

Version

Developed by:	Compliance Officer	On Date: 20 December 2017
Last review by:	Compliance Officer	On Date: September 2023
Last approval by:	Board of Managers	On Date: 24 October 2023

Contents

OBJECTIVE AND BACKGROUND2

1. DEFINITIONS.....4

2. GOVERNANCE, ROLES AND RESPONSIBILITIES.....6

3. PRINCIPLES11

4. SHARING PERSONAL DATA.....14

5. PRIVACY BY DESIGN AND DEFAULT & STORING DATA SECURELY14

6. DATA RETENTION16

7. RECORD OF PROCESSING ACTIVITIES20

8. LAWFUL PROCESSING OF PERSONAL DATA.....22

9. DATA BREACH26

10. WHAT INFORMATION MUST A BREACH NOTIFICATION CONTAIN?.....27

11. DATA PROTECTION IMPACT ASSESSMENT27

12. THIRD PARTY MANAGEMENT AND OUTSOURCING30

13. POTENTIAL SCENARIOS.....30

14. PRIVACY ROLE IDENTIFICATION, ASSESSMENT AND AGREEMENT33

15. TRANSFER OF PERSONAL DATA TO THIRD PARTIES AND NON-EU COUNTRIES35

16. DISCIPLINARY PROCEDURE FOR ANY VIOLATION OF THIS POLICY36

17. ANNEXES37

OBJECTIVE AND BACKGROUND

The board of managers (the “Board” or “Board of Managers”) of ECE Real Estate Partners S.à r.l. (the “Company” or the “AIFM” or the “Manager”) has defined and endorsed the present policy (the “Data Protection Policy” or the “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 may be 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 “Privacy Legal Framework”).

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 Employees of the Manager which must be familiar with this Policy and comply with its terms, 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 Employees 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 employees before being adopted.

Any of the Managers’ Employees 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 AIFM which are made available to the Managers’ Employees.

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 agreement and subscription booklet) when subscribing to the relevant AIF under the management 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 Employees and the Manager at risk.

This Policy shall be updated upon any amendment in the legislation, or on the discretion of the Privacy Champion or Board of Managers.

1. DEFINITIONS

For the purposes of this policy, “**Personal Data**” or “**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 employees, suppliers and marketing contacts. Personal Data, the Manager may gather may include (non-exhaustive list):

- ID card and / or passport copies;
- 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.

“**Board**” means the Board of Managers of the AIFM.

“**CNPD**” means the Commission Nationale pour la Protection des Données.

“**Counterparty**” means the entities or subject involved in relevant data processing activities, as further detailed in Chapter 11 below.

“**Controller**” or “**Data 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.

“**DPO**” means the Data Protection Officer.

“**DPA**” means the Data Protection Agreement under article 28 of GDPR.



“**DPIA**” means the Data Protection Impact Assessment.

“**EC**” means the European Commission.

“**Employee**” or “**Employees**” means any employee, employees member or secondee of the AIFM, including job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors.

“**GDPR**” means the Regulation (EU) 2016/679 of the European Parliament and of 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, and repealing Directive 95/46/EC, as amended.

“**Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, as further detailed in Chapter 9.

“**Policy**” means the present Privacy and Data Protection Policy and Procedure addressing the main GDPR topics and setting the data protection framework of the AIFM.

“**Processor**” or “**Data 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.

“**Privacy Champion**” means the AIFM stakeholder acting as main privacy and data protection point of contact of the AIFM, as further detailed in Chapter 2.

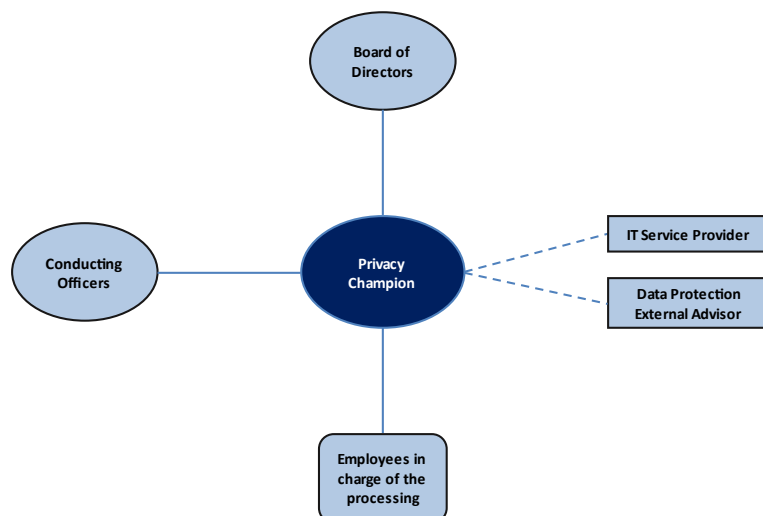
“**SCCs**” means the standard data protection clauses.

“**Adequacy Decision**” means a formal decision made by the EC which recognises that another country, territory, sector or international organisation provides an equivalent level of protection for Personal Data as the EU does, as further detailed in Chapter 12 below.

“**Transfer**” of data means their transmission to a third party. 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.

“**Special Categories of 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 offences¹, or related proceedings shall not be collected by the Manager, unless specifically set forth herein or required by applicable law.

2. GOVERNANCE, ROLES AND RESPONSIBILITIES



Privacy Champion

The AIFM appointed a Privacy Champion - namely the Compliance Officer - acting as the main privacy and data protection point of contact, responsible for providing advice on data protection, as well as monitoring compliance with the Privacy Legal Framework within the Company, under the supervision and responsibility of the Board.

The Privacy Champion is appointed on the basis of his professional qualities and abilities, such as the specialist knowledge of regulatory compliance topics and the organizational structure of the Company. The Privacy Champion must be promptly and adequately involved in all matters concerning the protection of Personal Data and must directly report to the Board.

In particular, the Privacy Champion's duties consist of:

- Monitoring compliance with the current Policy, as well as the Privacy Legal Framework, assessing the risks of each processing activity in the light of the nature, scope, context and purposes;
- Answer questions on data protection from investors, Employees, 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;
- Informing the AIFM and raising awareness on the obligations deriving from the Privacy Legal Framework;
- Providing consultancy to the AIFM regarding the Privacy Legal Framework and related activities;
- Together with the Risk Manager, participating in the DPIAs;
- Collaborating in the assessment of privacy related risks and the measures for the reduction of such risks, starting from the design phase of a new processing activity (privacy by design);
- Supporting the AIFM in evaluating events that might constitute a Data Breach and the consequent need to notify the CNPD and/or the Data Subjects;
- Proposing to the AIFM the privacy areas on which to carry out audit or compliance checks;
- Verifying the implementation status and the effectiveness of the organizational and technological security measures;
- Analyzing the documentation under the Privacy Legal Framework;
- Providing guidelines and instructions for the definition corporate training programs on privacy matters at least on a yearly basis, for the purpose of disseminating an adequate culture and awareness in this area;

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.

- Supporting the Board in handling feedback to the CNPD and to the Data Subjects following appeals, reports or complaints; Mr. José María Ortiz shall act as the contact point for the supervisory authorities 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.

Reference should be done to Annex 3 for further information on the assessment performed to support the decision of the Board, for the time being, not to designate a Data Protection Officer (“DPO”) but, rather, a Privacy Champion.

In order to fulfil its role, every Employee in charge of the processing is required to always include the Privacy Champion in any communication in which personal data is processed. This is to ensure that the Privacy Champion as the central person is aware of all data processing activities and then lists them in the register of data processing.

Conducting Officers

All the Conducting Officers, under the guidance of the Privacy Champion, are responsible for the compliance with the Privacy Legal Framework within the Company.

In particular, they support the Privacy Champion in the performance of his duties, such as, among others:

- Raising awareness and advising the Employees regarding the obligations arising from the Privacy Legal Framework;
- Cooperating with the Privacy Champion to facilitate access by the latter to the information required for the performance of his duties;
- Supporting the Privacy Champion in carrying out his activities within the AIFM, promptly bringing Personal Data protection matters considered particularly relevant to the Privacy Champion’s attention (e.g., Data Subject complaints or breaches of the Privacy Legal Framework);
- For each data processing activity, to inform the Privacy Champion in relation to this, so that no data processing activity is carried out without the Privacy Champion being involved;

- Promptly reporting to the Privacy Champion events that may lead to Data Breaches, providing all the contextual elements conducive to the risk assessments for Data Subjects and the need for reporting.

Employees in charge of the processing

All Employees, regardless of their function, classification or level, and more generally those who carry out processing activities on behalf of the AIFM, are in charge of processing Personal Data relating to and/or in any case connected to the functions and work assigned to them by the AIFM.

Employees are required to duly cooperate with the Privacy Champion with regard to all privacy and data protection requirements, especially those mentioned within this Policy. In case of any doubt, prompt escalation to the Privacy Champion should be performed.

All the Employees are required to confirm that they have read and will adhere to all the obligations outlined in this Policy.

When establishing a new business relationship, Employees shall provide the applicable information notice (please refer to Chapter 8 below), verify the privacy role of the Counterparty (e.g., Data Controller, Data Processor, Joint Controller and negotiate relevant privacy agreements (e.g., data processing agreement, joint controller agreement, please refer to Chapter 11 below) with the assistance and under the supervision of the Privacy Champion.

Where applicable, Employees, with the assistance of the Privacy Champion, will also verify through initial and ongoing due diligence, that such a contracting party has in place appropriate policies, procedures, technical, organizational and security measures under the Privacy Legal Framework (please refer to Chapter 11 below).

In case Personal Data are transferred outside the Economic European Area (please refer to Chapter 12 below), Employees are required to escalate to the Privacy Champion for analysis and authorization of the relevant processing of Personal Data.

Should the Employees detect a processing activity potentially representing a high risk to the rights and freedoms of Data Subjects, the processing at issue shall not be commenced or continued and prompt escalation to the Privacy Champion shall be performed (please refer to Chapter 10 below).



Should the Employees suspect that a Data Breach may have occurred or that a Data Breach took place (please refer to Chapter 9 below), immediate escalation to the Privacy Champion shall be performed.

For each data processing activity, to inform the Privacy Champion in relation to this, so that no data processing activity is carried out without the Privacy Champion being involved.

In addition, all the Employees are requested to collaborate with the Privacy Champions to keep the Record duly updated (please refer to Chapter 7 below), as well as to ensure the effective erasure (or anonymization, where previously authorized) of Personal Data under the applicable retention periods (please refer to Chapter 6 below).


A central obligation for all Employees is also the strict adherence to the confidentiality of all Company information and any information concerning the Company. Accordingly, all Employees are not authorized to process any Company information in any way, unless the Board of Managers have expressly approved it. It is emphasized here that information is meant not solely meant as Personal Data but also any kind of information that might be related to the Company. A breach with this obligation leads to consequences for the respective Employee.

Support from IT service provider and external advisor

To ensure the provision of the resources necessary to carry out relevant activities under the Privacy Legal Framework, the AIFM makes available to the Privacy Champion the support of IT Service Provider(s) and Data Protection External Advisor(s), if needed.

In this context, it is noted that the annual trainings for the purpose of applying all relevant requirements are carried out by external advisors. At the discretion of the Privacy Champion or the Board of Managers, further training for Employees may be scheduled by the Privacy Champion.

Board of Managers

ECE Real Estate Partners S.à. r.l.	
08.10. Privacy and Data Protection Policy and Procedure	

3. PRINCIPLES

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

<p>THE PRINCIPLE OF TRANSPARENCY</p>	<p>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.</p>
<p>THE LEGITIMATE PURPOSE TEST</p>	<p>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:</p> <ol style="list-style-type: none"> (1) Mutual agreement (2) Legal obligation, or (3) The legitimate interest of the Controller.
<p>PRINCIPLE OF MINIMISATION</p>	<p>Personal Data shall only be processed when strictly necessary to achieve the specified, explicit and legitimate purpose.</p>
<p>PRINCIPLE OF ACCURACY</p>	<p>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.</p>
<p>PRINCIPLE OF STORAGE LIMITATION</p>	<p>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.</p>
<p>PRINCIPLE OF INTEGRITY AND CONFIDENTIALITY</p>	<p>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).</p>



**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 (if applicable)
- 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 Privacy Champion and the Risk Manager.

The Board notes that ECE Group GmbH & Co. KG is providing IT services to the Manager, the Manager relies on the security description as provided by its service provider while ECE Group GmbH & Co. KG 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 Employees shall follow the below guidelines to comply with the standards on security and privacy:

- Avoid any abuse of your username;
- Use safe password and do not disclose them under any circumstances;
- In cases when data is stored on printed paper, Employees 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;
- Employees 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 Group GmbH & Co. KG as outlined in its current Information Technology procedure. The Employees shall not share usernames or passwords, unless permitted by exceptional circumstances which shall be disclosed to the Manager by the relevant Employees;
- The Manager ensures that passwords must be adequately complex and changed periodically via the password policy of its commissioned service provider, ECE Group GmbH & Co. KG as outlined in its current Information Technology procedure;
- Employees 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 Group GmbH & Co. KG 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 Employees personal accounts;
- Employees 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 Group GmbH & Co. KG or when suspicions are otherwise aroused.
- The Manager shall ensure that its Employees completes a basic annual 'cyber security' training in relation to opening emails, , confidential data, handling of Personal Data etc.;
- The Manager shall ensure that its wireless network is password protected and encrypted, it shall also ensure that no data is stored on CDs or memory sticks, except for marketing purposes, in which case the data shall be encrypted and locked away securely when not being used via the password policy of its commissioned service provider, ECE Group GmbH & Co. KG 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 Group GmbH & Co. KG 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 Employees must report loss of a device; laptop, mobile phone, tablet etc. immediately to the Privacy Champion 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

When it comes to data retention, we adhere to the principle of retaining Personal Data for no longer than necessary to fulfill the purposes for which it was collected, unless a longer retention period is required or permitted by the applicable laws.

Requirements The duration of data retention varies depending on the type of Personal Data and processing activities, based on the following principles:

- Legal Retention: The AIFM will comply with applicable laws when storing Data;
- Limited Retention: The AIFM will limit the historic retention of Data so as to only store documents strictly needed;
- Maintained Retention: The AIFM will ensure that Data are regularly and systematically destroyed at the end of the retention period as further detailed below;
- Safe Retention: The AIFM will store Data in accordance with its information technology policy and procedures;
- Justified Retention: The AIFM will only store Data beyond their retention period if it is justified to do so as further detailed in this Policy.

All Employees are responsible for ensuring they apply the requirements of this Policy and do not act in a way which is otherwise than in accordance with its terms. Under the supervision and support of the Privacy Champion, specific Employees's responsibilities include:

- Creating, receiving, and managing paper and electronic records as part of their daily work according to the practices established herein, as well as within the record of processing activities;
- Understanding how to use IT platforms and systems to properly archive, manage and delete documents as further detailed in the information technology policy and procedures;
- Evaluating and identifying paper and electronic records to determine their appropriate classification, storage and deletion, as detailed within as well as within the record of processing activities;
- Where required, cancel Data in accordance with the terms outlined in this Policy, as well as the record of processing activities.

To determine the appropriate retention period for Personal Data, we consider the nature and sensitivity of the information, the potential risk of harm from unauthorized use or disclosure, the purposes for which we process the data, and applicable legal requirements and guidelines from European authorities, such as, among others:

- Data used for direct marketing purposes (e.g., client's name, email address, social media account) shall be kept for no longer than 3 years (French data protection authority ('CNIL') Decision No. 2016-264 of 21 July 2016);
- Balance sheet, profit, and loss account, cash flow statements, official record of inspection of companies' account, are considered as supporting documents of the accounting and financial documents and therefore are prescribed for 10 years from the end of the fiscal year in which they relate (Articles 16 and 189 of the Code of Commerce);
- Data retention of Personal Data of Employees varies from 2 years to 10 years depending on the type of data and purpose of collection (reference should be done to the Code of Commerce, Civil Code and Labour Code);

- With regard to video surveillance, the CNPD considers that the images can be kept in principle for up to 8 days (Lignes directrices en matière de vidéosurveillance);
- Regarding recruitment data not resulting in candidate's hiring, Luxembourg law does not lay out specific retention periods. However, the CNIL advised within the Recruitment Operations Recommendation to adopt a 2 years retention period;
- Data obtained in the context of AML/CTF/KYC about client shall be kept for no longer than 5 years (Art. 3, Law of 12 November 2004 on AML/CFT Law, as amended);
- Personal Data related to building visitor registration shall be kept for no longer than 3 months (Deliberation CNPD n° 64/2007).

Reference should be made to the record of processing activities implemented by the AIFM for detailed information about the applicable retention period for each relevant processing activity. If not specified otherwise, Retention Periods are based on the date of the final version or last action.

Exceptions applies to the Retention Periods and related deletion or anonymization activities, such as the following suspension events:

- Contemplated or actual litigation or regulatory investigation;
- A Data Subject request under the Privacy Legal Framework; or
- An order for production from a regulatory or law enforcement body.

In such cases, Employees members are required to notify the Privacy Champion in a timely manner. Where an exception to this Policy which is not otherwise documented herein applies as a result of a potentially lawful reason which might prevent the AIFM destroying Data at the end of its Retention Period, such exception must be timely discussed with the Privacy Champion.

In case an exception to the Retention Periods applies, Data must be preserved and not amended until the Privacy Champion and the legal department / advisor determine they are no longer needed.

In addition, the Data shall be segregated, restricted and maintained until such time as the additional retention requirement expires with the assistance of the Information Technology department / service provider. Each Employee is responsible for ensuring Employees follow appropriate organizational use restrictions.

If a Employees member wishes on a case-by-case basis to retain specifically designated records, which may potentially contain Personal Data, beyond the established Retention Periods and to meet its own business needs, a specific authorization must be obtained from the Privacy Champion. In no instance should the retention period be shortened.

Eventually, it should be noted that not all documents contain Data and, therefore, such documents may be discarded or deleted at the discretion of the Employees once they have served their purpose.

6.1. Data destroying and anonymization

At the expiration of its Retention Period, Data shall be securely destroyed or anonymized. Destruction is defined as physical or technical destruction sufficient to render the information irretrievable by ordinary commercially available means. Anonymous data is defined as data that is rendered anonymous in such a way that the Data Subject is not or no longer identifiable and cannot be re-identified.

Destruction shall be considered secure where:

- Electronic Data has been securely overwritten and or the device(s) on which they are stored have been irretrievably destroyed;
- Manual Data have been shredded using crosscut shredding.

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;
- ;
- Audio / Video recording via MS Teams 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 employees 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.

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.

In the event the destruction of Data is carried out by a third party on our behalf, a destruction certificate or equivalent must be obtained.

Authorization for destruction shall be provided by the Privacy Champions together with the Employee identified as owning the Data. Annually, usually by end of November, the Privacy Champions is requested to guide the Employees in conducting a formal Data deletion process to identify and destroy records that have become obsolete under the current Policy, as well as the record of processing activities.

Following the abomination yearly exercise, a statement supporting the destruction process shall be periodically prepared and sent via email to the Privacy Champion to demonstrate that records containing Data were destroyed in accordance with this Policy.

The DPO may periodically carry out random checks on the effective compliance with this Policy. To such an extent, each Employee shall ensure to be able to demonstrate at any time, upon request from the DPO, the adherence to this Policy, as well as the effective erasure (or anonymization, where previously authorized) of Data.

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. RECORD OF PROCESSING ACTIVITIES

In accordance with Article 30 GDPR, the Manager maintains a record of all processing activities under its responsibility.

The Record represents a fundamental tool for the accurate and correct management of Personal Data processing, and it has a double relevance:

- Internal, because it allows to have an update of the outstanding processing also with a view to DPIA and to the identification of appropriate safeguards;
- External, as it is essential to demonstrate the compliance with the legal requirements in the field of data protection; for this purpose, it is made available to the CNPD, in case of an inspection.

The maintenance and update process of the Record is activated by the Privacy Champion in the following cases:

- Occasionally, if a new processing is initiated or an existing one is modified. The cases that may require an update of the Record include for instance, but is not limited to, the following: the processing of further data typologies, the inclusion or the removal of any purpose of processing, the addition or the removal of eventual extra-EU Transfers, modifications to the processing typology (paper/electronic form), the inclusion or removal of suppliers/third parties involved;
- Periodically, aiming at verifying the exact correspondence between the processing mapped in the Record and the ones carried out by the Company, updating the processing previously recorded, where necessary, and analyzing the eventual existence of new processing activities to be mapped.

All the Employees are requested to collaborate with the Privacy Champions to keep the Record duly updated.

Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller should evaluate the need to carry out a DPIA (as specified within Chapter 10), so that it is possible for the Company to legitimately proceed with the processing activities. Only once the activity has been recorded and the potential DPIA has been evaluated and/or performed, then it will be possible to initiate or carry on the processing activity.

Article 30, paragraph 1, lists the mandatory information that the Record of the Data Controller needs to report:

- The name and contact details of the Data Controller and, where applicable, of the joint controller of the processing, of the Controller's representative and of the Data Protection Officer;
- The purpose of the processing;
- The processing categories carried out on behalf of each Data Controller;
- A description of the categories of Data Subjects (as clients, prospects, employees, collaborators and so on) and of the categories of Personal Data, which may be examined in depth, at will, by the editor but that have to include, at least, the reference to common, sensitive and judicial Personal Data;
- The categories of recipients to which Personal Data have been or will be communicated, included the recipients of third countries or of international organizations;

- If applicable, the Transfers of Personal Data towards a third country or an international organization, and their identification; for the Transfers referred to in the second subparagraph of the Article 49 it has to be reported also the information and the documentation of the appropriate safeguards (as, for instance, the use of standard contractual clauses);
- Where possible, the deadline for the erasure of the different data categories;
- Where possible, a general description of the technical and organizational security measures to protect the processing systems and data.

The Article 30, paragraph 2, lists the mandatory information that the Record of the Data Processor needs to report:

- The name and contact details of the Data Processor(s), of each Data Controller on behalf of which the Data Processor(s) acts, of the Data Controller's representative or Data Processor's representative and, if applicable, of the Data Protection Officer;
- The processing categories carried out on behalf of each Data Controller;
- Where applicable, the Transfers of Personal Data towards a third country or an international organization, included the identification of the third country or of the international organization and, for the Transfers referred to in the second subparagraph of the Article 49, the documentation of the appropriate safeguards;
- Where applicable, a general description of the technical and organizational security measures referred to in Article 32.

The Privacy Champions 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 should be in writing, including in electronic form.

8. LAWFUL PROCESSING OF PERSONAL DATA

The Company generally only processes Personal Data if it is legally required to do so. For example, the Company has typically defined the following activities covered by a legal basis for processing purposes:

- Conducting of a customer due diligence check;
- Payment of salaries;
- Reporting of investor data to local authorities, e.g. to tax authorities for CRS and FATCA reporting obligations;



- Exchange of Employees data with Caisse Nationale de Santé;
- Exchange of Employees data with Centre commun de la sécurité sociale.

The Company checks on a case-by-case basis before any processing of Personal Data whether a legal basis covers this processing.

8.1. Legal basis of processing and purposes

The AIFM will only process Personal Data for a specific purpose associated to a duly identified legal basis of processing under Article 6 of the GDPR. Given the specific activities of the AIFM, the following basis are more likely to apply:

- Consent: namely, the Data Subject's Consent for the processing of his or her Personal Data for one or more specific purposes (e.g., processing of Special Categories of Personal Data, marketing activities);
- Performance of a contract: namely when the processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract (e.g., clients, employment, suppliers or service providers contractual relationships);
- Compliance with a legal obligation: namely when the processing is necessary for compliance with a legal obligation to which the AIFM is subject (e.g., AML/CTF requirements);
- Legitimate interests: the processing of Personal Data is necessary to pursue the AIFM's own legitimate interest (or that of a third party); in this case, a legitimate interest assessment is carried out by the Privacy Champion to satisfy a three-part test:
 - o Purpose test: are you pursuing a legitimate interest?
 - o Necessary test: is the processing necessary for that purpose?
 - o Balancing test: do the individual's interests override the legitimate interest?If the assessment (please refer to Annex 5) leads to identifying the legal basis of the data processing in the legitimate interest, the Privacy Champion documents and files the assessments made, keeping the documentation available to the CNPD, in compliance with the accountability principle.
- The AIFM may, in very limited cases, in accordance with Article 6 of the GDPR, apply other basis for processing such as: (i) to protect the vital interests of the Data Subject or another natural person or (ii) to perform a task carried out in the public interest.

In general, the AIFM's processing of Personal Data will be strictly limited to the context of the performance of its business based on the performance of a contract, the compliance with a legal obligation or its legitimate interest to perform specific processing activities, unless the Data Subject is requested to give his/her specific Consent for other purposes.

For each relevant processing activity and purpose of AIFM, the Privacy Champion oversees the application of a proper legal basis of processing, as well as the provision of the relevant information notice, as included in annex 6 and 7.

8.2. Rights of 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:

- 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 8 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.

- The right to restriction of processing

The Data Subject shall have the right to obtain from the Controller restriction of processing if:

- 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;
- the processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead; or
- 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.).

- 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.

- 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 Privacy Champion or the Risk Manager, so that they can update their records.

- 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.

- 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. DATA BREACH

Employees should notify the Board or the Privacy Champion immediately if they are concerned about a possible Data Breach. If a breach is discovered outside of term time by a Employees, they should alert the Privacy Champion immediately.

Data Breaches must be reported to the 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 Employees 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:

- Formation of a crisis management team (the “CT”) which shall consist of the Risk Manager, Privacy Champion and Main Contact Person;
- 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;
- The CT shall inform the CNPD within 72 hours and identify the key internal and external messaging for communications strategy and issue;
- The CT shall secure IT systems and stop additional data loss;
- 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;
- The Board shall report to police when/if considered appropriate;
- The Board shall notify regulators/consult with legal team/insurer etc.

10. WHAT INFORMATION MUST A BREACH NOTIFICATION CONTAIN?

The Notification must contain:

- The nature of the Data Breach including, where possible;
- the categories and approximate number of individuals concerned;
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer;
- a description of the likely consequences of the Data Breach; and
- a description of the measures taken, or proposed to be taken, to deal with the Data Breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

11. DATA PROTECTION IMPACT ASSESSMENT

A DPIA is a process designated to analyze, identify, and minimise the processing activities that by their nature, field of application, context and purposes potentially represent a high risk to the rights and freedoms of natural persons, such as:

- Use of systematic and extensive profiling with significant effects;
- Process of Special Categories of Personal Data or criminal offence Data on a large scale;
- Systematic monitoring of publicly accessible places on a large scale;
- Planning of new products and/or services or significant alterations;
- Relevant project initiatives;
- Outsourcing initiatives;

- Technological changes (e.g., relevant alterations to technological solutions or versions upgrades that may have impacts on the existing processing);
- Organizational alterations (e.g., business reorganizations and significant process changes);
- Corporate operations (e.g., acquisitions or disposals).

Depending on the circumstances of the processing, the following may be performed by the AIFM:

- Occasional DPIA, in case of new processing or relevant alterations to existing processing which may represent a high risk to the rights and freedoms of Data Subjects;
- Periodical / cyclical DPIA, in case of periodical audit of all the existing processing.

The DPIA is mandatory for the processing activities “*likely to result in high risks*” within the meaning of Art. 35 of the GDPR, such as:

- Use of systematic and extensive profiling with significant effects;
- Process of special category or criminal offence data on a large scale; or
- Systematic monitoring of publicly accessible places on a large scale activities.

The DPIA shall normally be formalized in a dedicated report and performed before the performance of the potential high risk processing activity to determine:

- The likelihood and the severity of any impact on individuals, namely the inherent risk of the processing in question;
- Appropriate technical and organizational security measures implemented or to be implemented to mitigate the inherent risk (namely, the residual risk) as to justify the relevant processing activity.

In the event that the processing of Personal Data undergoing the DPIA is characterized by a high residual risk, despite the application of the identified security measures, the Privacy Champion initiates the process of preventive consultation towards the CNPD before starting or carrying on the processing.

According to the CNPD recommendations, a DPIA can be considered sufficiently complete to meet the GDPR requirements if it:

- Contains systematic description of the processing (nature, scope, context and purposes);
- Addresses the necessity and the proportionality of the processing;
- Identify and assess risks to individuals;



- Manages the rights and freedoms of the Data Subjects;
- Assess the compliance and security measures;
- Identify any additional measures to mitigate relevant risks;
- Has involved interested parties and the point of view of Data Subjects where appropriate.

12. THIRD PARTY MANAGEMENT AND OUTSOURCING

When performing data protection activities on Data Subjects, the AIFM may qualify as:

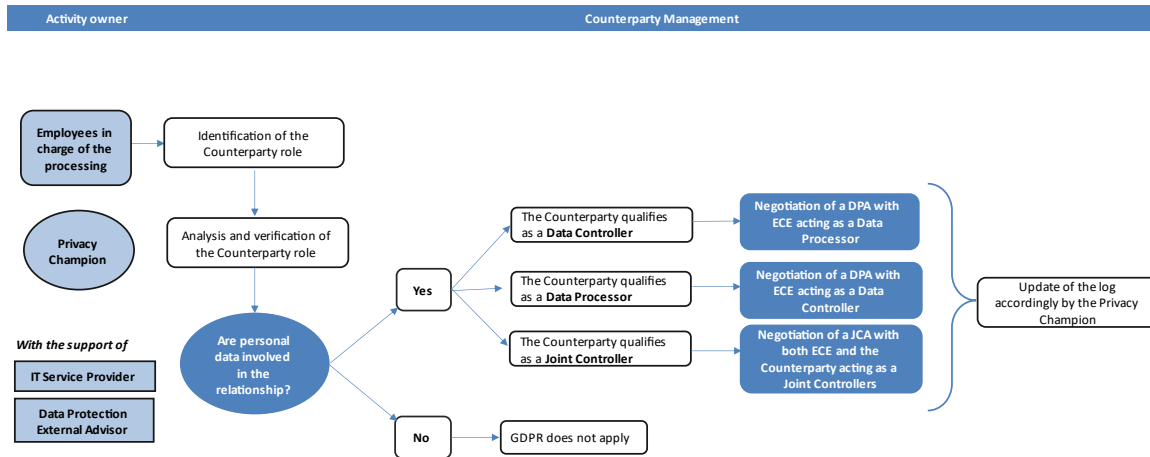
- Controller as long as alone determines the purposes and means of the processing of Personal Data (e.g., in relation to the Employees processing activities, external providers processing Personal Data of behalf of the AIFM);
- Processor as long as it processes Personal Data on behalf of a Controller;
- Join controller as long as jointly with other Controllers, determines the purposes and means of the processing of Personal Data.

13. POTENTIAL SCENARIOS

The GDPR establishes obligations about the assessment of the privacy and data protection role of the entities or subjects involved in relevant data processing activities (namely, the Counterparties).

The management of the Counterparties involves the following steps:

- (1) Identification of the privacy role to be assigned to the Counterparties, who are required to process Personal Data of Data Subjects when performing their activities; and
- (2) Adequacy assessment of the Counterparties in terms of reliability, experience and ability to carry out Personal Data processing activities.



As for step (1) above, the processing can be carried out on behalf of:

- Data Controller: the natural or legal person, the public authority, the service or the other entity that, individually or along with others, determines the purposes and the means of the Personal Data processing (Article 4(7) of GDPR);
- Data Processor: the natural or legal person, the public authority, the service or the other entity that processes Personal Data on behalf of the Data Controller (Article 4(8) of GDPR);
- Joint controllers: two or more Data Controllers that jointly determine the purposes and means of processing (Article 26 of GDPR).

In particular - concerning scenarios A and B above - whether a processing is carried out on behalf of the Data Controller, the Data Controller must recourse uniquely to one or more Data Processor(s) which possess sufficient safeguards to implement appropriate technical and organizational security measures, with the aim to ensure that the processing meets the GDPR requirements and also guarantees the protection of the Data Subject.

The Data Controller authorizes the Data Processor to process Personal Data by contract or other legal acts, for instance the letter of appointment as external service provider, specifying the field covered, the duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of Data Subjects, the obligations, and rights of the Data Controller.

The contract – or the annex to the relevant agreement with the service provider - is also known as DPA, and it is governed by Article 28 of the GDPR, according to which the Data Processor is at least required to:

- Process the Personal Data only on documented instructions from the Data Controller, including with regard to Transfers of Personal Data, unless required to do so by the applicable law. In this case the Data Processor shall inform the Data Controller of that legal obligation before processing, unless the law prohibits such information on important grounds of public interest;
- Ensure that persons authorized to process the Personal Data have committed themselves to confidentiality;
- Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk under Article 32 of GDPR;
- Not engage another Processor without prior specific or general written authorization of the Data Controller; in case, the same data protection obligations as set out in the contract or other legal act between the Data Controller and the Data Processor must apply;
- Assist the Data Controller in ensuring compliance with relevant Data Breach and data protection impact assessment requirements taking into account the nature of processing and the information available to the Processor;
- Assist the Data Controller for the fulfilment of its obligation to respond to requests for exercising the Data Subject's rights;
- Delete or return all the Personal Data to the Data Controller after the end of the provision of services relating to processing, and delete existing copies unless the applicable law requires storage of the Personal Data; and
- Make available to the Data Controller all information necessary to demonstrate compliance with the GDPR obligations and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Data Controller.

Concerning scenario C described above, under Article 26 of GDPR, the Joint Controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under GDPR - in particular as regarding the exercising of the rights of the Data Subjects and their respective duties to provide the information notices referred to in Articles 13 and 14 of GDPR - by means of an arrangement between them (namely, the Joint Controller Agreement, hereinafter “JCA”) unless, and in so far as, the respective responsibilities of the Controllers are determined by any applicable law to which the Controllers are subject. The arrangement may designate a contact point for Data Subjects.

The JCA referred to above shall duly reflect the respective roles and relationships of the Joint Controllers vis-à-vis the Data Subjects. The essence of the arrangement shall be made available to the Data Subject.

14. PRIVACY ROLE IDENTIFICATION, ASSESSMENT AND AGREEMENT


Should the AIFM engage with a Counterparty, the interested Employee is required to proceed with the Counterparty privacy role assessment duly involving from beginning the Privacy Champion. The aim is to verify in advance the existence of a Personal Data processing activity connected to the contractual relationship with the Counterparty, as well as the nature of its involvement under the scenarios described in Chapter 11.1 above.

In this context, the Privacy Champions will keep a list of the relevant Counterparties, as well as the AIFM Employee in charge of the Counterparty relationship (each a “Main Contact Person”) by means of a dedicated log (as included in annex 4).

Specifically, the Main Contact Person, assisted by the Privacy Champion, proceeds with the verification of the Counterparty role and adequacy assessment. the AIFM will only engage Counterparties which comply with the Privacy Legal Framework or equivalent requirements. To this aim, the AIFM performs due diligence and oversight on all its Counterparties. An important aspect of the due diligence is to ensure that the Counterparty comply with the GDPR in respect to Personal Data and monitoring that they continue to comply. Indeed, 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 Privacy Champion accordingly who shall then keep a list of the above-mentioned information within the dedicated Counterparty management log.

Afterwards, the Privacy Champion proceeds with the provision or negotiation of the relevant contractual arrangements as follow:

- Should the AIFM act as Data Controller, being the owner of the processing, it is required to submit a dedicated DPA tailored on the specificities of the Counterparty;
- Should the AIFM act as Data Processor, it is required to negotiate the DPA normally provided by the Counterparty. Should the latter not occur, the Privacy Champion will explicitly request the Counterparty DPA or, alternatively, provide the AIFM a DPA;
- Should the AIFM and the Counterparty act as Joint Controllers, provision of a dedicated JCA on a case-by-case scenario.

ECE Real Estate Partners S.à. r.l.	
08.10. Privacy and Data Protection Policy and Procedure	

In all scenarios mentioned above, the Privacy Champion duly verify the compliance of the negotiated DPA or JCA with the GDPR. In addition, all relevant privacy relationships of the AIFM are duly recorded within a Counterparty log maintained by the Privacy Champion.

15. TRANSFER OF PERSONAL DATA TO THIRD PARTIES AND NON-EU COUNTRIES

As a general remark, and as detailed in Chapter 4 above, the AIFM does not Transfer Personal Data to third parties unless at least one of the following conditions is met:

- The Transfer of Personal Data is necessary for the performance of a contract as specified within the relevant information notice and/or privacy contractual relationship;
- There is a provision of law that requires such communication (e.g., for purposes relating to anti-money laundering regulations, prevention of fraud, bribery, or market abuse, regulatory and tax reporting purposes);
- The relevant consent has been obtained from the Data Subject;
- The Transfer takes place for anonymized or pseudonymized data only for statistical or market analysis purposes;
- The Transfer of Personal Data is required by a judgement of court or tribunal and any decision of an administrative authority; if coming from a jurisdiction outside the EU, such Transfer of data may only take place on the basis of mutual legal assistance treaty in force between the requesting country and the EU or Luxembourg.

There are restrictions on international Transfers of Personal Data. No data may be Transferred outside of the EEA without first discussing it with the Privacy Champions.

Any Transfer of Personal Data anywhere outside the Grand Duchy of Luxembourg and Germany must be approved by the Board. Indeed, the AIFM will not perform such Transfer unless at least one of the safeguards under Chapter V of GDPR apply, such as, among others:

- Adequacy Decision about a third country or the international organisation ensuring an adequate level of protection;
- Application of SCCs adopted either by the EC or the relevant supervisory authority;
- Binding corporate rules;
- Approved code of conduct; or
- Consent.

If strictly necessary, the AIFM will perform the Transfer of Personal Data outside the EEA based on the Adequacy Decision of the EC that, as of today, has recognised the following countries as having a privacy and data protection framework at least equivalent to the European Union: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom and Uruguay.

In the event that the country or one or more of the countries to which Personal Data is to be transferred is not subject to an Adequacy Decision from the EC, the AIFM applies SCCs as appropriate and included in Annex 1 and 2 below.

16. DISCIPLINARY PROCEDURE FOR ANY VIOLATION OF THIS POLICY

Due to the high relevance of the data protection provisions and the special degree to which the AIFM requires the confidentiality of each Employee, The AIFM reserves the right to initiate disciplinary procedures in the event of any breach by an Employee in which a breach may result in consequences for the respective Employee.

The disciplinary procedure can be initiated by both the Privacy Champion and a Board Member of the AIFM. Such disciplinary procedure must be strictly documented, whereby the accused Employee must be given sufficient time and space for a counter-statement.

17. ANNEXES

17.1. Standard Data Protection Clause (Controller)



Standard Clause I
a.pdf



CELEX_32021D0914_E
N_TXT_Standard cont



Standard Clause
I.pdf

17.2. Standard Contractual Clauses (Processors)



Standard clause
II.pdf

17.3. Assessment on the necessity to appoint a DPO

As of today - pursuant to Article 37 of the GDPR, as well as the relevant WP29 Guidelines – the AIFM shall not be considered as an entity for which the designation of a DPO is mandatory based on, among others, the following considerations:

- The AIFM is not a public authority or body;

- The core activities of the AIFM do not consist of processing operations which required regular and systematic monitoring of Data Subjects on a large scale; rather, processing operations shall be considered as ancillary activities and not as inextricable part of the AIFM business;
- The core activities of the AIFM do not consist of processing on a large scale of Special Categories of Personal Data relating to criminal convictions and offences but, rather, is limited to the collection of such Personal Data to fulfil AML/CTF regulatory requirements only. Moreover, the number of Data Subjects, volume of Personal Data, duration and geographical extent of the processing are limited.

As a result, the AIFM decided, for the time being, not to appoint a DPO but, rather, a Privacy Champion performing equivalent tasks as further detailed in Chapter 2 above. the AIFM involves the Privacy Champion in all issues which relate to the protection of Personal Data and ensures that he has sufficient resources, acts independently, is contactable by Data Subjects and is bound by secrecy and confidentiality rules when performing relevant privacy and data protection activities.

17.4. Management of third parties' privacy relationships



ECE Management
of third parties privac

17.5. Legitimate interest impact assessment



LIA
TEMPLATE_ECE.xlsx

17.6. 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:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- 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

17.7. 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 employees of relevant service providers);
- Financial information (such as bank account data, tax code);
- Characteristics (nationality, country and date of birth of board members shareholders, employees 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;
- Depositories;
- 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:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- 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

17.8. Privacy notice (how we use information of external entities other than Employees and investors)

Why do we collect and use information of external entities?

We collect and use information of external entities 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 external entities data (non-exhaustive list):

- to carry out required legal background checks;
- to carry out know your customer checks;
- to carry out name screening via adverse media;
- to run any delegation oversight, if required;

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

- Personal information (such as name and address);
- Know your customer documents.

Collecting external entities 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 external entities information with?

We routinely share external entities information with:

- Local authorities;
- Investors;
- Entities that are authorized to audit the Company.



Why we share external entities information

We do not share information about our external entities 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, natural persons 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:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- 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