to or collected by the Employer will be processed (meaning collected, used, stored, disclosed, transmitted, etc.) in accordance with this Privacy Statement by (i) the Employer, or (ii) by the Employer's subcontractors and service providers as further described in this Privacy Statement, or (iii) by the Employer's clients or third-party recipients.

The Employer has taken reasonable safeguards to ensure the confidentiality and security of your Personal Data. Reasonable and appropriate technical, physical, and organizational measures have been implemented to protect Personal Data against accidental or unlawful destruction or loss, damage, alteration, unauthorized disclosure, or access, and against all other forms of unlawful processing. No automated decisions are or will be made by the Employer as a result of your Personal Data being processed.

Any reference to:

- "**employees**" or "**employment relationship**" in this Privacy Statement shall be read in a larger sense to include employees, secondees, interns or trainees, as well as external consultants and any other permanent or temporary staff;
- "**you**" or "**yours**" refers to the individual natural living person working for Gen II and to whom this Privacy Statement applies.

We invite you to carefully read the Privacy Statement below so that you can also understand your rights with respect to the privacy of your Personal Data during the course of your employment relationship. **For more detailed information on your employment relationship with Gen II and all related Personal Data processing activities, please also read carefully your local Employee Handbook.**

If you have any questions or requests pertaining to the processing of your Personal Data, please contact: privacy@gen2fund.com.

Contents

1. What Personal Data could we collect and process?

We may collect Personal Data **directly** from you during the recruitment and onboarding process, via forms that you are requested to fill in and documents that you are requested to provide. We also collect your Personal Data during the course of your employment relationship, from correspondence with you or through meetings and assessments, or as required upon termination of your employment relationship.

We may also collect Personal Data about you **indirectly**, through public sources or legally accessible databases, used by our HR and Compliance Department to perform their background check activities, via your manager in the context of your performance reviews or general feedback, or because you are using IT tools and applications made available by Gen II to its employees, or you are present in the Gen II premises where CCTV and badge readers are installed. In some cases, Gen II may collect Personal Data about you from third parties, such as references supplied by former employers, information from employment background check providers or information from credit reference agencies.
We primarily collect **your** Personal Data; however, due to our legal and regulatory obligations, as well as internal policies and procedures, we may also collect Personal Data of **your relatives and next of kin**, spouse or equivalent, or children. See more information below.

We are committed to protecting the privacy of all your Personal Data in an open and transparent manner.

The categories of Personal Data we process include:

Identification information, such as your name, surname, middle name, nickname, date of birth, gender, your ID, passport, copy of your identity card, passport, or your tax identification number and any other documentation required by law or necessary to fulfil employment duties;

Contact details, such as your personal and professional phone number, your personal and professional email address, your home address, your current and/or previous country of residence, your emergency contact details;

Photo, image or **likeness** and the **sound** of your voice;

Your **signature**, whether handwritten, photocopied, digital or electronic;

Your **professional, family and social background, relationships and military obligations, yours or of a family member:** such as your CV, employment and education details, job title, current and previous positions, references, professional memberships and qualifications, diplomas, hobbies, background checks, marital status, household composition, insurance affiliation, military leave or FMLA requests and information. “Military identification information” means information identifying a person as a member of the armed forces, or a veteran, as defined in said section, including, but not limited to, a selective service number, military identification number, discharge document, military identification card or military retiree identification card;

Financial and tax-related information such as your salary, bank account details, income, benefits, tax residency, professional credit card details, compensation, and potential bonus;

E-mail, internet, intranet, computer and mobile device(s) (including personal when such are used under the company’s Bring Your Own Device Policy) access and activity monitoring

details, such as your IP address, your browser type and language, access logs (including account name, access times, Wi-Fi and websites use, search history and monitoring thereof) or data in relation to communications including communications sent or received on any professional devices (such as frequency, volume, etc.), geolocation data from the professional device, and on personal devices when those are used for business purposes; communications we send you regarding our events and services, details of how you interact with the provided IT tools and applications, devices used and other similar information, intranet activity, stored documents and emails, usernames and passwords, app use, mobile browsing and search history and any information regarding the use of company-issued devices; if not exempt, **records of your actual time worked** through the time-tracking tools in use, storage of documents and emails;

Communication information, such as recordings of meetings and instant messaging conversations, SMS, voice mail, email communications, phone calls, phone logs, chat logs, text messages, social media postings;

Physical access or absence details to our premises, such as badge logs, security monitoring footage and video-surveillance logs (collected via our badge readers and video-surveillance systems in our premises);

Professional evaluations and career assessment details, including workplace conduct, records and references, employment history, such as results of personality questionnaires, performance assessments, feedback, references, disciplinary records, grievance, or capability reports and proceedings, benefit plans;

Travel details and expenses, such as travel itineraries, corporate credit card statements, frequent flyer, and other bonus programs;

Presence details, such as your holidays, absences, timesheets, teleworking time, and place;

Vehicle details, such as company car license plate number;

Information collected via non-obligatory surveys such as likes/ dislikes, preferences, food preferences or intolerances, clothes size, and preferences.

We may also collect and process sensitive Personal Data, in limited circumstances and to the extent legally permitted:

Social security number, driver's license, or state identification numbers with the following restrictions:
Gen II will always as per its policy (1) protect the confidentiality of Social Security Numbers, (2) prohibit unlawful disclosure of Social Security Numbers, and (3) limit access to Social Security Numbers. Gen II also imposes the following requirements on all employees who have access to Social Security Numbers:

- They do not ask any individual for their Social Security Number except to comply with lawful requirements of government agencies or as permitted by law;
- They do not use individual's Social Security Numbers as an ID number, password, account number, or other purpose;
- If they obtain an individual's Social Security Number, they do not disclose it to any third party, except as required or permitted by law, or store or transmit it in a manner which is not secure and confidential.

Geo-location data, including GPS location data from company-issued mobile devices and company-owned vehicles, or logs of mobile device location when such is used for multi-factor authentication purposes or to enter the company portal;

Medical information, such as your health certificates and sickness records, short-term or long-term disabilities, requests for paid sick or safe time (PSST): we strongly recommend you limit the information you are providing us with to the strict legal minimum;

Religious beliefs, provided by you whenever you may request, for example, accommodation to observe its practices.

Sexual preferences and sexual orientation, only to the extent this information has been provided by you, in the context of the Gender Anti-Discrimination Policy, including for example preferred gender pronouns, requests for accommodations, reports on sexual harassment or otherwise;

Background information provided by you, such as your criminal record extract, or collected from open data, legally available databases, or public records as part of our ongoing risk management processes to the extent legally permitted, salary history, employment history and recommendations, work authorizations, fitness for duty reports and data;

Information related to Gen II's Equal Employment Opportunity policy, including any information collected or shared by you around race or ethnic origins (inclusive of traits historically associated with race, including, but not limited to, hair texture and protective hairstyles), color, creed, religion, national origin, ancestry, alienage or citizenship status, sex, gender, pregnancy, childbirth, breastfeeding and medical conditions related to pregnancy, gender identity, gender expression, transgender status, sexual orientation, marital or civil partnership/union status, familial status, disability (mental and physical) including HIV and AIDS, protected medical condition (cancer and genetic- characteristics), genetic information including results of genetic testing and predisposition or carrier status, sexual and reproductive health decisions, age, military and/or veteran status, unemployment status, domestic or sexual violence or stalking victim status, caregiver status, or any other characteristic protected by applicable federal, state or local law.

Regarding **Personal Data of your relatives and next of kin**, please note that we may collect and process their identification information (such as name, surname, age, date of birth, gender), contact details (such as email address, home or professional address, country of residence), your relationship with them, copies of their national identity cards or passports (in case you request us to assist with obtaining residence permits), health certificates (when filing for child sickness leave), or photos (in case they are participating in an event organized by Gen II, in which case we will seek your consent, especially for minors).

When you provide Gen II with Personal Data about your relatives and next of kin, or any other individual who is not in direct relationship with Gen II, please ensure that you provide them with relevant information as to the processing of their Personal Data as provided for in this Privacy Statement.

We understand the importance of protecting children's privacy. It is not our policy to intentionally collect, use, disclose, store, or in general process Personal Data pertaining to minors, with the exception of their name, surname, social security number where needed and date of birth solely for the purpose of granting you leave in relation to your children such as sickness leave, maternity leave,

and parental leave. If we need to process Personal Data pertaining to minors in the context of events organized by the Employer, you shall be separately informed, as necessary.

2. For which purposes do we process your Personal Data and on which legitimacy grounds?

a) Processing necessary for the performance and execution of your employment agreement

We will process your Personal Data for the purpose of fulfilling our contractual obligations under the employment agreement. This includes:

- To administer the employment relationship;
- Maintaining personnel records and record retention requirements;
- To contact you for any business purpose, such as day-to-day communications, news and updates, internal and external training opportunities;
- To proceed to the payment of your salary and other appropriate monetary or non-monetary benefits and to make the relevant tax deductions, social security arrangements or specific programs;
- To make necessary arrangements for expense reimbursements;
- To ensure that you are safe and protected during working hours (including during business travel) and that you have an adequate work environment;
- To be able to reach out to your emergency contacts in case anything happens to you;
- To be able to inform you about emergency situations at work, especially when it is not possible, or you are not expected to have access to your work contact details;
- To ensure your professional development, including the organization of trainings and promotion of career opportunities;
- To maintain a high level of employer-employee relationship by regularly consulting you on different matters via employee surveys;
- To provide you with tools and applications aiming to facilitate your work but also interaction with your colleagues worldwide (such as the employee directory or onboarding introduction message);
- To make sure you are able to access our IT infrastructure and any applications (internal or external) on a need-to-know basis;
- To ensure proper performance of your contractual duties, which shall allow us to monitor your working hours, teleworking, your performance as well as gather evidence for possible grievance or disciplinary actions and obtain work related feedback from your colleagues;
- To manage flexible time work arrangements and holidays;
- To assess the continuation or termination of our employment relationship, including during or after the probation period; and
- To provide you (or your family) with any agreed benefit, including but not limited to insurance, company vehicle, pension scheme, health, and wellness benefits.

b) Processing necessary for compliance with legal obligations

We will process your Personal Data to comply with applicable national or federal laws and regulations. This includes:

- Our obligations related to anti-money laundering laws, fight against corruption, health and security at work, whistleblowing, work ethics, risk management which may also result in monitoring at the place of work;
- Our legal duties as an employer, including processing for social security, tax or accounting purposes, election of a staff delegation, maintenance of adequate reporting. Pursuant to applicable laws and regulations, the Employer may also need to disclose your Personal Data to government bodies or judicial authorities, as well as to tax administrations, social security, supervisory or other competent authorities;

- Our professional duties as a regulated company of the financial sector and any obligations deriving from the circulars or guidance issued by the supervisory authorities. Our legal obligation to ensure security and safety of our assets and employees; and
- Our privacy and data protection obligations to ensure response to the exercise of privacy rights and to Personal Data breaches and incidents.

Your sensitive Personal Data will be used for the following limited purposes:
- To ascertain your fitness to work (medical checks required under your local labor law);
- To record and manage sickness absences as required under your local labor laws or to justify a change in your current job position;
- To comply with our health and safety obligations;
- To ensure the honorability of our employees and prevent fraud;
- To provide you accommodation for religious practices or for lactation;
- To prevent unauthorized access to use or disclose/remove Gen II's property, including information systems, electronic devices, network, and data;

c) Processing necessary to protect your vital interests
We may exceptionally and only in very limited circumstances process your Personal Data if necessary to protect your vital interests in cases where you would no longer be physically capable of giving your consent (e.g. in case of medical emergency).

d) Processing necessary for purposes that are in the Employer's legitimate interest
We will process your Personal Data in order to pursue our legitimate interest both for our own internal purposes as well as for business purposes. This includes the following:
- To ensure reliable service provision to our customers or by our suppliers. This includes, without limitation, providing customers, suppliers, and other providers with your contact information, professional qualifications, and experiences, as required in the ordinary course of business;
- To showcase our heads of departments and specialists on our website and social media in order to demonstrate their talents and capabilities to current and prospective clients and general audience;
- To ensure proper personnel management, for example, payroll administration, compensation benefits, leaves and other absences administration, provision of benefits, management of work spaces;
- To manage recruitment, either directly (including via publicly availably platforms) or indirectly via referrals, or via recruitment agencies, and onboarding of new employees;
- To perform performance reviews and manage promotions or feedback, disciplinary, grievance or capability reports and proceedings;
- To organize business travels and administer related expenses;
- To offer you trainings, education, coaching or other forms of career guidance, personal development, talent management;
- To organize and extend invitations to company events, team building activities, corporate social responsibility initiatives as well as social & sports committee initiatives;
- To exercise or defend legal claims or for obtaining legal advice;
- To perform business processes and internal management, including general management, work scheduling, worked time recording, implementation of business control, checking compliance with internal procedures and policies, archiving, insurance purposes, in the context of dispute resolution;
- For verification purposes with banks and/or financial institutions, public administrations and/or independent authorities, attorneys, auditors in case you have signatory authority;
- In the context of mergers, acquisitions, and divestments if necessary, in order to manage such transactions;

- To protect our offices, IT infrastructure (including monitoring your access and use of emails, instant messages, internet, laptops, workstations, hard disks and shared folders on the servers) and to ensure the security of our network and information, in compliance with applicable data protection laws and regulations. This may lead to monitoring with the aim to log activity or scan correspondence of any kind or documents transiting through your professional devices in accordance with internal policies and procedures to identify risks and take adequate mitigation measures in accordance with applicable law. The monitoring will be performed gradually. The Employer performs statistical controls on the basis of traffic and log data. It is only in case these controls reveal abuse, misuse, illegitimate or dangerous use of the IT infrastructure or when the Employer has valid reasons to believe that there may be an increased risk for data loss (such as when you may be leaving the company pursuant to termination or resignation) that the monitoring may be intensified and lead to your identification. The Employer will in principle not access your private correspondence. However, if the private nature is not clear or specifically indicated in the object (that is, when it has the appearance of a professional correspondence), the Employer may review it;
- To secure our premises and prevent unauthorized people from entering the building or people accessing unauthorized areas;
- To ensure the security and safety of our assets (building, facilities, equipment, merchandise, cash, etc.) and employees, clients, and visitors;
- To detect and identify potentially suspicious or dangerous behavior;
- To identify the origin of accidents or incidents;
- To organize and supervise a rapid evacuation of people from the premises in the event of an incident;
- To alert the emergency services, fire brigade or the police and facilitate their intervention in case of an incident and to request assistance in performing all of the above in case of an emergency by assigning the monitoring of suspicious activity to a third party;
- To protect its assets and for security purposes, the Employer may rely on video surveillance through which your image may be processed;
- To monitor your working hours and the attendance time of the employees, as well as to confirm your declared place of work in cases of teleworking;
- To ensure that there is a business continuity plan in place;
- To investigate and manage complaints and legal disputes involving you or other employees, including accidents at work or suspected violations of internal policies, or involving our clients;
- To improve our business and to collect feedback, conduct staff surveys and data analytics studies (among other things to review and better understand employee satisfaction and turnover);
- To develop our business and activities, including marketing activities, client satisfaction and related follow-up;
- To collaborate with our professional advisors, such as lawyers, accountants, consultants, auditors, and other service providers (such as but not limited to archiving, security, IT, or printing services).
- To monitor the usage of the tools and the applications, ensure and enhance employee productivity and adherence to the Employer's policies and procedures.

  Additional information on the above purposes may be contained in the internal policies and procedures made available to you on the intranet, such as the Employee Handbook, the Employee Code of Conduct, the AML-KYC procedure, etc., as may be updated and posted from time to time therein.

e) Processing based on your consent

Where you have given your consent for the processing of Personal Data, in applicable jurisdictions such consent will serve as a legal basis for such processing (for example, medical conditions that the Employer needs to be aware of). You have the right to withdraw your consent at any time as per applicable internal policies and procedures. The withdrawal of your consent shall not affect the lawfulness of processing based on consent before its withdrawal.

3. With whom do we share your Personal Data?

In connection with one or more of the purposes outlined here above, we may disclose your Personal Data to the following recipients to the extent necessary and on a strict need-to-know basis:

- The management of Gen II as well as affiliates of the Gen II Group;
- Our department heads, as well as respective shareholders, agents, employees, consultants, representatives, financial intermediaries, auditors;
- Third parties that provide services to us such as IT suppliers (including forensic specialists), cloud-hosted applications, payroll service providers, background check services, financial, tax or legal advisors or institutions or accountants appointed by the Employer, insurance companies or brokers, travel agencies, transportation companies, hotels, catering companies, lunch voucher provider, tele-surveillance providers, shipment/courier companies, car leasing companies, credit card companies, photographers etc. Such third-party providers shall process your Personal Data upon our instructions or based on their know-how and expertise but with the aim to provide you with a benefit or service;
- Our clients or prospective clients in the context of services provided or proposed by Gen II and to the extent required for the provision of these services by you as an employee or to respond to certain limited diversity related inquiries by our clients or prospective clients;
- Third parties requesting verification of employment and references, providing general information concerning the employee such as dates of employment and positions held. No other data or information regarding any current or former Gen II employee, or their employment with Gen II, will be furnished unless the employee authorizes Gen II to do so in writing and also releases Gen II from liability in connection with the sharing of this information, or unless Gen II is required by law to furnish such information.
- Governmental, judicial, social security and supervisory authorities (data protection agencies, tax administrations, courts, regulators etc.) to the extent legally permitted or required;
- Third parties in the context of a sale of some or all of the Gen II business under strict confidentiality arrangements.

The privacy policy of external providers and third parties as well as their details, are available upon request to be sent via email to privacy@gen2fund.com. They are also made available on their websites or mobile applications when you choose to sign up for their services.

When you participate in events organized by Gen II or representing Gen II, you understand that your photo may be taken and videos depicting you or your likeness may be recorded by us (or communicated to us by you) for our legitimate interest to communicate about our activities, business related matters, talent and human resources, as well as our achievements, innovation and corporate social responsibility initiatives. Such photos or recordings may be shared internally or with the Gen II Group or may be published on our website and social media pages and/or the press for the above-mentioned purposes. You may at any time contact privacy@gen2fund.com in case you no longer wish for your photo/ video to be taken or published/shared with third parties as described herein.

We may share non-personal, completely anonymized, and aggregated information with third parties for several purposes, including data analytics, research, and thought leadership purposes.

4. How long do we keep/maintain your Personal Data?

We will maintain your Personal Data in principle for the longest of the following periods: (i) as long as is required for the processing in question, (ii) as long as necessary to comply with our legal and regulatory obligations or (iii) the limitation periods for litigation. Retention periods may vary based on

the processing activity, data collected or documents it is linked to; in case of specific questions please reach out to privacy@gen2fund.com.

5. How do we protect your Personal Data?

We use a combination of technical and organizational measures to make sure we keep your Personal Data secure, accurate and up to date. These measures include:

a. Administrative and technical controls to restrict access on a need-to-know basis;
b. Technological security measures including firewalls, encryption, and anti-virus software;
c. Physical security measures such as access badges to protect our premises;
d. IT security measures to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
e. Safeguards to ensure our ability to restore data in a timely manner in the event of technical or physical incident;
f. Processes for regular testing, assessment, and evaluation of the effectiveness of our measures;
g. Education and training of relevant staff to ensure they are aware of our privacy and confidentiality obligations when we handle Personal Data.

6. What are your privacy rights?

a) Right to information, rectification, erasure, and restriction of processing

In certain jurisdictions, you have the right to make a request to obtain, at no cost, within reasonable intervals and in a timely manner, the communication of your Personal Data being processed, as well as all information on the origin of such data.

In certain jurisdictions, you also have the right to rectify your Personal Data in case of inaccuracies.

In cases where the accuracy of the Personal Data is challenged, the processing is unlawful, or where you have objected to the processing of your Personal Data, you may ask for the restriction of the processing of such Personal Data. Should a processing be restricted, you will be informed before the restriction of processing is lifted.

In certain jurisdictions, you may request the deletion of Personal Data, without undue delay, when the use or other processing of such Personal Data is no longer necessary for the purposes described above, and in particular when consent relating to a specific processing has been withdrawn or where the processing is not or no longer lawful for other reasons.

b) Right to object

In certain jurisdictions, you may object to processing of your Personal Data which is based on the legitimate interests pursued by Gen II or by a third party. In such a case, Gen II will no longer process your Personal Data unless it has compelling legitimate grounds for the processing which override your interests, rights, and freedoms or for the establishment, exercise, or defense of legal claims.

c) Right to withdraw consent

You have the right to withdraw your consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. The withdrawal of consent shall only affect future processing.

d) Right to data portability

Where the processing of your data is based on consent or the execution of a contract with you, you may also have the right to data portability for information you provided to the Employer, meaning you can obtain a copy of your data in a commonly used electronic format so that you can manage and transmit it to another data controller.

e) Right to lodge a complaint

Should you wish to make a complaint about how Gen II processes your Personal Data, please contact our Global Data Protection Officer at privacy@gen2fund.com; your request will be processed as soon as possible. This is without prejudice to your potential right to file a complaint with the competent data protection authorities in your jurisdiction (in case such is foreseen in applicable law), should you have concerns about the processing of your Personal Data.

You can exercise your rights any time by contacting our Global Data Protection Officer, at the following address: privacy@gen2fund.com.

In order to reply to your request, we may ask to verify your identity. We undertake to handle each request within a reasonable timeframe of one (1) month.

7. Data Privacy Framework

Gen II complies with the EU-U.S. Data Privacy Framework ("**EU-U.S. DPF**") and the UK Extension to the EU-U.S. DPF, as set forth by the U.S. Department of Commerce. Gen II has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles ("**EU-U.S. DPF Principles**") with regard to the processing of Personal Data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework ("**DPF**") Program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

Gen II collects, uses, discloses, and disposes of Human Resource data. The specific scope and purpose of the data processing under the DPF is described in detail above in this Privacy Statement.

The type of third parties to which Gen II discloses information and the purposes for which it does so are described in Section 3 of this Privacy Statement.

We are subject to the investigatory and enforcement powers of the Federal Trade Commission ("**FTC**").

Individual Rights:

You have the right to access your Personal Data and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the DPF Principles, except where the burden or expense of providing access would be disproportionate to the risks to your privacy or where the rights of persons other than yours would be violated.

Additionally, you have the right to request that we limit the use and disclosure of your Personal Data. Specifically, you have the right to choose whether your Personal Data may be disclosed to a third party or used for a purpose that is materially different from the purpose stated herein. Once we receive and confirm the request, we will stop using or sharing the Personal Data, except as necessary to perform our services reasonably expected by an average consumer who requests those services and as permitted by applicable laws and regulations.

If you wish to limit the use or disclosure of personal information in accordance with the Framework, please contact the Global Data Protection Officer at privacy@gen2fund.com.

Accountability for Onward Transfer:
Gen II may share your Personal Data with external third parties, such as vendors, consultants and other service providers who are performing certain services on behalf of Gen II. Such third parties have access to Personal Data solely for the purposes of performing the services specified in the applicable service contract, and not for any other purpose. Gen II may face potential liability when we perform onward transfers to third parties. Gen II's accountability for Personal Data that we receive under the EU-US DPF, and the UK Extension to the EU-US DPF and subsequently transfer to a third party is described in the DPF program set forth by the US Department of Commerce ("**DoC**"). Gen II remains responsible and liable under the DPF Principles if a third-party engages to process the personal data on our behalf in a manner inconsistent with the DPF Principles, unless Gen II US proves that we are not responsible for the event giving rise to the damage.

In cases of onward transfer to third parties of human resource data received pursuant to the DPF, Gen II US shall remain liable under the DPF Principles, if its agent processes such personal information in a manner inconsistent with the DPF Principles, unless Gen II US proves that it is not responsible for the event giving rise to the damage.

Please note that Gen II may disclose Personal Information in response to a lawful request by public authorities, including to meet national security or law enforcement requirements.

Dispute Resolution – Independent Recourse Mechanism:
We are committed to resolving any privacy complaints under the DPF Principles. Therefore, in compliance with the EU-U.S. DPF, and the UK Extension to the EU-US DPF, Gen II US commits to cooperate and comply with the advice of the panel established by the EU Data Protection Authorities ("**DPAs**"), and the UK Information Commissioner's Office ("**ICO**") with regard to unresolved complaints concerning the handling of Personal Data received in reliance on the EU-US DPF, and the UK Extension to the EU-U.S. DPF.

To contact us regarding any transfers made under the DPF, please reach out directly to our Global Data Protection Officer at privacy@gen2fund.com. If you have not received timely response to your concern, or we have not addressed your concern to your satisfaction, you may seek further assistance, at no cost to you, from the EU DPA panel, which acts as our organization's independent recourse mechanism. Individuals can invoke this right by contacting their national DPA: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en

If your DPF concern cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms: https://www.dataprivacyframework.gov/s/article/G-Arbitration-Procedures-dpf?tabset-35584=2.

8. SPECIAL NOTICE TO CALIFORNIA RESIDENTS

This section of the Privacy Statement supplements the information provided herein and applies solely to individuals who reside in the U.S. State of California. The purpose of this section is to demonstrate our compliance with the CCPA, CPRA and other California privacy laws.

Information we collect: We collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular

consumer or device ("**Personal Information**"). In particular, we have collected the categories of Personal Information detailed under Section 3 hereabove within the last twelve (12) months.

Sensitive Personal Information: We do collect the categories of Sensitive Personal Information detailed under Section 3 hereabove.

Personal Information does not include:
Publicly available information from government records;
De-identified or aggregated consumer information;
Information excluded from the CCPA's scope, like:
health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data; personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

Sources: We obtain the categories of Personal Information listed above from the sources indicated under Section 2 here above.

Use of Personal Information: We may use the Personal Information we collect for one or more of the purposes identified under Section 4 here above. We do not collect additional categories of Personal Information or use the Personal Information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Sharing Personal Information: We may disclose your personal information to a third party for a business purpose as indicated under Section 5 here above. When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to keep that Personal Information confidential and not use it for any purpose except those related to performing the contract. In the past 12 months, we have disclosed the Personal Information for the purposes and to the parties identified in Section 5 above.

Sale of Personal Information: In the past 12 months, we have not sold any Personal Information.

The CCPA/CPRA grants additional privacy rights with respect to your Personal Information. Please note that the CCPA/CPRA provides certain exceptions with respect to the Personal Information of California job applicants, you may therefore not have all of the privacy rights listed below in connection with Personal Information we have about you in the context of the specific relationship with you.

The CCPA/CPRA privacy rights may include:

Access to specific information and data portability rights:
You may have the right to request that we disclose certain information to you about our collection and use of your Personal Information over the past 12 months. Once we receive and confirm your verifiable consumer request, we will disclose to you:

- the categories of Personal Information that we collected about you;
  (ii) the categories of sources from which that Personal Information was collected;
  (iii) our business or commercial purpose for collecting or selling/sharing that Personal Information;
  (iv) the categories of third parties with whom we share that Personal Information;
  (v) the specific pieces of Personal Information we collected about you;

(vi) if we sold or disclosed your Personal Information for a business purpose, two separate lists disclosing:

- Sales, identifying the Personal Information categories that each category of recipient purchased and
- Disclosures for a business purpose, identifying the Personal Information categories that each category of recipient obtained.

Right to limit the use and disclosure of Sensitive Personal Information:
You may have the right to request that we limit our use and disclosure of your Sensitive Personal Information. Once we receive and confirm your verifiable consumer request, we will stop using or sharing your Sensitive Personal Information, except as necessary to perform our services reasonably expected by an average consumer who requests those services and as permitted by applicable laws and regulations.

Right to correct: You may have the right to correct your Personal Information. Once we receive and confirm your verifiable consumer request, we will make commercially reasonable efforts to correct any inaccurate Personal Information we hold about you.

Right to opt-out of Personal Information sharing: You have the right to request that we stop sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing or by electronic or other means, your Personal Information and Sensitive Personal Information, including for the purposes of cross-context behavioral advertising. Please note that this right shall not include sharing of Personal Information when:

(a) you use or direct us to intentionally disclose Personal Information or intentionally interact with one or more third parties;
(b) we use or share an identifier for a consumer who has opted out of the sharing of their Personal Information or limited the use of their Sensitive Personal Information for the purposes of alerting persons that the consumer has opted out of the sharing of their Personal Information or limited the use of the consumer's Sensitive Personal Information; and
(c) we transfer to a third party your Personal Information as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of our business, provided that information is used or shared consistently. If the third party materially alters how it uses or shares the Personal Information in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to you. Such notice shall be sufficiently prominent and robust to ensure that you can easily exercise your rights.

Deletion Request Rights:
You may have the right to request that we delete any Personal Information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we will delete (and direct our service providers to delete) your Personal Information from our records, unless an exception applies.
We may deny your deletion request if retaining the information is necessary for us or our service providers to:

- Complete the transaction for which we collected the Personal Information, provide a service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.

- Debug products to identify and repair errors that impair existing intended functionality. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 seq.).
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.
- Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
- Comply with a legal obligation.
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

Exercise Access, Data Portability and Deletion Rights:
To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to us by email at privacy@gen2fund.com.

Only you or a person registered with the California Secretary of State that you authorize to act on your behalf, may make a verifiable consumer request related to your Personal Information. You may also make a verifiable consumer request on behalf of your minor child.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. 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.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

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. Making a verifiable consumer request does not require you to create an account with us. We will only use Personal Information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Response Timing and Format:

We endeavor to respond to a verifiable consumer request within 45 days of its receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing. If you have an account with us, we will deliver our written response to the registered email associated with the account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option. Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your Personal Information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your 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 you with a cost estimate before completing your request.

Non-Discrimination

We will not discriminate against you for exercising any of your CCPA rights. Unless permitted by the CCPA, we will not:

- Deny you use of our services.
- Provide you with a different level or quality of services.

9. SPECIAL MENTION TO THE USE OF COMMUNICATION AND COMPUTER SYSTEMS FOR US EMPLOYEES

Gen II communication and computer systems are intended for business purposes. This includes the computers, related hardware, software, and networks, as well as telephones, voice mail, e-mail, Internet systems, and other computer or electronic communication or data storage systems. Any personal use must be kept to a minimum and not interfere with performance or operations and must not violate any Company policy or applicable law.

Employees' access to the computer systems is limited to documents, emails and other information that is necessary for their jobs. Employees are prohibited from searching for, accessing, viewing, printing and/or using documents, e-mails, and any other data stored on the computer systems in the absence of a legitimate business need or Company objective, and any such use will be considered unauthorized.

Employees have no legitimate expectation of personal privacy regarding their use of the Gen II systems and/or with respect to any matter stored in, created, received, accessed through, or sent over the Gen II systems, whether Company related or personal.

All employees are advised that any and all telephone conversations or transmissions, electronic mail or transmissions, transmissions made through other Company applications or programs, or any internet access or usage by an employee by any electronic device or system, including but not limited to the use of a computer, telephone, wire, radio, or electromagnetic, photoelectronic or photo-optical systems may be subject to monitoring by the Company at any and all times and by any lawful means.

More specifically, Gen II may access, monitor, review, use, and disclose any and all aspects of the computer systems and all communications, files, documents, or other information contained on or accessible through the computer systems, including without limitation, past voice mail and e-mail messages, documents, metadata and other electronic information without notice to users of the system, in the ordinary course of business when the Company deems it appropriate to do so. Further, Gen II may review Internet usage. This includes possible monitoring by the Company of websites visited by employees, chat rooms, instant messages, news groups and social networking activities, e-mail (including personal e-mail accounts and communications, such as Gmail, Hotmail, Yahoo Mail, Facebook, or Twitter / X, accessed by employees using the Computer Systems), and blogs, as well as the review of deleted files, temporary files, cached files, browsing history, phone numbers dialed and of calls received, metadata, and other electronic information stored on the Company's central back-up system or otherwise available as part of its data management, in all cases whether such systems, data, accounts, or uses are Company-related or personal. An employee does not have any greater right of privacy or otherwise diminish the Company's right of access, review, use and/or disclosure by using passwords or other security measures on the Company's Computer Systems. In addition, system security features do not create any privacy rights for employees in the messages and files on the Computer Systems. Also, files that employees delete can be retrieved and pages they view can be monitored by the Company in real time or after they have viewed them. As a condition of use, employees expressly consent to the Company's monitoring and/or recording of telephone calls made via the Company's telephones, as well as other monitoring as set forth above.

The Company's monitoring of the computer systems may also include, but is not limited to, accessing, recording, disclosing, intercepting, inspecting, reviewing, retrieving, and printing communications, logins, and other uses of the computer systems, as well as keystroke capturing and/or other network sniffing technologies. This examination and monitoring may be performed by observation, audit, or through other means. The reasons for which the Company may obtain such access include, but are not limited to: maintaining the system; preventing or investigating allegations of system abuse or misuse; conducting other investigations; assuring compliance with software copyright laws; complying with

legal and regulatory requests for information; and ensuring that Company operations continue appropriately during an employee's absence.

In addition, by using the computer systems, employees expressly waive all applicable privileges, including but not limited to the privilege against self-incrimination and the attorney-client, attorney work product, doctor-patient, accountant-client, clergy-penitent, sexual assault counselor-victim, domestic violence advocate-victim, and marital privileges, with respect to any matter stored in, created, received, accessed through, or sent over the computer systems. Employees should not keep any personal information or files on the computer systems if they do not want the Company to see or access that information.

The Company may store electronic communications and other electronic data for a period of time after the communication or other data is created. From time to time, copies of communications and data may be deleted.

The Company's policies, including but not limited to those prohibiting harassment, solicitations and disclosure of trade secrets or other confidential business or proprietary information of Gen II or its customers, in their entirety, apply to the use of the Company's communication and computer systems. Additionally, employees may not use the Company's communication and computer systems in violation of any law, including but not limited to those related to copyrights and software piracy.

All employees, upon request, must inform management of any private access codes or passwords.

No employee may access, or attempt to obtain access to, another employee's communication or computer systems without appropriate authorization.

Employees may not install, duplicate, or remove software on the Company's computer systems without prior management approval. Personal computers and other electronic devices (cell phones, PDAs, etc.) may not be connected directly to the Company's computer systems without prior management approval.

Employees are prohibited from using personal e-mail accounts to conduct Company business. Employees may not use any third-party email or instant messaging accounts or services (such as Gmail, AOL, Yahoo) on the Company's computer systems that are not ordinarily used in the performance of their job duties.

When traveling internationally, employees are prohibited from logging into or otherwise accessing Gen II's electronic systems unless they follow the process indicated in the Employee Handbook.

Employees must take every precaution to protect proprietary and confidential business information about Gen II and our clients. Employees are prohibited from sending or forwarding confidential messages, files, or other information to unauthorized persons or outside locations.

Some employees may be authorized to use their own portable communication devices (PCDs) for business purposes. These employees should work with the IT department to configure their PCD for business use. Employees have no reasonable expectation of personal privacy regarding the use of such devices for business purposes, and all use is subject to monitoring, to the maximum extent permitted by applicable law. Communications sent via a personal PCD also may be subject to monitoring if sent through the Company's networks, and the PCD must be provided for inspection and review upon request. Additional information on the use of PCDs is available in the Employee Handbook.

10. Amendment of this Privacy Statement

This Privacy Statement shall be made available to you during your onboarding to the company and permanently thereafter on our website. The Employer may amend this Privacy Statement from time to time to ensure that you are fully informed about all processing activities and the Employer's compliance with applicable data protection legislation.