ECE European Prime Shopping Centre Funds

08.10. Data Protection

Version

Developed by:	Jennyfer Nündel	On Date: 20 December 2017

Last review by:	Marie Astrid Willems	On Date: 20 May 2022
Last approval by:	Board of Managers	On Date: 25 May 2022

Content

OBJECTIVE AND BACKGROUND

The board of managers of ECE Real Estate Partners S.à r.l. (the "**Board**" or the "**Manager**") has defined and endorsed the following Data Protection Policy in order to comply with obligations under EU Regulation 2016/679 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 (the "**GDPR**"), the Luxembourg law of 1 August 2018 concerning the organization of the CNPD (the Luxembourg data protection authority), the general data protection regime (the "**Data protection Act**") and any further rules as maybe implemented from time to time in the Grand Duchy of Luxembourg regarding the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

The aim of this policy is to formalize an internal procedure that will enable the protection of natural persons in relation to the processing of Personal Data (as defined below) in compliance with GDPR, regardless of whether the processing itself takes place within the European Union or abroad.
This policy applies to all processing steps of personal data of all the staff of the Manager which must be familiar with this policy and comply with its terms, as well as to the Manager's advisor and its staff, ECE Real Estate Partners G.m.b.H. and ECE Living G.m.b.H., with respect to data related to investors only, suppliers, marketing contacts and business partners of the Manager. Business partners or other third parties must take corresponding actions if they work with Personal Data at or on behalf of the Manager.

This policy supplements other policies relating to staff use of internet and email use and may be supplemented or amended by additional policies and guidelines from time to time.

Any new or modified policy will be circulated to the Manager's staff before being adopted.
Any of the Managers' staff is made available this policy at his/her date of entry. A standard declaration of commitment of the Managers' employees is available.

Data confidentiality is also outlined in specific documents of the IFM which are made available to the Managers' staff.

Visitors are informed on the website of the Manager by a privacy notice where the current version of this policy is shared as well.

Investors in the alternative investment funds ("**AIFs**") managed by the Manager are informed by way of the relevant AIF documentation (in particular in the subscription booklet) when subscribing to the relevant AIF of the Manager, and consent in this context to the processing of their Personal Data.

The Manager takes compliance with this policy very seriously.

Failure to comply puts both the staff and the Manager at risk.

1. DEFINITIONS

For the purposes of this policy, "**Personal Data**" means any information relating to an identified or identifiable natural person (a so-called "**Data Subject**"); such as investors, committee members, board members, shareholders, current and former employees, agency, contract and other staff, suppliers and marketing contacts. Personal Data, the Manager may gather may include

- individuals' contact details,
- addresses,
- Log-in data (such as User ID and passwords, browser history),
- educational background,
- financial and pay details,
- details of certificates and diplomas,
- education and skills,
- marital status, nationality, job title, and
- Curriculum Vitae.

While GDPR is protecting "personal data" of natural persons, data which concerns legal persons, including the name and the form of the legal person and the contact details of such legal person only, is not protected by GDPR. We have though taken a wider approach which includes personal data under GDPR, but also data in relation to legal persons in case that such information can lead to a natural person.

"**Sensitive Personal Data**", *i.e.,* Personal Data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences[1], or related proceedings shall not be collected by the Manager, unless specifically set forth herein or required by applicable law.

"**Controller**" means ECE Real Estate Partners S.à r.l., *i.e.* the legal person which determines the purposes and means of the processing of Personal Data.

[1] Any criminal record check which is justified by applicable law can be collected pursuant to this policy. The Manager will collect a criminal record excerpt from any new employee. In addition, employees who should be appointed on senior management level and/or as board members on the level of the Manager will need to submit to the CSSF documentation to prove their good repute which generally includes the submission of a criminal record excerpt.

"**Processor**" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller."**Consent**" of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her. Consent can be revoked at any time.

Adequate level of data protection means the transmission of personal data to countries outside the European Union or the
European Economic Area (EEA), i.e. in the so-called "third countries", is only
admissible to the extent that there is an adequate level of data protection in these countries. A data protection level is, as a matter of principle, adequate if it corresponds to the data protection concepts of the European legislation, i.e. if the core of the private sphere, as it is unanimously understood in the Member States of the European Union, is protected. Whether a third country has an adequate level of data protection, is decided by the EU Commission. So far, the European Commission has confirmed an adequate level of data protection for the following countries: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Switzerland, Uruguay and lastly New Zealand.

Data subject means a data subject within the meaning of this Global Privacy Policy which is every natural person whose personal data are collected, processed and/or used. Apart from employees (including trainees, applicants, external employees) and customers, natural persons are protected who stand behind legal entities and/or business partnerships if the information about the community of persons also refers to them or could impact them (single shareholder company or sole proprietorship) or also our contact partners at our business partners.

Transfer of data means their transmission to a third party (= other controller).
The controller may pass on personal data to third parties or the third party may consult or retrieve data made available for that purpose. There is no transfer of data if the data are not passed on to a third party but to the data subject, a contractor (= contract data processor) or persons or bodies on the level of the controller.

2. RESPONSIBILITIES

The Board has decided that no data protection officer shall be appointed under Section 4 of GDPR and has decided that the below tasks shall be assigned to the following persons:

Advice training and awareness

The Compliance Officer shall inform and advise the Controller and its staff about applicable data protection provisions, including awareness-raising and training of staff. All employees of the Manager must be trained in “Data protection law” and must participate in corresponding measures. The relevant “Data protection law” presentation is shared with the employees of the Manager.

Policy Compliance

The Compliance Officer shall monitor compliance with this policy and shall conduct the related audits.

Point of Contact

The Compliance Officer shall answer questions on data protection from investors, staff, board members and other stakeholders, as well as responding to individuals such as employees who wish to know which data is being held on them by the Manager.

Data related risk assessments

The Risk Manager shall provide advice (where requested) as regards the data protection impact assessment and monitor its performance pursuant to Article 35 of GDPR, as well as any other risk assessment.

Communication with authorities

The Board shall be responsible for the communication and the cooperation with the competent supervisory authority; Mr. José María Ortiz shall act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 of GDPR, and to consult, where appropriate, with regard to any other matter.

Communication with Processors

The communication to Processors will be shared between the staff of the Manager. The Compliance Officer will keep a list of the relevant person (each a “**Main Contact Person**”) and Processor. The responsibilities of the Main Contact Person shall include the duty to provide this policy to the relevant Processor.

In addition, the Main Contact Person shall approach the relevant Processor and inquire information regarding (1) the collected / processed data; (2) the data protection level; (3) the countries into which the data is processed and (4) the relevant person in charge of data protection. The Main Contact Person shall then inform the Compliance Officer accordingly who shall then keep a list of the above-mentioned information.

In case that a Data Subject requires information about its Personal Data or in case that Personal Data should need to be rectified or deleted, the Compliance Officer will contact the Main Contact Person, who shall then inform the Processor, accordingly. In case that Personal Data should need to be rectified or deleted, the Main Contact Person shall ask for a confirmation of data rectification / deletion.
Any Processor shall be bound to respond to an inquiry of the Manager within one (1) month after receipt of the inquiry.

Finally, the Main Contact Person shall at least on an annual basis verify the compliance with this policy and report the results to the Compliance Officer who shall then report to the Board.

In case that the Main Contact Person should be in any doubt regarding the compliance with this policy or the inaccurateness of collected data, he or she shall contact the Compliance Officer and the Risk Manager.

Commissioned processing
If a company is awarded a contract to process Personal Data and processes these data in accordance with the instructions of the Manager, there is, as a rule, a case of commissioned processing (e.g. storage of data, execution of marketing activities, printing/mailing of payroll data etc.). In these
case, the Manager remains responsible for the admissibility of data processing by the contractor: the data remain data of the Manager and may not be used for own purposes by the contractor. In these cases, it is necessary to enter into a contract for the provision of services and into a so-called commissioned processing agreement which legitimates the transfer of the data.
The commissioned processing agreement requires the written form (template agreement is available upon request). It regulates, amongst other things, the instruction authority of the Manager as a principal concerning the way in which the Personal Data etc. are to be processed, the data category, the data processing services, the purposes of processing etc.
and the necessary technical and organizational measures for the privacy of these data.

Transfer outside the EEA

There are restrictions on international transfers of Personal Data. No data may be transferred outside of the EEA without first discussing it with the Compliance Officer. Specific Consent from the Data Subject must be obtained prior to transferring their data outside the EEA.

Any transfer of Personal Data anywhere outside the Grand Duchy of Luxembourg and Germany must be approved by the Board, unless the standard data protection clause set forth in Annex 1 and 2 is adhered to in writing.

3. PRINCIPLES

The Board agrees that the following **Main Data Principles** shall apply:

THE PRINCIPLE OF TRANSPARENCY	Personal Data shall only be collected in a fair and lawful manner in accordance with this policy and GDPR. This generally means that Personal Data shall not be collected or processed unless the Data Subject given its Consent or the following Legitimate Purpose Test is fulfilled.
THE LEGITIMATE PURPOSE TEST	Personal Data shall only be collected for specified, explicit and legitimate purpose and cannot be further processed in a manner that is incompatible with these purposes. The Consent of a Data Subject shall be the preferred purpose, but other accepted specified, explicit and legitimate purposes are as follows: (1) Mutual agreement (2) Legal obligation, or (3) The legitimate interest of the Controller.
PRINCIPLE OF MINIMISATION	Personal Data shall only be processed when strictly necessary to achieve the specified, explicit and legitimate purpose.
PRINCIPLE OF ACCURACY	Personal Data shall be collected accurately and, where necessary, kept up to date; Personal Data that are inaccurate shall be erased or rectified without delay.
PRINCIPLE OF STORAGE LIMITATION	Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed.
PRINCIPLE OF INTEGRITY AND CONFIDENTIALITY	The Manager shall keep Personal Data secure against loss or misuse. Where Processors process Personal Data as a service on the Manager's behalf, the Board will establish what, if any, additional specific data security arrangements need to be implemented in agreements with those Processors. The Manager shall therefore check at least on an annual basis the IT security of its server(s).
THE PRINCIPLE OF ACCOUNTABILITY	The Controller shall demonstrate to be responsible for, and be able to demonstrate compliance with the above Main Data Principles. The Controller shall therefore undertake a special data audit to manage and mitigate risks.

4. SHARING PERSONAL DATA

The Board notes that it is necessary to share Personal Data with Processors and other third parties in the financial environment. The transfer of data to third parties requires, as a matter of principle, a legal basis, i.e. it must for instance be necessary for the purpose of fulfilment of the employment relationship or the performance of a contract with an investor. The Board notes that it is its responsibility to ensure that Personal Data is shared in a secure manner and in compliance with this policy. It notes that Personal Data is shared in particular with:

- Processors (such as depositaries, auditors, advisors, transfer agents etc.)
- HR providers
- Payroll providers
- Social Services
- Recruitment agencies
- Banks
- Pension providers
- Tax, government and any relevant regulatory authorities, such as the CSSF
- Prosecuting authorities and courts, and/or other relevant third parties connected with legal proceedings or claims
- Third parties where the Manager is required to do so by law
- External accountants, and
- Occupational health providers

It is not allowed to process data to a person or a country outside of the EEA which has not been validated by the Board. This does not concern data which are manifestly made public by the relevant Data Subject.

It is also not allowed to use Personal Data for direct marketing purposes, any such request shall be immediately notified to the Compliance Officer and the Risk Manager.

The Board notes that ECE Projektmanagement International G.m.b.H. is providing IT services to the Manager, the Manager relies on the security description as provided by its service provider while ECE Projektmanagement International G.m.b.H. has not yet been subject to an external audit.

5. PRIVACY BY DESIGN AND DEFAULT & STORING DATA SECURELY

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Board will be responsible for ensuring that all new data security processes and IT projects commence with a privacy plan and that ongoing projects are reviewed in a timely manner.

When relevant, and when it does not have a negative impact on the Data Subject, privacy settings will be set to the most private by default.

As a matter of principle, all Personal Data must be protected against loss, manipulation but also unauthorized consultation. Requirements for data protection exist, more particularly, for automated data processing (e.g. physical access, data access, entry, transmission control). By way of a measure which is to ensure appropriate privacy, the Manager / its staff shall follow the below guidelines to comply with the standards on security and privacy:

- Avoid any abuse of your userame;

- Use safe password and do not disclose them under any circumstances;

- In cases when data is stored on printed paper, staff shall ensure that it is kept in a secure place where unauthorised personnel cannot access it;

- Printed data shall be shredded in the confidential waste bins of the Manager when it is no longer needed;

- Staff shall use secure remote access software for accessing the IT system from another location as foreseen in Section 3.2 of the Manager's current Information Technology procedure;

- The Manager ensures that all network users have individual logins via its commissioned service provider, ECE Projektmanagement International G.m.b.H. as outlined in its current Information Technology procedure.The staff shall not share usernames or passwords, unless permitted by exceptional circumstances which shall be disclosed to the Manager by the relevant staff;

- The Manager ensures that passwords must be adequately complex and changed periodically via the password policy of its commissioned service provider, ECE Projektmanagement International G.m.b.H. as outlined in its current Information Technology procedure;

- Staff should lock away devices such as laptops, tablets and mobile phones when not in use;

- The Manager ensures that an antivirus and malware software is installed and kept up to date as well as operating systems on laptops, tablets and mobile phones via its commissioned service provider, ECE Projektmanagement International G.m.b.H. as outlined in its current Information Technology procedure;

- Mobile phones for professional use must be password protected and able to have their content accessed/deleted remotely as outlined in the current Manager's Information Technology procedure;

- Emails containing Personal Data should not be sent from staff personal accounts;

- Staff should be vigilant of emails with suspicious attachments from emails addresses which have similar name configurations hyperlinks and proceed cautiously either when alerted by the commissioned service provider, ECE Projektmanagement International G.m.b.H. or when suspicions are otherwise aroused.

- The Manager shall ensure that its staff completes a basic 'cyber security' training in relation to opening emails, scanning USBs, handling Personal Data etc.;

- The Manager shall ensure that its wireless network is password protected and encrypted, it shall also ensure that data stored on CDs or memory sticks is encrypted and locked away securely when not being used via the password policy of its commissioned service provider, ECE Projektmanagement International G.m.b.H. as outlined in its current Information Technology procedure;

- The Board must approve any new cloud used to store data and should review the service agreements with existing cloud servers in a timely manner;

- The Manager ensures that servers containing Personal Data are kept in a secure location or in the cloud, away from general office space and protected by a strong firewall via its commissioned service provider, ECE Projektmanagement International G.m.b.H. as outlined in its current Information Technology procedure;

- The Manager ensures that data is regularly backed up in line with the Manager's backup procedures as outlined in its current Information Technology procedure;

- Any staff must report loss of a device; laptop, mobile phone, tablet etc. immediately to the Compliance Officer and the Risk Manager who shall then inform the Board to the extent necessary and in line with internal procedures with respect to the loss of devices;

- The Manager shall also keep a record of third party access to data – e.g. payroll companies, pension providers etc.

6. DATA RETENTION PERIODS, DATA DELETION AND SAFE DESTRUCTION OF RECORDS

The Manager will retain Personal Data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the Personal Data was obtained, but if relevant, the length of retention will be determined in a manner consistent with published legal and regulatory data retention guidelines from time to time in place.

Unless otherwise required by applicable law, the Manager will normally keep Personal Data no longer than five (5) years after the end of a business relationship (the "**Minimum Retention Period**").

Disposal of records that have reached the end of the Minimum Retention Period should be deleted or archived in line with the below guidance.

A local review will determine whether records are to be selected for permanent preservation, destroyed, digitized to an electronic format or retained for litigation purposes.

Whatever decision is made, such decision needs to be documented as part of the records of the Manager.

All records containing Personal Data, or sensitive policy information should be made either unreadable or unreconstructable. In detail:

- Paper records should be shredded in the confidential waste bins of the Manager;
- CDs / DVDs / Floppy Disks should be cut into pieces;
- Audio / Video Tapes and Fax Rolls should be dismantled and shredded;

- Hard Disks should be dismantled and sanded;

The Manager shall try to impose on the external provider providing its confidential waste bins to train its staff in the handling of confidential documents. The shredding needs to be planned with specific dates and all records should be identified as to the date of destruction.

Where records have been identified as being worthy of permanent preservation arrangements should be made to transfer the records to an appropriate archive. Sample appendices are provided for the recording of all records to be used.

These records shall be kept in an excel spreadsheet or other database format.

7. POLICY RECORD KEEPING

To demonstrate compliance with GDPR, documentation relating to data processing activities shall be maintained.

In accordance with Article 30 GDPR the Manager as controller maintains a record of all processing activities under its responsibility.
The contents of the records of processing activities result from Article 30 Para 1 GDPR and include the following data:
● the name and contact details of the controller,
● the name and contact details of the representative of the controller,
● the name and contact details of a possible data protection officer,
● the purposes of the data processing,
● description of the categories of data subjects and personal data concerned.
● the recipients or categories of recipients with whom data can be shared,
● deadlines for the erasure of the data,
● planned data transfers to third countries as well as
● where possible, a general description of the technical and organisational measures

The Compliance Officer shall ensure (if legally required) that each Processor and, where applicable, the Processor's representative shall maintain a GDPR compliant record.

The records referred to above shall be in writing, including in electronic form.

8. RIGHTS OF THE DATA SUBJECT

The Board notes that the Manager is not processing data in an automatic way. It is thus acknowledged that the Manager will need to fulfill the following rights of Data Subjects:

1) Information to the Data Subject

   Being transparent and providing accessible information to Data Subjects and information about how the Manager will use Personal Data is important for the Manager. In case a Data Subject wishes that his/her information shall be treated confidentially, privacy notices can be found in the Annex 3 of this policy.

   The notice sets out the purposes for which Personal Data on Data Subjects is held by the Manager, highlights that the work of the Manager may require it to give information to third parties, and provides that each Data Subject has a right of access to the Personal Data that the Manager holds about them.

2) The right to restriction of processing

   The Data Subject shall have the right to obtain from the Controller restriction of processing if
   (a) the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the Controller to verify the accuracy of the Personal Data;
   (b) the processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead; or
   (c) the Controller no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims.

   Where the processing has been restricted, the data can no longer be processed. The method used to restrict the process may vary depending on the situation (e.g. temporary move to another file, locking of data temporary removal from a website, etc.).

3) The right of access

The Data Subject shall have access to a complete copy of the Personal Data relating to him / her. **NO CHARGES** should be made to the Data Subject. These requests should be processed within **ONE (1) MONTH**, provided there is no undue burden and it does not compromise the privacy of other Data Subjects.

4) The right to rectification

The Data Subject shall have the right to obtain from the Controller without undue delay the rectification of inaccurate personal data concerning him or her.
Taking into account the purposes of the processing, the Data Subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

For example, if an employee's personal circumstances change, please inform the Compliance Officer or the Risk Manager, so that they can update their records.

5) The right to be forgotten

Unless, a Legitimate Purpose requires otherwise, where a person no longer wishes for their Personal Data to be processed, the Controller must delete the data, and inform the relevant Processor accordingly who shall then in turn confirm deletion of the relevant data.

6) The right to data portability

The Data Subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance from the Controller to which the personal data have been provided.

9. NOTIFICATION

Staff should notify the Board or the Compliance Officer **immediately** if they are concerned about a possible data breach. If a breach is discovered outside of term time by a staff member, they should alert the Compliance Officer immediately.

Data breaches must be reported to the COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES (**CNPD**) within **72 hours**. If the breach is sufficiently serious to warrant notification to the public, the breach must be reported without undue delay.

If there is a high risk to the rights and freedoms of individuals, Data Subjects must be notified.

All members of staff have an obligation to report actual or potential data protection compliance failures.

This allows the Manager to (a) investigate the failure and take remedial steps if necessary; (b) maintain a register of compliance failures; and (c) notify the CNPD of any compliance failures that are material either in their own right or as part of a pattern of failures.

In case of a data breach the following checklist shall be followed:

1) Formation of a crisis management team (the "**CT**") which shall consist of the Risk Manager, Compliance Officer and Main Contact Person

2) The CT shall assess the level of risk of data breach – no risk/risk/high risk – if unaddressed such as breach is likely to have a significant detrimental effect on individuals /Data Subjects

3) The CT shall inform the CNPD within 72 hours and identify the key internal and external messaging for communications strategy and issue

4) The CT shall secure IT systems and stop additional data loss

5) The CT shall speak to those affected/involved: If there is a high risk to the rights and freedoms of individuals, data subjects must be notified.

6) The Board shall report to police when/if considered appropriate

7) The Board shall notify regulators/consult with legal team/insurer etc.

10. WHAT INFORMATION MUST A BREACH NOTIFICATION CONTAIN?

The Notification must contain:

(a) The nature of the personal data breach including, where possible:

(b) the categories and approximate number of individuals concerned;

(c) the categories and approximate number of personal data records concerned;

(d) the name and contact details of the data protection officer;
(e) a description of the likely consequences of the personal data breach; and
(f) a description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

11. APPROVAL OF THE BOARD

This policy was approved by the Board on 25 May 2022.

Annex 1 – STANDARD DATA PROTECTION CLAUSE (CONTROLLER)


Standard Clause I a.pdf


CELEX_32021D0914_EN_TXT_Standard contr


Standard Clause I.pdf

Annex 2 - STANDARD CONTRACTUAL CLAUSES (PROCESSORS)


Standard clause II.pdf

Annex 3 - **Privacy Notice (How we use employee information)**

Why do we collect and use employee information?

We collect and use employee information under section 6(1)(b) of the GDPR which states '*Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract'*. We use employee data:

- to carry out required legal background checks
- to ensure employees receive their salary and pension contributions
- to monitor and review performance
- to ensure employees have a right to work in the Grand Duchy of Luxembourg
- to monitor sickness and absence levels
- enabling a comprehensive picture of the workforce
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring

The categories of employee information that we collect, hold and share include:

- Personal information (such as name and address)
- Financial information (such as bank account data, National Insurance number, tax code)
- Characteristics (such as ethnicity, language, nationality, country of birth)
- Sickness and absence information
- Relevant medical information

Collecting employee information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the GDPR, we will inform you whether you are required to provide certain information to us or if you have a choice in this.

Storing data

We hold data for the period of time as set out by our data retention guidance in accordance with applicable law which is normally a maximum of five (5) years after the end of our professional relationship.

Who do we share employee information with?

We routinely share employee information with:

Pensions authorities,
Payroll companies,
Insurance companies
Our shareholders,
Accountants,
Auditors

Why we share employee information
We do not share information about our employees with anyone without consent unless the law and our policies allow us to do so.

Requesting access to your personal data

Under data protection legislation, employees have the right to request access to information about them that we hold.

To make a request for your personal information, please contact Ferman Ciftci, Compliance Officer.

We respectfully request that you request information during term time to give us the best opportunity to comply with your request within one calendar month although you are under no legal obligation to do so.

You also have the right to:

1) object to processing of personal data that is likely to cause, or is causing, damage or distress
2) prevent processing for the purpose of direct marketing
3) object to decisions being taken by automated means
4) in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
5) claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the CNPD under https://cnpd.public.lu/fr.html

Contact:

If you would like to discuss anything in this privacy notice, please contact

Ferman Ciftci,
Compliance Officer,
Ferman.ciftci@ece.com

Annex 3: **Privacy Notice (How we use investor information)**

Which data is concerned?

While GDPR is protecting “personal data” of natural persons, data which concerns legal persons, including the name and the form of the legal person and the contact details of such legal person only, is not protected by GDPR. We have though taken a wider approach and protect “investor information” which includes personal data under GDPR, but also data in relation to legal persons in case that such information can lead to a natural person.

Why do we collect and use investor information?

We collect and use investor information under section 6(1)(b) of the GDPR and section 6(1)(c) which state '*Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract*' and '*Processing is necessary for compliance with a legal obligation to which the controller is subject'*.
We use investor data:

- to carry out required legal background checks
- to ensure investors receive their distributions
- to monitor and review performance
- allowing better financial modelling and planning
- to identify the investor
- to monitor and report on investment progress
- to provide appropriate investor care
- to assess the quality of our services
- to comply with our obligation under the limited partnership agreement, as well as the subscription agreement;
- to comply with our KYC obligation
- to comply with regulatory requirements due to our status as fully-regulated alternative investment fund manager
- to ensure investors receive their distributions
- to monitor and report on the investment progress
- to comply with our duties under the applicable laws and regulations
- to comply with our duties regarding research and statistics

The categories of investor information that we collect, hold and share include:

- Personal information (such as name and address of board members, committee members and shareholders, as well as relevant staff of relevant service providers)
- Financial information (such as bank account data, tax code)
- Characteristics (nationality, country and date of birth of board members shareholders, staff of relevant service providers).

Collecting investor information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the GDPR, we will inform you whether you are required to provide certain information to us or if you have a choice in this.

Storing data

We hold data for the period of time as set out by our data retention guidance in accordance with applicable law which is normally a maximum of five (5) years after the end of our professional relationship.

Who do we share investor information with?

We routinely share investor information with:

- General Partner;
- Depositaries;
- Transfer and registrar agents;
- Advisors;
- Accountants;
- Auditors;
- Local regulatory and tax authorities;
- Shareholders (to the extent required to be disclosed in the financial statements);
- Legal and tax counsels;
- International authorities or bodies, to the extent competent.

Why we share investor information

We do not share information about our investors with anyone without consent which is usually given by entry into the subscription form, unless the law and our policies allow us to do so.

Requesting access to your personal data

Under data protection legislation, investors have the right to request access to information about them that we hold. To make a request for your personal information contact Ferman Ciftci, Compliance Officer.

We respectfully request that you request information during term time to give us the best opportunity to comply with your request within one calendar month although you are under no legal obligation to do so.

You also have the right to:

1) object to processing of personal data that is likely to cause, or is causing, damage or distress
2) prevent processing for the purpose of direct marketing
3) object to decisions being taken by automated means
4) in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
5) claim compensation for damages caused by a breach of the data protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the CNPD under https://cnpd.public.lu/fr.html

Contact:

If you would like to discuss anything in this privacy notice, please contact

Ferman Ciftci
Compliance Officer
Ferman.ciftci@ece.com