PUBLIC PRIVACY STATEMENT

At Gen II, we are committed to your privacy and data protection, and we believe in the empowerment of your privacy rights. This Privacy Statement describes how we may collect and use information relating to you as an identified or identifiable natural person ("Personal Data"), whether directly or indirectly, manually or via automated means or otherwise. Please note that as our use of your Personal Data depends on how you interact with us, our services and/or our website, not all parts of this Privacy Statement may apply to you.
*If you work for or are seconded to Gen II, please refer to the Gen II Staff Privacy Statements.

*If you are seeking employment with Gen II, please refer to the Gen II Candidate Privacy Statement which can be found here and within each job opening description.

*For more information about the cookie collection on our website, please refer to our Cookie Notice.

Gen II (or "we", "our", "us") refers to one or more of the legal entities of the Gen II Group which you may have a business engagement or other relationship or in general interact with.

Gen II Luxembourg Services SARL, located at 22, Rue des Bruyères, L-1274 Howald, has been designated as Gen II's representative in the European Union for data protection matters, pursuant to Article 27 of the General Data Protection Regulation.

Gen II processes Personal Data in compliance with applicable laws and regulations, in particular, in accordance with the Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR"), the UK's retained version of Regulation EU 2016/678 and the Data Protection Act 2018 ("UK GDPR"), the Data Protection (Jersey) Law 2018 and the Data Protection Authority (Jersey) Law 2018 ("Jersey DPL"), the Data Protection Acts 1988 to 2003 and the Data Protection Act of 2018 of the Republic of Ireland, the Canadian Personal Information Protection and Electronics Documents Act ("PIPEDA"), as well as the California Consumer Privacy Act ("CCPA") as amended and/or replaced by the California Privacy Rights Act ("CPRA") and currently in force (GDPR, CCPA, CPRA and all other applicable privacy laws and regulations are all collectively referred to in this Privacy Statement as "Data Protection Legislation").
Each of the Gen II legal entities mentioned above shall act independently as a controller / data controller, within the meaning of the Data Protection Legislation, depending on the purposes described herein.

Accessibility

If you require support or an alternative format to review this Privacy Statement, please contact us through any of the contact methods listed below.

1. Personal data we may collect

The Personal Data we may collect or generate about you depends on your interactions and engagement with us, be it through our website and social media pages, our service offering or collaboration with our service providers and stakeholders.

We may at times collect the following categories of Personal Data:

Data automatically collected or generated – When you visit our website or interact with software and applications that we either own or are licensed to use and make available to you, we may collect data such as your connectivity, technical and aggregated usage data, your IP address and public location, device and application data (like type, operating system, mobile device or app id, browser version, language settings), date and time stamps of usage, the relevant cookies and other tracking technologies installed on or interacted with via your device, your activity (including sessions, clicks, use of available features, logged interactions). Please note that we use analytics tools (e.g., Google Analytics or Adobe Analytics) to collect data about the use of our website and other applications. Analytics tools collect data such as frequency

of visits, pages visited, source of visit and interactions with our various online features. More information regarding the use of cookies and other tracking mechanisms can be found in our Cookie Policy.

- **Contact details,** such as your name, surname, job title, email address, professional or home address, country of residence, phone number.

- **Photo, image or likeness** and information related to access and video-surveillance logs (collected via our badge readers and video-surveillance systems in our premises).

- **Financial and tax-related information**, such as your income, tax identification number, tax residency, tax status, payment or bank account details, shares, but only when necessary for us to provide our services directly to you or to our clients. Your source of wealth and source of funds information in the context of our statutory obligations under anti-money laundering, countering terrorist and proliferation financing, sanctions, and due diligence information requirements; this may vary depending on what you state to be your source of wealth and funds (e.g., information regarding any relevant inheritances, your income, your employment, your assets and investments, your bank account details and credit history).

- **Identification and background information**, such as your name, birthday, national ID, passport, immigration visa, social security number, signature, your occupation, professional and employment information (which may include your level of education, professional qualifications, professional / regulatory body memberships, your present employment, employer's name and details of directorships and other offices which you may hold) and information collected in the context of our regulatory and security background and compliance checks and other related processes, including but not limited to our client acceptance process and our vendor due diligence and other risk management processes.

- Information you choose to upload on your **social media** when you render your account public and interact with us online or include relevant links in your communications with us. This may include your photo, lifestyle and social circumstances, marital status and members of your family, employment and education details and any other information you have chosen to upload publicly or share with us.

  Our customers and vendors may provide us with additional data such as their billing details, business needs and preferences. Such information will not be treated as personal data to the extent it concerns a legal entity and therefore not an identifiable human being (e.g., corporate bank account, billing address or generic email address).

- We may sometimes collect, and process so called "sensitive" or "special categories of" Personal Data but this will be limited to what is required to provide you or our clients with the relevant services or interactions, to the extent the processing is necessary for us to meet a legal or regulatory obligation or is otherwise expressly permitted by the Data Protection Legislation or in certain exceptional circumstances where, we have first obtained your explicit consent. Special Categories of Personal Data includes information about your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, and data concerning health, sex life, and sexual orientation as well as, in certain countries/territories, criminal record and sanction screening data. Please note that, unless required, we will not actively ask you to provide us with such type of Personal Data and we would strongly advise you against disclosing it to us without reason.

  Where we are provided with your Personal Data indirectly (mainly via our clients or other third parties), we take steps to ensure that you are informed and that our interlocutors comply with their own obligations under the Data Protection Legislation. This may include your receiving this Privacy Statement from a third party, in which case you can always contact us via the methods detailed below in order to request more information in this regard.

  Save where we may administer trusts to which there are child beneficiaries, we do not knowingly collect or process Personal Data from children under the age of sixteen (16). We strongly advise all parents and guardians to teach their children safe and responsible handling of Personal Data on the internet. If you are a parent or a guardian and you become aware that your child has provided us with their Personal

Data, please contact us. If we become aware that we have inadvertently collected Personal Data from an individual under the age of sixteen, we will attempt to prohibit and block such use and will take appropriate steps to promptly delete any Personal Data stored with us with regard to such child. If we need to rely on consent as a legal basis for processing Personal Data related to an underaged individual, we will seek a parent's or guardian's consent before we collect or use that Personal Data.

2. How We Use Your Personal Data

We use your Personal Data adhering to the basic principles of the Data Protection Legislation for specific and limited purposes and only where we have a valid legal basis:

a. In the context of our services and business relationships

- For the performance of an agreement, or for entering into an agreement with you;
- To provide you with access to our portals and any of our software applications and their functionalities (either owned by us or licensed to us);
- To provide, improve and secure our services or as otherwise required in connection with our services to you or our clients;
- To internally facilitate and streamline our operations via procedures, workflows and related tools;
- To fulfil our legitimate interest in the effective and lawful operation of our business so long as such interest is not outweighed by your rights and interests;
- To manage our relationships with our clients, prospective clients, suppliers, service providers, subcontractors and external consultants, including maintaining contacts of prospective clients, initial client account opening, risk assessment and client acceptance processes, financial accounting, invoicing and risk analysis purposes, ongoing relationship management which may involve ongoing risk assessments, communication of service offerings and updates related to our business, contacting you to receive feedback on our services;
- To respond to your inquiries and communications, send you information as part of the services;
- To make sure we have a business continuity plan in place;
- To facilitate services we receive from our professional advisors, such as lawyers, accountants, auditors and consultants or other service providers (such as archiving, security services, IT, printing or other);
- To maintain a digital mail office for incoming and outgoing correspondence, including in the context of domiciliation services;
- To identify our client opportunities such as maintenance of relationships with stakeholders and our centers of influence as well as to ensure external representation of Gen II, cross-border collaboration, reporting on sales activities and education of new salespeople;
- To share references with potential clients to the extent you have not objected to it;
- To ensure security threat protection and prevention of data breaches as well as cyber-attacks;
- To configure and manage access rights for our visitors in order to prevent unauthorized presence in our offices ;
- To facilitate spaces arrangement (office and parking) of our visitors;
- For the security of access to the internal Wifi Network. Such use of your Personal Data may at times require your explicit consent, in which case we will prompt you to actively provide it via electronic means and you will always be able to opt-out if you no longer wish for such use of your data to take place;
- For quality control of client deliverables, internal incident reporting and implementation of security controls; To transfer your call messages or other communications to the concerned staff members;

b. For our legal and regulatory obligations

- To verify your identity, where we are legally allowed or obliged to do so;
- To comply with our legal or regulatory obligations (such as anti-money laundering/know your customer obligations customer and vendor due diligence, commercial, tax, regulatory or reporting duties, professional duties and compliance with requests or requirements of any public authority);
- To confirm the good standing of service providers (vendor due diligence), prevent fraud, anti-money laundering and terrorist financing;
- To prevent potentially illegal activities, to screen for and prevent undesirable or abusive activity (phishing,

spam, etc.), fraud and credit risk;
- To protect the rights, property, or safety of Gen II and its assets, including but not limited to our offices, IT infrastructure, proprietary software, our employees, clients, visitors, or contractors while present at our premises and to detect unlawful or dangerous behaviors (including by monitoring access to our premises, infrastructure and assets and use thereof, implementing cybersecurity programs and using video surveillance tools in specific public areas of our premises as disclosed therein);
- To manage litigation and other claims or complaints and to alert and assist enforcement authorities in case of incident or unlawful act.

c. In the context of our website and online presence

- To administer, operate, maintain, and support our website, social media and other online applications;
- To understand and analyze the usage trends and preferences of our visitors and users, to present our website and its contents in a suitable and effective manner for you, to create statistics and reporting for internal purposes only;
- To understand how our services are used and how our campaigns are performing, and to gain insights which help us dedicate our resources and efforts more efficiently;
- To enhance Gen II's online visibility in marketing, advertising, and selling our services to you and others;
- To facilitate and optimize our marketing campaigns, to measure the effectiveness of the external marketing campaigns, ad management and sales operations, and to manage and deliver advertisements for our products and services more effectively, including on other websites and applications. Such activities allow us to highlight the benefits of using our services, and thereby to increase your engagement and overall satisfaction with our services. This includes contextual, behavioral, and interest-based advertising based on the visitor's activity, preferences, or other data available to us or to our service providers and business partners. Such use of your Personal Data may at times require your explicit consent, in which case we will prompt you to actively provide it via electronic means and you will always be able to opt-out if you no longer wish for such use of your data to take place;
- To address Gen II commercial communications to you (as long as you have agreed to this at the point of providing your Personal Information and for as long as you do not opt- out) or to notify you about any changes to our services;
- To ensure our business development and related promotional activities such as client or employee testimonials or reviews.
- To enable your contact with the Company via the website;
- To communicate with our clients and prospects, management of newsletter subscriptions, as well as statistics and reporting;
- To facilitate the recruitment on publicly available platforms.

d. In the context of events and our Corporate Social Responsibility

- To organize events and other online or offline initiatives in the context of our Corporate Social Responsibility and to extend invitations to you thereto as well as prepare related communications and promotional material, press releases, articles, interviews or other.

3. Source of collection of personal data

Gen II may collect your Personal Data through various sources as listed here below:

a. Directly from you

- On such forms and documents you may complete and provide to us either by way of enquiry or as we may require from you in respect to the services we provide;
- On such documents as are submitted to us as part of our due diligence gathering procedures and/or in compliance with any other statutory or regulatory requirements;
- Any personal information provided by way of correspondence with us by telephone, e-mail or otherwise.

b. From third-party sources:

- Legal entities in which you have an ownership, management or employment interest;
- Your or your above entities professional advisors;
- Company registries, court databases, published sanctions/ sanctions databases, financial crime databases or credit reference databases;
- Other financial institutions who hold and process your personal information and who may share that with us;
- Regulators or other official authorities with jurisdiction over us or those structures that we administer or otherwise provide services in respect of;
- Other publicly available information such as published articles and online content.

c. From system generated information:

- CCTV and/or electronic swipe card use in our different office premises;
- Cookies and similar technology in use on our website(s);
- IT system monitoring in the event we provide you with access to our IT systems or provide any form of client portal.

4. How We May Share/Disclose Your Personal Data

In order to achieve the purposes listed above, we may disclose your Personal Data in the following situations:

a. **To our affiliates and members of the Gen II Group: We may share your Personal Data with our affiliates** when necessary for us to provide you with our services or when we have been asked by our clients to do so. All our affiliates are required to abide by this Privacy Statement.

b. **With our service providers, consultants, advisers, insurers and insurance agents, auditors or business partners and sub-processors:** Where necessary for us to support or administer our services and business, including promotion thereof. Third parties, processing your Personal Data on our behalf, will receive only limited Personal Data for the specific purpose for which they have been appointed. We enter into confidentiality and data processing agreements with all our partners to ensure that they comply with high levels of confidentiality and privacy and security standards, which we regularly review and are allowed to audit.

c. **With a client's own approved service providers** where Gen II is providing services and in its capacity as processor is following instructions to do so.

d. **Public authorities and related bodies:** to the extent required under applicable laws and where necessary to comply with our own legal and regulatory obligations. We may disclose your Personal Data to enforce applicable policies, including investigation of potential violations, to detect, prevent, or otherwise address fraud, security, or technical issues, and to protect against harm to the rights, property, or safety of our users, the public and/or as required or permitted by law.

e. **For business transfers:** We may disclose and transfer your Personal Data if we are involved in a merger, sale, acquisition, restructuring, reorganization, dissolution, bankruptcy or other change of ownership or control including due diligence of such transaction.

f. **With other online users or the public:** When you share your Personal Data or otherwise interact in public areas or online (for example on our social media platforms) with other individuals, such information may be viewed by other users and may be publicly distributed outside.

g. **With your consent:** We may disclose your Personal Data for any other purpose with your consent. Should you decide to participate in events, workshops, trainings, or other initiatives organized or sponsored by Gen II, please note that your image or likeness may appear on photos or videos taken by Gen II or on its behalf and may be shared publicly for purposes related to the event or initiative. If you wish to object to such publication you may contact us via the means described below.

5. Where We May Transfer Your Personal Data

We maintain, store, and process your Personal Data in the following locations:

a) within the European Economic Area or certain other countries or territories deemed to provide adequate safeguards for the protection of Personal Data by the European Commission, in particular in Luxembourg, Ireland, Jersey and the UK; and
b) within the United States of America, if you are mainly interacting with our Gen II entities in the US or via our website.

Your Personal Data may also be transferred to other locations as reasonably necessary in the context of our collaboration with certain recipients mentioned above.

In case one of the locations where your Personal Data is transferred does not provide what is considered by the European Commission as an adequate level of Personal Data protection, Gen II will ensure that those Personal Data transfers are covered by appropriate safeguards such as the Standard Contractual Clauses approved by the European Commission or the UK and Jersey or any other additional mechanism proposed by competent supervisory authorities or otherwise authorized under applicable Data Protection Legislation, as the case may be.

In case one of the locations where your Personal Data is transferred does not provide what is considered by the European Commission as an adequate level of Personal Data protection, Gen II will ensure that those Personal Data transfers are covered by appropriate safeguards. Gen II is committed to the standards established in the EU-US Data Privacy Framework, the UK Extension to the EU-US DPF and the Swiss-US Data Privacy Framework (Swiss-US DPF). Additional safeguards are the Standard Contractual Clauses approved by the European Commission or the UK and Jersey or any other additional mechanism proposed by competent supervisory authorities or otherwise authorized under applicable Data Protection Legislation, as the case may be.

For more details on our commitments to the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) and the rights of EU, UK and Swiss individuals, please see section 9. EU-US DATA PRIVACY FRAMEWORK, THE UK EXTENSION TO THE EU-U.S. DPF, AND THE SWISS-U.S. DATA PRIVACY FRAMEWORK

Gen II will always take all steps reasonably necessary to ensure that your Personal Data is treated securely and in accordance with this Privacy Statement and the Data Protection Legislation and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your Personal Data.

6. How Long We Store Your Personal Data

We will store your Personal Data only for as long as necessary for the relevant processing activity to be completed and/or for the retention period necessary for us to comply with our legal and regulatory obligations, resolve related disputes and enforce our legal agreements and policies.
Anonymized data may be maintained by Gen II for longer periods of time, as necessary for reporting, statistics, training purposes as well as for us to be able to strengthen our security or improve our services and the functionalities of the applications we offer.

7. How We Protect And Secure Your Personal Data

We use a range of administrative, technical, and physical safeguards in order to ensure that we keep your Personal Data secure, accurate and up to date and that we protect it from loss, misuse, unauthorized access, disclosure, unauthorized alteration, or unlawful destruction. We will manage and maintain Personal Data Breach records in a privacy software. In addition, we require IT and security service providers to put in place appropriate technical and organizational security measures in respect of any of your Personal Data.

The above measures include:

a. Education and training to all our staff to ensure they are aware of our privacy obligations when handling personal data;
b. Administrative and technical controls to restrict access to your Personal Data on a "need to know" basis;
c. Technological security measures, including firewalls, encryption and anti-virus software and other security controls performed as part of our cybersecurity program; and
d. Physical security measures to access our premises.

Unfortunately, the transmission of your Personal Data via the Internet is not guaranteed to be secure. Although we do our best to protect your Personal Data, we cannot guarantee the security of your Personal Data when transmitted to us.

8. Your Rights

You have the following rights regarding the processing of your Personal Data by us, subject to applicable exemptions:

- Right to access the Personal Data held about you and receive additional information about how it is processed. That additional information includes details of the purposes of the processing, the categories of personal data concerned and the recipients of the Personal Data. Provided that the rights and freedoms of others are not affected, we will supply you a copy of your Personal Data. Two requests per year will be free of charge, more frequent requests may be subject to a reasonable fee. We will fulfill your request by sending you a copy electronically, unless the request expressly specifies a different method;
- Right to correct, or complete any inaccurate or incomplete Personal Data;
- Right to request erasure of your Personal Data from our systems (e.g., where the Personal Data is no longer necessary in relation to the specified purposes);
- Right to restrict the processing of your Personal Data in certain circumstances (e.g., where you contest its accuracy, object to this processing, or you consider the processing as unlawful);
- Right to receive your Personal Data in an interoperable format, or have it directly transmitted to another organization;
- Right to withdraw your consent at any time where you have provided us with your consent to the processing of your Personal Data; and
- Right to object the processing of your Personal Data (in particular where we rely on legitimate interests, including for profiling).

You also have the right to lodge a complaint with the competent Data Protection Authority although we would always ask that you kindly first notify any grievance in writing to our Global Data Protection Officer at the contact details below to enable us the opportunity to first try and resolve your issue. You may do so in the country of your habitual residence, your place of work or the place of the alleged infringement. For a list and contact details of the data protection regulatory authorities in our different jurisdictions please see Data Protection Supervisory Authorities.

To exercise any of these rights or if you have any questions regarding our use of your Personal Data, please contact our Global Data Protection Officer at Privacy@gen2fund.com.

We will respond to individual complaints and questions relating to privacy and will investigate and attempt to resolve all complaints. We will manage and maintain the data subject requests and privacy complaints register in a privacy software tool. We will only be able to answer favorably to any of the above requests related to the right to oppose, right of erasure and right of restriction provided that it does not interfere with, or contradict our legal obligations (e.g. a legal obligation to keep the related Personal Data, or a legal obligation to protect the Personal Data of another individual) or due to any other impediment that would justify that we would not be able to grant such requests.

In order to comply with your request, we may ask you to verify your identity. We undertake to handle each request without undue delay and within the timeframes set out by applicable Data Protection Legislation, which will typically be one (1) month or four (4) weeks.

9. Eu-Us Data Privacy Framework, The Uk Extension To The Eu-U.s. Dpf, And The Swiss-U.s. Data Privacy Framework

The following Gen II U.S. entities are adhering to the EU-U.S. DPF Principles, including as applicable under the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF Principles: Gen II Fund Services (Colorado), LLC, Sensr Solutions, LLC, Gen II Compliance Services, LLC, LLC, Gen II Fund Services (Texas), LLC, Gen II Management, LLC, Gen II Tax Services, LLC, Gen II Fund Services (Florida), LLC, Gen II Fund Services (New Jersey) LLC, Gen II Fund Services (California), LLC, Gen II Fund Services, LLC.

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, and the Swiss-U.S. Data Privacy Framework (Swiss-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), including the UK Extension to the EU-U.S. DPF, 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. Gen II has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles, including the UK Extension to the EU-U.S. DPF, and/or the Swiss-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/.

The scope and purpose of the data processing under the EU-US Data Privacy Framework, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework is described in detail in Section 1 and 2 of 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 4 of this privacy statement.

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

Individual Rights of EU, UK and Swiss individuals:
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 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, the UK Extension to the EU-US DPF, and the Swiss-U.S. DPF and subsequently transfer to a third party is described in the DPF program set forth by the US DOC. Gen II remains responsible and liable under the EU-US DPF Principles, including the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF Principles if a third-party engages to process the personal data on our behalf in a manner inconsistent with the EU-US DPF Principles, including the UK Extension to the EU-U.S. DPF, and/or the Swiss-US 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 shall remain liable under the Principles, if its agent processes such personal information in a manner inconsistent with the 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 for EU, UK and Swiss individuals:
We are committed to resolving any privacy complaints under the DPF Principles. Therefore, in compliance with the EU-U.S. DPF, the UK Extension to the EU-US DPF, and the Swiss-U.S. DPF, Gen II US commits to cooperate and comply with the advice of the panel established by the EU Data Protection Authorities ("DPAs"), the UK Information Commissioner's Office ("ICO"), and the Swiss Federal Data Protection and Information Commissioner ("FDPIC") with regard to unresolved complaints concerning the handling of personal data received in reliance on the EU-US DPF, the UK Extension to the EU-U.S. DPF and the Swiss-US 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.

10. Special Notice To California Residents

This Section 8 of the Privacy Statement supplements the information provided herein and applies solely to visitors, users and other 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 1 herein within the last twelve (12) months.

Sensitive Personal Information: We may collect the following types of Sensitive Personal Information as such term is defined in the CCPA/CPRA: Type1.A. Personal Information that reveals a consumer's social security number, driver's license number, state ID card number and passport number, Type 1.B. Personal Information that reveals a consumer's financial account number, debit card number, credit card number. This shall not include information that is publicly available.

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 following categories of sources:

- Directly from our clients or their agents. For example, from documents that our clients provide to us related to the services for which they engage us;
- Indirectly from our clients or their agents. For example, through information we collect from our clients in the course of providing services to them;
- Directly and indirectly from activity on our website or other software applications. For example, from submissions through our website portal or website usage details collected automatically;
- From third parties that interact with us in connection with the services we perform.

Use of Personal Information: We may use the Personal Information we collect for one or more of the purposes identified herein under Section 2. 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. 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 following categories of Personal Information for the purposes and to the parties identified in Section 3 above. In the past 12 months, we have not sold any Personal Information.

The CCPA grants additional privacy rights with respect to your Personal Information. Please note that the CCPA provides certain exceptions with respect to the Personal Information of California employees, job applicants, owners, directors, vendors, suppliers, and contractors. If you are a Gen II California employee, job applicant, partner or independent contractor or a vendor or supplier of Gen II, you may not have any or all of the privacy rights listed below in connection with Personal Information we have about you in the context of that relationship with you.
The CCPA privacy rights include:

Access to specific information and data portability rights:
You 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:

(i) 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 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 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 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 a different level or quality of services.

11. Inaccurate or amended information

Please let us know as soon as possible if any of the Personal Data we hold about you changes (including your correspondence details). Failure to provide accurate information or to update information when it changes may have a detrimental impact upon our ability to provide services or communicate with you.

12. Contact

If you have any questions or comments about this Privacy Statement, the ways in which we collect and use your Personal Data, your choices, and rights regarding such use, or wish to exercise your rights under applicable Data Protection Legislation, please do not hesitate to contact us at:

Email address: Privacy@gen2fund.com

Postal address:
Gen II Luxembourg Services SARL, 22, Rue des Bruyères, L-1274 Howald, Luxembourg
Attn: Global Data Protection Officer

Phone number:
Luxembourg: +352 20281

US toll-free number:
888-GEN2-001

13. Changes To This Privacy Statement

We may from time to time update this Privacy Statement by posting an amended version on our website. The amended version will be effective as of the date it is published. When we make material changes to this Privacy Statement, we will provide you with notice as appropriate under the circumstances (e.g., by displaying a message the next time you visit our website, or by sending you an email). Please refrain from using our services in case you do not agree with the way Gen II processes your Personal Data.