PRIVACY STATEMENT FOR CANDIDATES

Dear Candidate,

Thank you for your interest in Gen II. The protection of the personally identifiable information relating to you as an individual ("**Personal Data**") already from this early stage of interaction with you is very important for us. The purpose of this Candidate Privacy Statement ("**Privacy Statement**") is to inform you about how we collect, process, use, disclose and store your Personal Data (information that can directly or indirectly identify you as an individual) in the context of your candidacy for an open position at Gen II (regardless of whether it is a full-time or part-time position, fixed or unlimited term, internship, or any other type of occupation).

We invite you to read carefully the applicable Privacy Statement for Candidates below based on your place of residence so that you can also understand your rights with respect to the privacy of your Personal Data during the recruiting process.

(Please follow the quick links below depending on your main place of residence)

Contents

CANDIDATES IN EUROPE

1) Who is Gen II?

Gen II (or 'we', 'us', 'our' as used in this Privacy Statement) refers to the Gen II legal entity that will function as your employer in the context of the specific open position.
Gen II will act as a Controller/Data Controller, as such term is defined in the applicable Data Protection Legislation.

A list of our staff engaging legal entities per jurisdiction / territory is below, alternatively please speak to Gen II Human Resources staff if you are in any doubt about which Gen II legal entity is the Controller / Data Controller of your Personal Data whilst you will be working for us.

Jurisdiction	Name	Address
Luxembourg	Gen II Luxembourg Services SARL	22, Rue des Bruyères, L-1274 Howald, Luxembourg
	Gen II Management Company (Luxembourg) SARL	
Jersey	Gen II Group Services (Jersey) Limited	47 The Esplanade, St Helier, Jersey, JE1 0BD
	Gen II (Jersey) Limited	
United Kingdom	Gen II Services (UK) Limited	8 Sackville Street, London, W1S 3DG
	Gen II Group Services (UK) Limited	1200 Parkway, Fusion 3, Whiteley, PO15 7AD
Ireland	Gen II Fund Services (Ireland) Limited	16 Fitzwilliam Place, Dublin, Ireland, D02 K227

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") (referred to in this Privacy Statement as "Data Protection Legislation").
If you have any questions or requests pertaining to the processing of your Personal Data, please contact our Global Data Protection Officer at: privacy@gen2fund.com.

2) How do we collect your Personal Data?

We may collect your Personal Data directly from you or indirectly from third parties, in the following ways:

a Directly from you:
During the recruitment process, via our website and social media, recruitment platform, correspondence exchanges, telephone conversations, interviews, or other interactions with you. You may also participate in job fairs or recruitment competitions we organize;

b. Indirectly from:
- i. the recruitment agencies with which we collaborate (when you get in direct contact with them, and they share your Personal Data with us);
- ii. referrals of other Gen II employees through our referral program or of other affiliated to us parties and stakeholders;
- iii. third parties such as social media and legally accessible online and offline platforms and databases used by our HR Department in the course of the recruitment process to the extent relevant for an open position;

iv. the people you have mentioned as your reference contacts; and

c. In an automated way:
   i. via CCTV and/or electronic swipe card use in our different office premises;
   ii. as a result of your use of our online recruitment tools (your computer or mobile device details, your IP, logs for your connectivity) or feedback forms.

3) What Personal Data could we collect?

Depending on your interaction with us, we may collect the following Personal Data from the moment you apply for an open position with Gen II until, if you are successful, you sign a contract with us:

- Identification information, such as your name, surname, middle name, nickname, and any other identification information you may choose to include in your CV and application form or on your social media pages, a copy of your ID or passport (which may also include additional details) if you accept an offer, in order for us to draft your employment agreement;

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

- Photo, in case you decide to include it in your CV or social media pages;

- Your signature when you choose to sign your motivation letter;

- Your professional information, social background and relationships such as your CV, employment and education details, job title, current and previous positions, references, professional memberships and qualifications, diplomas, hobbies, background checks, and any information you may have rendered public on social media such as LinkedIn;

- Financial information such as your previous salary and your salary and bonus expectations;

- E-mail, internet, computer, and mobile device(s) access and use monitoring details, such as your IP address, your browser type and language, access logs;
- Communication information such as email exchanges, text messages, voice mail or recruitment management system notifications;

- Professional evaluations and career assessment details, such as results of psychometric and technical tests assessing your technical knowledge and/or your organizational and managerial skills, personality questionnaires, performance assessments, feedback;

Gen II will not request or collect any sensitive Personal Data (such as health, criminal record or financial information) during the stage of recruitment. You may be requested to provide us with additional information regarding your criminal background and employment health-check where legally required, but this will only be the case once you have accepted an employment offer and signed an employment contract. Therefore, such processing of Personal Data will be governed by the Employee Privacy Statement which you will receive before signing your contract as part of the onboarding documents.

We strongly advise you against sharing any sensitive Personal Data at the stage of recruitment, whether via your CV, motivation letter or publicly available social media pages.

4) For which purposes is your Personal Data processed?

a. To assess your suitability to the position of your interest;
b. To match your remuneration expectations with our available budget;
c. To review your references ;
d. To prepare a job offer and the related contractual documentation;
e. To communicate with you for the purposes of recruitment and onboarding;

f. To manage our recruitment platforms, social media accounts and any IT tool/ software that is internally used for the documentation and handling of the recruitment process;
g. To comply with our legal and regulatory obligations (including but not limited to obligations on anti-money laundering, independence, fight against corruption or equality and diversity);
h. To communicate with public authorities where necessary (following their request or in case the position has been shared with the Administration of Work – Inspection du Travail et des Mines);
i. To produce reports and statistics for our management ;
j. To perform business improvements and related collection of feedback, conduct surveys and data analytics studies (with the aim to better understand the candidate experience and satisfaction);
k. To receive advice and support from our professional advisors where necessary (including lawyers, consultants, other service providers for archiving and security etc.).

With particular regard to the context of technical assessments, the Personal Data collected are processed in order to assess the candidates' technical skills and organizational and managerial skills to determine the fit to the relevant department for which the candidate has applied to.

The test will be scored and used, together with the analysis of the resume, to help determine whether a candidate has the right profile to move ahead in the recruitment process. This decision will not be automated: after a preliminary human review of a candidate's resume by the recruiting team, every assessment will be sent out for the review of a member of the talent acquisition team before a decision is made. The assessment will not be shared with the relevant manager, the latter will have only the feedback from the recruiting team. To have further information on how your Personal Data will be processed by the collaborating vendor, please read their privacy policy here.

5) With whom do we share your Personal Data?

Your Personal Data, in the context of recruitment, may be shared with the following recipients:

a. Our internal departments, including HR, Finances, IT and our management;
b. Our service providers, such as software providers, cloud hosting providers, our recruitment platforms and social media pages, tools used to manage and document the recruitment process;
c. Governmental, judicial, social security and supervisory authorities where necessary;
d. Other members of the Gen II Group as necessary, for example in case of shared positions or for reporting purposes;
e. The recruitment agency with which you were initially in contact in order to keep them informed about the status of your application;
f. Our advisors (for legal, tax or other matters).

Please note that some of the recipients of your Personal Data mentioned above, may be based in countries outside the European Economic Area ("EEA"), where laws may not provide the same level of data protection as that ensured within the EEA. In such cases, we shall make sure that adequate safeguards are in place to protect your Personal Data while at the same time complying with our legal and regulatory obligations. Further details regarding recipients of your Personal Data and the measures we have put in place can be obtained from us by contacting our Global Data Protection Officer at privacy@gen2fund.com.

6) For how long do we keep your Personal Data?

Gen II will keep your Personal Data for the entire duration of the recruitment process. If you are not hired, we will store your Personal Data for a period of 3 years from your last application, unless you choose to maintain your information on our recruitment management systems with the aim to apply for a new opportunity at a later stage, in which case our retention period will be extended until the moment when you delete your account from our recruitment management systems. During this period your data may be re-used by Gen II in order to contact you for a new opportunity which may be of interest to you and initiate a new recruitment process to the extent you have agreed thereto. If you are hired, your Personal Data will be stored in your HR file during the duration of our employment relationship and for 10 years thereafter.

7) How do we secure 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:

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

8) What are your privacy rights?

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

You may 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.

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. This means that Personal Data will, with the exception of storage, only be processed with or for the establishment, exercise, or defense of legal claims, for the protection of the rights of another individual or entity or for reasons of important public interest of the European Union or of an EU Member State. Should a processing be restricted, you will be informed before the restriction of processing is lifted.

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

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 also have the right to data portability for information you provided to Gen II, 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 right to file a complaint to the competent data protection regulatory authority in the jurisdiction 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 authorities in our different jurisdictions please see Data Protection Supervisory Authorities.

We will respond to individual complaints and questions relating to privacy and will investigate and attempt to resolve all complaints. We will only be able to answer favorably to any of the above requests related to your rights 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 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.

9) 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: 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, 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 Statement 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 5 of this Privacy Statement.

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

Individual Rights for EU and UK 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 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 ("**US 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 for EU and UK individuals:
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.

10) 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 laws, 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
Attn: Global Data Protection Officer

Phone number:
+352 20281

11) Amendment of this Privacy Statement

This Privacy Statement shall be made available to you when you apply for an open position at Gen II, on our online recruitment platforms. Gen II may amend this Privacy Statement from time to time to ensure that you are fully informed about all processing activities and our compliance with applicable data protection legislation. In case of material changes which take place during an active recruitment process, you will be notified of changes to this Privacy Statement by appropriate means.

CANDIDATES IN THE USA

1) Who is Gen II?

Gen II (or 'we', 'us', 'our' as used in this Privacy Statement) refers to the Gen II entity that will function as your employer in the context of the specific open position.

Gen II will act as a Controller/ Business in charge of the processing, as such terms are defined in the applicable Data Protection Legislation.

A list of our staff engaging legal entities per jurisdiction / territory is below, alternatively please speak to Gen II Human Resources staff if you are in any doubt about which Gen II legal entity is the Controller / Data Controller of your Personal Data whilst you will be working for us.

Jurisdiction	Name	Address
USA	Gen II Fund Services, LLC	1675 Broadway, New York, NY 10019
	Gen II Compliance Services, LLC	
	Sensr Solutions, LLC	
	Gen II Management, LLC	505 Sansome Street, Ste 875, San Francisco CA 94111
	Gen II Tax Services, LLC	
	Gen II Fund Services (California), LLC	4131 N. Central Expressway, Suite 800, Dallas TX 75204
	Gen II Fund Services (Texas), LLC	
	Gen II 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, New Jersey, NJ07960

Gen II processes Personal Data in compliance with applicable laws and regulations, amongst which the California Consumer Privacy Act ("CCPA") as amended and/or replaced by the California Privacy Rights Act ("CPRA") and currently in force (all collectively referred to in this Privacy Statement as "Data Protection Legislation").

Gen II Luxembourg Services SARL, with offices 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 GDPR.

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

2) How do we collect your Personal Data?

We may collect your Personal Data directly from you or indirectly from third parties, in the following ways:

a. Directly from you:
   During the recruitment process, via our website and social media, recruitment platform, correspondence exchanges, telephone conversations, interviews, or other interactions with you. You may also participate in job fairs or recruitment competitions we organize;
b. Indirectly from:
   i. the recruitment agencies with which we collaborate (when you get in direct contact with them, and they share your Personal Data with us);
   ii. referrals of other Gen II employees through our referral program or of other affiliated to us parties and stakeholders;
   iii. third parties such as social media and legally accessible online and offline platforms and databases used by our HR Department in the course of the recruitment process to the extent relevant for an open position;
   iv. the people you have mentioned as your reference contacts; and
c. In an automated way:
   i. via CCTV and/or electronic swipe card use in our different office premises;
   ii. as a result of your use of our online recruitment tools (your computer or mobile device details, your IP, logs for your connectivity) or feedback forms.

3) What Personal Data could we collect?

Depending on your interaction with us, we may collect the following Personal Data from the moment you apply for an open position with Gen II until, if you are successful, you sign a contract with us:

- **Identification information**, such as your name, surname, middle name, nickname, and any other identification information you may choose to include in your CV and application form or on your social media pages, a copy of your ID or passport (which may also include additional details) if you accept an offer, in order for us to draft your employment agreement;

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

- **Photo**, in case you decide to include it in your CV or social media pages;

- Your **signature** when you choose to sign your motivation letter;

- Your **professional information, social background and relationships** such as your CV, employment and education details, job title, current and previous positions, references, professional memberships and qualifications, diplomas, hobbies, background checks, and any information you may have rendered public on social media such as LinkedIn;

- **Financial information** such as your previous salary and your salary and bonus expectations;

- **E-mail, internet, computer, and mobile device(s) access and use monitoring details,** such as your IP address, your browser type and language, access logs;

- **Communication information** such as email exchanges, text messages, voice mail or recruitment management system notifications;

- **Professional evaluations and career assessment details,** such as results of psychometric and technical tests assessing your technical knowledge and/or your organizational and managerial skills, personality questionnaires, performance assessments, feedback;

Gen II will not request or collect any sensitive Personal Data (such as health or financial information) during the stage of recruitment. You may be requested to provide us with additional information regarding your criminal background and employment health-check where legally required, but this will only be the case once you have accepted an employment offer and signed an employment contract. Therefore, such processing of Personal Data will be governed by the Employee Privacy Statement which you will receive before signing your contract as part of the onboarding documents.

We strongly advise you against sharing any sensitive Personal Data at the stage of recruitment, whether via your CV, motivation letter or publicly available social media pages.

4) For which purposes is your Personal Data processed?

a. To assess your suitability to the position of your interest;
b. To match your remuneration expectations with our available budget;
c. To review your references ;
d. To prepare a job offer and the related contractual documentation;
e. To communicate with you for the purposes of recruitment and onboarding;
f. To manage our recruitment platforms, social media accounts and any IT tool/ software that is internally used for the documentation and handling of the recruitment process;
g. To comply with our legal and regulatory obligations (including but not limited to obligations on anti-money laundering, independence, fight against corruption or equality and diversity);
h. To communicate with public authorities where necessary;
i. To produce reports and statistics for our management;
j. To perform business improvements and related collection of feedback, conduct surveys and data analytics studies (with the aim to better understand the candidate experience and satisfaction);
k. To receive advice and support from our professional advisors where necessary (including lawyers, consultants, other service providers for archiving and security etc.).

With particular regard to the context of the technical assessments, the Personal Data collected are processed in order to assess the candidates' technical skills and organizational and managerial skills to determine the fit to the relevant department for which the candidate has applied to.
The test will be scored and used, together with the analysis of the resume, to help determine whether a candidate has the right profile to move ahead in the recruitment process. This decision will not be automated: after a preliminary human review of a candidate's resume by the recruiting team, every assessment will be sent out for the review of a member of the talent acquisition team before a decision is made. The assessment will not be shared with the relevant manager, the latter will have only the feedback from the recruiting team. To have further information on how your Personal Data will be processed by the collaborating vendor, please read their privacy policy here.

5) With whom do we share your Personal Data?

Your Personal Data, in the context of recruitment, may be shared with the following recipients:

a. Our internal departments, including HR, Finances, IT and our management;
b. Our service providers, such as software providers, cloud hosting providers, our recruitment platforms and social media pages, tools used to manage and document the recruitment process;
c. Governmental, judicial, social security and supervisory authorities where necessary;
d. Other members of the Gen II Group as necessary, for example in case of shared positions or for reporting purposes;
e. The recruitment agency with which you were initially in contact in order to keep them informed about the status of your application;
f. Our advisors (for legal, tax or other matters).

We shall make sure that adequate safeguards are in place to protect your Personal Data while at the same time complying with our legal and regulatory obligations. Further details regarding recipients of your Personal Data and the measures we have put in place can be obtained from us by contacting our Global Data Protection Officer at privacy@gen2fund.com.

6) For how long do we keep your Personal Data?

Gen II will keep your Personal Data for the entire duration of the recruitment process. If you are not hired, we will store your Personal Data for a period of 1 year from the data of last communication with you, unless you choose to maintain your information on our recruitment management systems with the aim to apply for a new opportunity at a later stage, in which case our retention period will be extended until the moment when you delete your account from our recruitment management systems. During this period your data may be re-used by Gen II in order to contact you for a new opportunity which may be of interest to you and initiate a new recruitment process to the extent you have agreed thereto. If you are hired, your Personal Data will be stored in your HR file during the duration of our employment relationship and for 10 years thereafter.

7) How do we secure 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 to relevant staff to ensure they are aware of our privacy and confidentiality obligations when we handle Personal Data.

8) 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. This means that Personal Data will, with the exception of storage, only be processed with or for the establishment, exercise, or defense of legal claims, for the protection of the rights of another individual or entity or for reasons of important public interest of the European Union or of an EU Member State. 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 also may have the right to data portability for information you provided to Gen II, meaning you may 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.

We will respond to individual complaints and questions relating to privacy and will investigate and attempt to resolve all complaints. We will only be able to answer favorably to any of the above requests related to your rights 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 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.

9) 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: 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, 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 5 of this Privacy Statement.

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

Individual Rights or EU and UK 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 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 ("**US 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 for EU and UK individuals:
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.

10) 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 laws, please do not hesitate to contact us at:

Email address: privacy@gen2fund.com

Postal address:
Gen II Fund Services, LLC
1675 Broadway,
New York, NY 10019
Attn: Global Data Protection Officer

Phone number:
US: +1 212-408-0550

11) Amendment of this Privacy Statement

This Privacy Statement shall be made available to you when you apply for an open position at Gen II, on our online recruitment platforms. Gen II may amend this Privacy Statement from time to time to ensure that you are fully informed about all processing activities and our compliance with applicable data protection legislation. In case of material changes which take place during an active recruitment process, you will be notified of changes to this Privacy Statement by appropriate means.

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 not collect any Sensitive Personal Information for the purposes of recruitment, please refrain from sharing any within your CV or motivation letter or on your publicly available profile on social media.

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:

(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 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 a different level or quality of services.

CANDIDATES IN CANADA

1) Who is Gen II?

Gen II (or we, us, our as used in this Privacy Statement) refers to Sensr Solutions (Canada), Inc. with offices at Suite 2500, Park Place, 666 Burrard Street, Vancouver BC V6C2X8, Canada, who will function as your employer in the context of the specific open position.
Gen II will function as a Data Controller, as such term is defined in the applicable Data Protection Legislation. Gen II processes Personal Data in compliance with applicable laws and regulations, in particular, in accordance with the Personal Information Protection and Electronic Documents Act ("PIPEDA") (referred to in this Privacy Statement as "Data Protection Legislation").
If you have any questions or requests pertaining to the processing of your Personal Data, please contact our Global Data Protection Officer at: privacy@gen2fund.com.

2) How do we collect your Personal Data?

We may collect your Personal Data directly from you or indirectly from third parties, in the following ways:

a. Directly from you:
   During the recruitment process, via our website and social media, recruitment platform, correspondence exchanges, telephone conversations, interviews, or other interactions with you. You may also participate in job fairs or recruitment competitions we organize;
b. Indirectly from:
   i. the recruitment agencies with which we collaborate (when you get in direct contact with them, and they share your Personal Data with us);
   ii. referrals of other Gen II employees through our referral program or of other affiliated to us parties and stakeholders;
   iii. third parties such as social media and legally accessible online and offline platforms and databases used by our HR Department in the course of the recruitment process to the extent relevant for an open position;
   iv. the people you have mentioned as your reference contacts; and
c. In an automated way:
   i. via CCTV and /or electronic swipe card use in our different office premises;
   ii. as a result of your use of our online recruitment tools (your computer or mobile device details, your IP, logs for your connectivity) or feedback forms.

3) What Personal Data could we collect?

Depending on your interaction with us, we may collect the following Personal Data from the moment you apply for an open position with Gen II until, if you are successful, you sign a contract with us:

- **Identification information**, such as your name, surname, middle name, nickname, and any other

identification information you may choose to include in your CV and application form or on your social media pages, a copy of your ID or passport (which may also include additional details) if you accept an offer, in order for us to draft your employment agreement;

- **Contact details**, such as your personal phone number, your personal email address, your home address, your current and/or previous country of residence;
- **Photo**, in case you decide to include it in your CV or social media pages;
- Your **signature** when you choose to sign your motivation letter;
- Your **professional information, social background and relationships** such as your CV, employment and education details, job title, current and previous positions, references, professional memberships and qualifications, diplomas, hobbies, background checks, and any information you may have rendered public on social media such as LinkedIn;
- **Financial information** such as your previous salary and your salary and bonus expectations;
- **E-mail, internet, computer, and mobile device(s) access and use monitoring details,** such as your IP address, your browser type and language, access logs;
- **Communication information** such as email exchanges, text messages, voice mail or recruitment management system notifications;
- **Professional evaluations and career assessment details,** such as results of psychometric and technical tests assessing your technical knowledge and/or your organizational and managerial skills, personality questionnaires, performance assessments, feedback;

Gen II will not request or collect any sensitive Personal Data (such as health or financial information) during the stage of recruitment. You may be requested to provide us with additional information regarding your criminal background and employment health-check where legally required, but this will only be the case once you have accepted an employment offer and signed an employment contract. Therefore, such processing of Personal Data will be governed by the Employee Privacy Statement which you will receive before signing your contract as part of the onboarding documents.

We strongly advise you against sharing any sensitive Personal Data at the stage of recruitment, whether via your CV, motivation letter or publicly available social media pages.

4) For which purposes is your Personal Data processed?

a. To assess your suitability to the position of your interest;
b. To match your remuneration expectations with our available budget;
c. To review your references ;
d. To prepare a job offer and the related contractual documentation;
e. To communicate with you for the purposes of recruitment and onboarding;
f. To manage our recruitment platforms, social media accounts and any IT tool/ software that is internally used for the documentation and handling of the recruitment process;
g. To comply with our legal and regulatory obligations (including but not limited to obligations on anti-money laundering, independence, fight against corruption or equality and diversity);
h. To communicate with public authorities where necessary;
i. To produce reports and statistics for our management;
j. To perform business improvements and related collection of feedback, conduct surveys and data analytics studies (with the aim to better understand the candidate experience and satisfaction);
k. To receive advice and support from our professional advisors where necessary (including lawyers, consultants, other service providers for archiving and security etc.).

With particular regard to the context of the technical assessments, the Personal Data collected are processed in order to assess the candidates' technical skills and organizational and managerial skills to determine the fit to the relevant department for which the candidate has applied to.

The test will be scored and used, together with the analysis of the resume, to help determine whether a candidate has the right profile to move ahead in the recruitment process. This decision will not be automated: after a preliminary human review of a candidate's resume by the recruiting team, every assessment will be sent out for the review of a member of the talent acquisition team before a decision is made. The assessment will not be shared with the relevant manager, the latter will have only the feedback from the recruiting team. To have further information on how your Personal Data will be processed by the collaborating vendor, please read their privacy policy here.

5) With whom do we share your Personal Data?

Your Personal Data, in the context of recruitment, may be shared with the following recipients:

a. Our internal departments, including HR, Finances, IT and our management;
b. Our service providers, such as software providers, cloud hosting providers, our recruitment platforms and social media pages, tools used to manage and document the recruitment process;
c. Governmental, judicial, social security and supervisory authorities where necessary;
d. Other members of the Gen II Group as necessary, for example in case of shared positions or for reporting purposes;
e. The recruitment agency with which you were initially in contact in order to keep them informed about the status of your application;
f. Our advisors (for legal, tax or other matters).

We shall make sure that adequate safeguards are in place to protect your Personal Data while at the same time complying with our legal and regulatory obligations. Further details regarding recipients of your Personal Data and the measures we have put in place can be obtained from us by contacting our Global Data Protection Officer at privacy@gen2fund.com.

6) For how long do we keep your Personal Data?

Gen II will keep your Personal Data for the entire duration of the recruitment process. If you are not hired, we will store your Personal Data for a period of 1 year from the data of last communication with you, unless you choose to maintain your information on our recruitment management systems with the aim to apply for a new opportunity at a later stage, in which case our retention period will be extended until the moment when you delete your account from our recruitment management systems. During this period your data may be re-used by Gen II in order to contact you for a new opportunity which may be of interest to you and initiate a new recruitment process to the extent you have agreed thereto. If you are hired, your Personal Data will be stored in your HR file during the duration of our employment relationship and for 10 years thereafter.

7) How do we secure 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:

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

8) What are your privacy rights?

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

You may 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.

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.

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

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 also have the right to data portability for information you provided to Gen II, 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.

We will respond to individual complaints and questions relating to privacy and will investigate and attempt to resolve all complaints. We will only be able to answer favorably to any of the above requests related to your rights 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 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.

9) 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 laws, please do not hesitate to contact us at:

Email address: privacy@gen2fund.com

Postal address:
Sensr Solutions (Canada), Inc.
Suite 2500, Park Place, 666 Burrard Street, Vancouver, BC V6C2X8, Canada
Attn: Global Data Protection Officer

Phone number:
604-757-1570

10) Amendment of this Privacy Statement

This Privacy Statement shall be made available to you when you apply for an open position at Gen II, on our online recruitment platforms. Gen II may amend this Privacy Statement from time to time to ensure that you are fully informed about all processing activities and our compliance with applicable data protection legislation. In case of material changes which take place during an active recruitment process, you will be notified of changes to this Privacy Statement by appropriate means.