Last update: February 14 2025

EUROPE STAFF PRIVACY STATEMENT
(Ireland, Jersey, Luxembourg, UK)

This staff privacy notice (the **Privacy Statement**) explains what personally identifiable information relating to you as an individual (your **Personal Data**) we collect, store, and in general process about you in the context of your working relationship with Gen II. It also informs you what we use your Personal Data for and who we may share it with, as well as your rights in relation to your Personal Data and whom you can contact for more information or in case you have any queries.

If you are a candidate seeking employment at Gen II please instead refer to our candidate privacy statement here.

Any reference to:

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

"**Gen II"** or "**the Employer"** or "**we"** refer to the Gen II legal entity that has a contractual relationship with you (e.g. a contract of employment, an internship agreement, a secondment agreement or a consultancy agreement) which shall act as a Controller /Data Controller (within the meaning given to those terms in applicable data protection/ privacy 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 work 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
Ireland	Gen II Fund Services (Ireland) Limited	Suite 101-103, 16 Fitzwilliam Place, Dublin 2, Ireland, D02 FF82

Any Personal Data provided to or collected by the Employer will be processed (i.e. collected, used, stored, transmitted, etc.) in accordance with this Privacy Statement by (i) the Employer, in its capacity as Data Controller, or (ii) by the Employer's subcontractors and service providers as further described in this Privacy Statement in their capacity as Data Processors.

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

If you have any questions or requests, you may contact the Employer's **Global Data Protection Officer at privacy@gen2fund.lu .**

1. What Personal Data do we collect and process?

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

We may also collect Personal Data about you **indirectly**, through public sources or legally accessible databases, as described below, used by our HR and Compliance Department to perform their activities, or via your manager in the context of your performance reviews or general feedback, or because you are using IT tools and applications made available by Gen II to its employees or you are present in the Gen II premises where CCTV and badge readers are installed. In some cases, Gen II may collect Personal Data about you from third parties, such as references supplied by former employers, information from employment background check providers or information from credit reference agencies.

We primarily collect **your** Personal Data, however, due to our legal and regulatory obligations, as well as internal policies and procedures, we may also collect Personal Data of **your relatives and next of kin**, spouse or equivalent, or children. See more information below.

We are committed to protecting the privacy of all Personal Data you share with us in an open and transparent manner.

The categories of Personal Data we process include:

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

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

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

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

Your **professional, family, and social background 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, marital status, household composition, insurance affiliation;

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

E-mail, internet, computer and mobile device(s) access and use monitoring details, such as your IP address, your browser type and language, access logs (including account name, access times, wifi and websites use and monitoring thereof) or data in relation to communications including communications sent or received on any professional devices (such as frequency, volume, etc.), and/or personal devices, to the extent allowed by applicable law when you are using such devices for business purposes, and communications we send you regarding our events and services, details of how you interact with the provided IT tools and applications, devices used and other similar information;

Communication information, such as recordings of meetings and instant messaging conversations, SMS, voice mail;

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

Professional evaluations and career assessment details, such as results of personality questionnaires, performance assessments, feedback, disciplinary, grievance or capability reports and proceedings;

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

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

Vehicle details, such as company car license plate number;

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

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

Medical information, such as your health certificates and sickness records, short-term or long-term disabilities: we strongly recommend you to limit the information you are providing us with to the strict legal minimum;

Trade Union information, when such is shared by you in the context of the staff delegation elections and operations;

Background information provided by you, such as your criminal record extract, or collected from open data, legally available databases or public records as part of our ongoing risk management processes to the extent legally permitted.

Regarding Personal Data of your relatives and next of kin, please note that we may collect and process their identification information (such as name, surname, age, date of birth, gender), contact details (such as email address, home or professional address, country of residence), your relationship with

them, copies of their national identity cards or passports (in case you request us to assist with obtaining residence permits), health certificates (when filing for child sickness leave) or photos (in case they are participating in an event organized by Gen II in which case we will seek your consent, especially for minors).

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

We understand the importance of protecting children's privacy. It is not our policy to intentionally collect, store or in general process Personal Data pertaining to minors, with the exception of their name, surname, social security number and date of birth solely for the purpose of granting you with leave in relation to your children such as sickness leave, maternity and parental leave, or for making available any medical or other benefits to which you may be contractually entitles in the course of your working for Gen II. If we need to process Personal Data pertaining to minors in the context of events organized by the Employer, you shall be separately informed as necessary.

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

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

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

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

b) Processing necessary for compliance with legal obligations

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

- Our obligations related to anti-money laundering laws, fight against corruption, health and security at work, whistleblowing, work ethics, risk management which may also result in monitoring at the place of work;
- Our legal duties as an employer, including processing for social security, tax or accounting purposes, election of a staff delegation, maintenance of adequate reporting. Pursuant to applicable laws and regulations, the Employer may also need to disclose your Personal Data to government bodies or judicial authorities, as well as to tax administrations, social security, supervisory or other competent authorities;
- Our professional duties as a regulated company of the financial sector and any obligations deriving from the circulars or guidance issued by the CSSF as a supervisory authority. Our legal obligation to ensure security and safety of our assets and employees;
- Our privacy and data protection obligations to ensure response to the exercise of privacy rights and to personal data breaches and incidents.

Your sensitive Personal Data will be used for the following limited purposes:

- To ascertain your fitness to work (medical checks required under Luxembourg labor law);
- To record and manage sickness absences as required under Luxembourg laws or to justify a change in your current job position;
- To comply with our health and safety obligations;
- To ensure the honorability of our employees and prevent fraud.

c) Processing necessary to protect your vital interests

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

d) Processing necessary for purposes that are in the Employer's legitimate interest

We will process your Personal Data in order to pursue our legitimate interest both for our own internal purposes as well as for business purposes. This includes the following:

- To ensure reliable service provision to our customers or by our suppliers. This includes, without limitation, providing customers, suppliers and other providers with your contact information, professional qualifications and experiences, as required in the ordinary course of business;
- To showcase our heads of departments and specialists on our website and social media in order to demonstrate their talents and capabilities to current and prospective clients and general audience;
- To ensure proper personnel management, for example, payroll administration, compensation benefits, leaves and other absences administration, provision of benefits, management of work spaces;
- To manage recruitment, either directly (including via publicly availably platforms) or indirectly via referrals, or via recruitment agencies, and onboarding of new employees;
- To perform performance reviews and manage promotions or feedback, disciplinary, grievance or capability reports and proceedings;
- To organize business travels and administer related expenses;
- To offer you trainings, education, coaching or other forms of career guidance, personal development, talent management;
- To organize and extend invitations to company events, team building activities, corporate social responsibility initiatives as well as social & sports committee initiatives;

- To exercise or defend legal claims or for obtaining legal advice;
- To perform business processes and internal management, including general management, work scheduling, worked time recording, implementation of business control, checking compliance with internal procedures and policies, archiving, insurance purposes, in the context of dispute resolution, etc. ;
- For verification purposes with banks and/or financial institutions, public administrations and/or independent authorities, attorneys, auditors in case you have signatory authority;
- In the context of mergers, acquisitions and divestments if necessary in order to manage such transactions;
- To protect our offices, IT infrastructure and (including monitoring your access and use of emails, instant messages, Internet, laptops, workstations, hard disks and shared folders on the servers) and to ensure the security of our network and information, in compliance with applicable data protection laws and regulations;). This may lead to monitoring with the aim to log activity or scan correspondence of any kind or documents transiting through your professional devices in accordance with internal policies and procedures to identify risks and take adequate mitigation measures in accordance with applicable law. The monitoring will be performed gradually. The Employer performs statistical controls on the basis of traffic and log data. It is only in case these controls reveal abuse, misuse, illegitimate or dangerous use of the IT infrastructure or when the Employer has valid reasons to believe that there may be an increased risk for data loss (such as when you may be leaving the company pursuant to termination or resignation) that the monitoring may be intensified and lead to your identification. The Employer will in principle not access your private correspondence. However, if the private nature is not clear or specifically indicated in the object (that is, when it has the appearance of a professional correspondence), the Employer may review it;
- To secure our premises and prevent unauthorized people from entering the building or people accessing unauthorized areas;
- To ensure the security and safety of our assets (building, facilities, equipment, merchandise, cash, etc.) and employees, clients and visitors;
- To detect and identify potentially suspicious or dangerous behavior;
- To identify the origin of accidents or incidents;
- To organize and supervise a rapid evacuation of people from the premises in the event of an incident;
- To alert the emergency services, fire brigade or the police and facilitate their intervention in case of an incident and to request assistance in performing all of the above in case of an emergency by assigning the monitoring of suspicious activity to a third party;
- To protect its assets and for security purposes, the Employer may rely on video surveillance through which your image may be processed;
- To monitor your working hours and the attendance time of the employees, as well as to confirm your declared place of work in cases of teleworking;
- To ensure that there is a business continuity plan in place;
- To investigate and manage complaints and legal disputes involving you or other employees, including accidents at work or violations of internal policies, or involving our clients;
- To ensure and enhance the employee productivity and adherence to the Employer’s policies and procedures;

- To improve our business and to collect feedback, conduct staff surveys and data analytics studies (among other things to review and better understand employee satisfaction and turnover);
- To develop our business and activities, including marketing activities, client satisfaction and related follow-up;
- To collaborate with our professional advisors, such as lawyers, accountants, consultants, auditors and other service providers (such as but not limited to archiving, security, IT or printing services).

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

e) Processing based on your consent

Where, in exceptional circumstances we have requested and you have given your consent for the processing of Personal Data, such consent will serve as a legal basis for such processing. You have the right to withdraw your consent at any time as per applicable internal policies and procedures. The withdrawal of your consent shall not affect the lawfulness of processing based on consent before its withdrawal.

3. Who do we disclose your data to?

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

- The management of Gen II as well as any affiliates of the Gen II Group for staff administration purposes;
- Our department heads, as well as respective shareholders, agents, employees, consultants, representatives, financial intermediaries, auditors;
- Third parties that provide services to us such as IT suppliers (including forensic specialists), cloud-hosted applications, payroll service providers, background check services, financial, tax or legal advisors or institutions or accountants appointed by the Employer, insurance companies or brokers, travel agencies, transportation companies, hotels, catering companies, lunch voucher provider, tele-surveillance providers, shipment/courier companies, car leasing companies, credit card companies, photographers etc. Such third-party providers shall process your Personal Data upon our instructions or based on their know-how and expertise but with the aim to provide you with a benefit or service;
- Our clients or prospective clients in the context of services provided or proposed by Gen II and to the extent required for the provision of these services by you as an employee;
- Governmental, judicial, social security and supervisory authorities (including the Luxembourg data protection agency, tax administrations, courts, regulators etc.) to the extent legally permitted or required;
- Third parties in the context of a sale of some or all of its business under strict confidentiality arrangements.

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

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

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

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

We will maintain your Personal Data in principle for the longest of the following periods: (i) as long as is required for the processing in question, (ii) as long as necessary to comply with our legal and regulatory obligations or (iii) the limitation periods for litigation.
Pursuant to our legal and regulatory obligations and subject to any amendments of the retention periods, the Employer will keep the following Personal Data for the periods described here below, unless you have explicitly consented to an extended retention period:

Description	**Retention Period - Luxembourg**	**Retention Period - Ireland, United Kingdom, and Jersey**
Excerpt of criminal records	1 month from receipt	10 years from end of employment
Employment agreement & Salary slips Information pertaining to your name, date of birth, tax registration number and address, recruitment data, reference checks, work permits.	10 years from the end of your employment agreement	10 years from the end of your employment agreement.
Employment fitness certificates	10 years from the date of the certificate	N/A
Payroll records (e.g. wages, time management sheets, tax and social security records)	10 years from the end of the year to which the records relate	10 years from the end of the year to which the records relates
Data relating to leaves administration	5 years from the expiry of the year during which contributions were paid for documents concerning the CNS / 10 years from the end of your employment agreement for other documents or entries on IT systems	3 years from end of absence period or 12 months from end of employment
Data relating to employee benefits	Sympass: During the employment relationship; Company cars, Electronic lunch vouchers, Insurance Scheme: 10 years from the closure of the financial year during which the benefit was issued; Tax declaration assistance: as long as the assistance	Benefit Information: Immediate from end of employment; Compensation and award statement: As superseded or end of employment;

	session is active and deleted once it is terminated; Donation initiatives: 12 months and deleted thereafter.	Death in Service Benefit Nomination Forms: Immediate from end of employment; Staff Pension Details: 100 years from date of birth.
Timesheets	3 years from the corresponding reference period	10 years from the end of the financial year
Data relating to initiatives of the Social and Sports Committee	5 years from collection	3 years from the date of the event
Staff delegation data	10 years from the end of mandate of the respective delegation	N/A
Log files	6 months from their creation	Security logs are kept for up to 13 months
Physical access monitoring (Badges)	100 days after the recording of access	365 days from last recording of access
Data resulting from video surveillance	8 days after the recordings unless the recording constitutes evidence in case of an incident, in which case it will be retained for as long as legally necessary	31 days from date of recording
Career assessments and evaluation	Performance management: For the duration of the employment relationship and 3 years thereafter; Disciplinary actions; Training and Development: For the duration of the employment relationship and 10 years thereafter;	Performance management: For the duration of the employment relationship and 12 months after the end of employment; Disciplinary actions: 12 months from the last action (outcome decision date) Training and development: For the duration of the employment relationship and 10 years thereafter.
Work Permits	For the duration of the employment relationship and 10 years.	For the duration of the employment relationship and 10 years thereafter.
Teleworking	10 years for the calendar of teleworkers as it can constitute a justification relating to tax obligations of the Company; and 6 months for the logs and any report created or email exchanged thereof unless it leads to litigation.	6 months for the logs and any report created or email exchanged thereof unless it leads to litigation.

5. Where do we transfer your Personal Data?

The Gen II Group of companies is currently located in Ireland, Jersey, Luxembourg, the UK and the USA but other third parties may be located outside of those jurisdictions.

For the purposes listed above, your Personal Data may be transferred to any of the afore-mentioned recipients and service providers in countries located in or outside of the European Economic Area (the **EEA**). Certain countries in which recipients and processors may be located and to which Personal Data may be transferred may not have the same level of protection of Personal Data as the one afforded in the EEA. In such cases, we will ensure that there are adequate safeguards in place to protect your Personal Data that comply with our legal obligations. For any questions pertaining to this section, you may contact our Global Data Protection Officer at privacy@gen2fund.lu .

6. Data Privacy Framework

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

Gen II collects, uses, discloses, and disposes of Human Resource data. The specific scope and purpose of the data processing under the DPF is described in detail under Section 1 and Section 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 3 of this privacy statement.

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

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

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

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

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

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

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

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

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

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

7. How do we protect your Personal Data?

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

- 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 the Employer or by a third party. In such a case, the Employer 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.
Your right to object is not subject to any particular formality.

c) Right to withdraw consent

Where in exceptional circumstances we have requested your consent to our use of your Personal Data, then you have the right to withdraw your consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
This also applies to any consent given before the coming into force of the EU General Data Protection Regulation on 25 May 2018. The withdrawal of consent shall only affect future processing.

d) Right to data portability

Where the processing of your Personal Data is based on consent or the execution of a contract with you, you also have the right to data portability for information that you provided to the Employer – i.e. 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

You can exercise your rights any time by contacting the Employer's Global Data Protection Officer, at the following address privacy@gen2fund.lu.
Should you wish to make a complaint about how the Employer processes your Personal Data, please make contact in the first instance at the email address indicated above; your request will be processed as soon as possible. This is without prejudice to your right to file a complaint with 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.

9. Amendment of this privacy statement

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