



General Data Protection Regulation

Process Document Description

<i>Objective/Description</i>	<p>Shelter Investment Management (SIM) attaches great importance to privacy and wants to fully respect this by treating personal data as safely and confidentially as possible. In this document, you will find the General Data Protection Regulation ('GDPR') Policy applicable within SIM. GDPR applies throughout the European Union from May 25, 2018 and requires the presence and implementation of contracts between data controllers and their data processors.</p> <p>The objective of this data protection statement in accordance with GDPR is to protect the rights of data subjects and to explain which personal data is processed and why.</p>
<i>Entity</i>	SIM

Update Document Management – Version History

<i>Version</i>	<i>Date</i>	<i>Status</i>	<i>Author</i>	<i>Modification Type</i>
1.0	27/04/2018	Draft	Ludovic Dellal	Creation of the document
2.0	02/05/2018	Update	Olivier Lechanteur	Update document
2.1	20/05/2019	Update	Olivier Lechanteur	Update contact list
2.2	25/06/2021	Update	Sandra Van Vaerenbergh	Update notification procedure
3.0	30/08/2023	Update	Sandra Van Vaerenbergh	Revision
3.1	15/06/2024	Update	Sandra Van Vaerenbergh	Removal of the opt-out for the register on treatment of activities
4.0	14/11/2025	Update	Sandra Van Vaerenbergh	Update of the document
5.0	13/02/2026	Update	Sandra Van Vaerenbergh	Update of the document with differentiating timetable for anonymization/deletion of data

Validation of this document

<i>Date</i>	<i>Approver</i>	<i>Function/Unit</i>	<i>Status</i>
18/05/2018	Christophe Pecoraro	Board Member	Validated
18/05/2018	Benedict Peeters	Board Member	Validated
20/05/2019	Benedict Peeters	Board Member	Validated
28/06/2021	Board (by Board Resolution)		Validated
11/09/2023	Board		Validated
30/08/2024	Board		Validated
18/11/2025	Board		Validated
17/02/2026	Board		Validated

Table of Contents

1	Introduction	3
2	Scope of this Policy	3
3	Types of Personal Data Collected	3
4	Data Protection Principles.....	4
5	Key Definitions	4
6	Roles and Responsibilities.....	4
7	Purpose of the collection and processing of Data	5
8	Retention Period	5
9	Timeline to report breaches	6
10	Data Protection Controls.....	6
11	Data Collection and Processing Principles	7
12	Data Security Principles.....	7
13	Data Retention Principles.....	8
14	Training and Awareness Principles	8
15	Compliance Monitoring and Review.....	8
16	Access to the Personal Data.....	9
16.1	Internal Use.....	9
16.2	External Use	9
17	Register of treatment of activities	9
18	Appendix: Contacts	10

1 Introduction

SIM, acting as **data controller**, is responsible for the processing of personal data of its clients, employees, contractors and other individuals ('data subjects'). SIM is committed to protecting personal data in accordance with the principles of **lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality**, as set out in the **General Data Protection Regulation ('GDPR')** and the Luxembourg Data Protection Act of 1 August 2018.

The objective of this data protection statement in accordance with GDPR is to inform the concerned data subjects about :

- the categories of personal data SIM collects;
- the purposes and legal bases for which SIM processes and stores personal data;
- the rights of data subjects under GDPR (including the right to lodge a complaint with the Commission Nationale pour la Protection des Données – CNPD);
- SIM's obligations and measures to ensure compliance and accountability in connection with personal data processing.

2 Scope of this Policy

This policy applies to all personal data processed by SIM in its capacity of data controller (and, where applicable as processor) in the course of its operations. It covers all processing activities, regardless of whether the data is stored electronically or on paper, and regardless of location, including processing performed by third-party service providers on behalf of SIM. The scope includes personal data relating to clients, employees, permanent service providers, interns, contractors, and other identifiable individuals.

3 Types of Personal Data Collected

In the course of our activities (including portfolio management services) SIM collects and processes the following categories of personal data related to the aforementioned data subjects:

- Identification- and contact details (e.g., name, surname, date of birth, address, registration number, etc..);
- personal information (e.g., nationality, gender, mother tongue, etc..);
- Family composition details (e.g., marital status, number of children) and where legally required, information about partners and children;
- Employment details and sector of activity;
- Financial information (e.g. bank account number, tax residence, salary, bonuses, commissions, etc ..);
- Information about family wealth and property rights (e.g., donations, inheritance, real estate property, insurance policies, holding vehicles, etc..);
- Payment and transaction history;
- Tax status;
- Technical and digital identifiers (e.g., IP address, device information) when accessing SIM's systems.

As a rule, SIM does not collect or process special categories of personal data (e.g., health-related information) unless required by law or with explicit consent, in accordance with GDPR.

4 Data Protection Principles

SIM adheres to the following data protection principles:

1. **Lawfulness, Fairness, and Transparency:** Personal data is processed lawfully, fairly, and in a transparent manner.
2. **Purpose Limitation:** Personal data is collected for specified, explicit, and legitimate purposes, and not further processed in a manner incompatible with those purposes.
3. **Data Minimization:** Personal data is adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
4. **Accuracy:** Personal data is accurate, kept up to date, and necessary steps are taken to rectify any inaccurate or incomplete data.
5. **Storage Limitation:** Personal data is retained for no longer than necessary for the purposes for which it is processed.
6. **Integrity and Confidentiality:** Personal data is processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
7. **Accountability:** SIM is responsible for and able to demonstrate compliance with these principles through documented policies, procedures, and controls.

5 Key Definitions

- **Data controllers** are natural or legal persons, public authorities, agencies, or any other bodies that, alone or jointly with others, determine the purposes, conditions and means of the processing of personal data.
- **Data processors** are natural or legal persons, public authorities, agencies, or any other bodies that process personal data on behalf of the controller.
- **Third parties** are natural or legal persons, public authorities, agencies or bodies other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

6 Roles and Responsibilities

1. **Data Protection Officer (DPO):** SIM has appointed a Data Protection Officer in accordance with GDPR requirements, given the nature and scale of its processing activities. The DPO operates independently and reports directly to senior management. Responsibilities include monitoring compliance with GDPR and this Policy, advising on data protection obligations, and acting as the contact point for the supervisory authority

(CNPD). For any questions, concerns, or requests regarding data protection, individuals can contact SIM's DPO using the details provided in the appendix.

2. Data Controllers and Processors: SIM identifies the roles of data controllers and processors for all personal data it handles and ensures that appropriate written agreements are in place with third-party processors, as required by GDPR article 28. These agreements include obligations regarding confidentiality, security measures, sub-processing, and audit rights.

7 Purpose of the collection and processing of Data

SIM collects and processes personal data strictly for specified, explicit, and legitimate purposes, including:

- Fulfilment of contractual obligations related to portfolio management and investment services;
- Compliance with legal and regulatory requirements applicable to Luxembourg-based (A)IFMs, including AML/CFT obligations, tax reporting, and CSSF regulations;
- Internal administrative and operational purposes necessary to support business activities.

Processing is based on the following legal grounds under GDPR:

- Performance of a contract (Article 6(1)(b));
- Compliance with legal obligations (Article 6(1)(c));
- Legitimate interests pursued by SIM (Article 6(1)(f)), where applicable.

Data subjects have the rights of access, rectification, erasure (“right to be forgotten”), portability, objection and restriction of processing, subject to applicable legal limitations.

Access to personal data is strictly controlled through role-based permissions and confidentiality obligations.

8 Retention Period

Retention periods vary depending on the purpose and legal requirements that are linked to the different categories of data (see below retention Matrix)

Data Category	Legal Basis	Retention Period	Notes / Exceptions
Investor KYC Data	AML/CFT Law (Art. 3 & 5)	5 years after relationship ends	Extend if investigation ongoing
Transaction Records	AML/CFT + CSSF Circulars	5 years after transaction	Longer if required by CSSF audit
Accounting & Tax Records	Luxembourg Commercial Code, VAT Law, Inheritance Tax Law	10 years	Includes invoices, ledgers
Cross-Border Tax Reporting	FATCA (Foreign Account Tax Compliance Act) + CRS (OECD Common Reporting Standard)	7 years after reporting year	Covers tax residency and reporting evidence
Fund Registers	CSSF Regulatory Requirements	10 years	For audit and supervisory review
Board Minutes / ExCo	Company Law	Permanent or 10+ years	Governance and legal defense
Marketing Data	GDPR (Consent)	Until consent withdrawn	Delete immediately upon withdrawal
Litigation Hold Data	Legal Defense	Until case resolved	Overrides normal retention schedule

9 Timeline to report breaches

If a data breach occurs the financial institution/(A)IFM must :

- Assess the risk level linked to the nature of the breach and the potential impact on the data subjects/individuals.
- Take the necessary actions to document, notify, mitigate and report the concerned breach (see table below)
- In case of high risk level : notify the Data Protection Authority within 72 hours of becoming aware of the breach (or within 48 hours for critical sectors under new EU rules since 2025) and inform affected individuals if there's a high risk to their rights. – see table below.

In case of critical risk level : Immediately notify the CNPD and the CSSF, activate a crisis response team, implement and execute a public communication plan.

Risk Level	Example Scenarios	Impact on Individuals	Recommended Action
Low	- Accidental email to wrong internal recipient (no sensitive data) - Minor system outage without data loss	Minimal inconvenience	Document internally, monitor, no CNPD report
Medium	- Loss of encrypted device (with strong password) - Small data set exposed (non-sensitive)	Limited risk of misuse	Assess risk, consider CNPD notification if doubt
High	- Exposure of KYC documents (passport, ID) - Breach of FATCA/CRS tax data - Large investor database leaked - Ransomware attack on core systems	Identity theft, financial fraud, reputational harm	Notify CNPD within 72h (or 48h best practice), inform affected individuals, implement mitigation
Critical	- Combined breach (financial + biometric data) - Data used for fraud or phishing - Breach affecting thousands of investors globally	Severe harm, regulatory sanctions, litigation risk	Immediate CNPD+ CSSF notification, crisis response team, public communication plan

10 Data Protection Controls

SIM continuously enhances its privacy framework to meet GDPR requirements and maintain compliance with regulatory developments. Appropriate technical and organizational measures are implemented to ensure that personal data is effectively managed and protected against accidental or unlawful destruction, deletion, loss, unauthorized access, or any other form of unlawful processing.

In particular:

- **Data Minimization and Accuracy:** SIM collects only data that is necessary, relevant, and proportionate to the purposes described. SIM ensures data remains accurate and up to date by requesting regular updates and advising data subjects to promptly inform SIM of any changes.
- **Security Measures:** SIM applies encryption, secure storage systems, and role-based access controls to protect personal data.

- **Confidentiality and Training:** Employees and contractors are bound by confidentiality obligations and receive regular training on data protection requirements.
- **Data Protection by Design and by Default:** Privacy principles are integrated into systems and processes from the outset.
- **Monitoring and Review:** SIM periodically tests and evaluates its security measures to ensure ongoing effectiveness.

11 Data Collection and Processing Principles

SIM adheres to the following principles in accordance with GDPR:

1. **Lawful Basis for Processing:** Personal data is processed based on one or more lawful bases under Article 6 of the GDPR, including performance of a contract, compliance with legal obligations and legitimate interests pursued by SIM.
2. **Data Subject Rights:** SIM respects the rights of data subjects, including rights to access, rectification, erasure (“right to be forgotten”), restriction of processing, objection, data portability, and the right not to be subject to automated decision-making. These rights may be subject to limitations under applicable laws (e.g., AML/CFT regulations).
3. **Data Transfers:** Any transfer of personal data outside the European Economic Area (EEA) is conducted in compliance with the GDPR requirements, using appropriate safeguards, such as adequacy decisions, Standard Contractual Clauses, or other mechanisms approved by the European Commission.
4. **Automated Decision-Making:** SIM does not engage in automated decision-making or profiling that produces legal or similarly significant effects on data subjects.

12 Data Security Principles

SIM implements appropriate **technical and organizational measures** to ensure a level of security appropriate to the risk, in accordance with GDPR Article 32.

These measures include:

- **Access Control:** Role-based permissions and authentication procedures to prevent unauthorized access.
- **Data Security:** Protection of data in transit and at rest, secure storage systems, and regular backups.
- **Confidentiality:** Staff training and confidentiality agreements for all employees and contractors.
- **Data Protection by Design and by Default:** Privacy principles integrated into systems and processes from the outset
- **Monitoring and Review:** Regular testing and evaluation of security measures to ensure ongoing effectiveness.
- **Incident Response:** SIM maintains a documented procedure in place to promptly identify, assess, and mitigate any risks in the event of a personal data breach. The CNPD will be notified within 72 hours unless

the breach is unlikely to pose a risk to individuals' rights and freedoms. Where required, affected data subjects will also be informed without undue delay.

13 Data Retention Principles

Personal data is retained only for as long as necessary to fulfil the purposes for which it was collected or as required by applicable laws and regulations. SIM maintains a data retention policy specifying retention periods for different categories of personal data.

After the retention period expires, personal data is securely deleted or anonymized. SIM regularly reviews retention schedules to ensure compliance with GDPR and legal requirements.

14 Training and Awareness Principles

SIM provides regular training and awareness programs to employees and contractors to ensure they understand their data protection responsibilities, GDPR requirements, and related policies and procedures.

The program covers:

- GDPR principles and SIM's data protection policies;
- Data subject rights and how to handle requests;
- Security measures and incident response procedures;
- Role-specific responsibilities for handling personal data.

SIM maintains records of training completion and uses internal communications (e.g., newsletters, reminders) to reinforce awareness and compliance.

15 Compliance Monitoring and Review

SIM monitors compliance with this GDPR Policy and periodically reviews, audits and risk assessments to ensure ongoing adherence to applicable data protection laws and regulations. Reviews are conducted at least annually and whenever significant regulatory or operational changes occur.

Updates to this Policy will be documented and communicated through appropriate channels, including publication on SIM's website and direct notification to employees and relevant stakeholders.

By implementing and regularly updating this GDPR Policy, SIM demonstrates its commitment to safeguarding personal data and ensuring compliance with the GDPR and Luxembourg data protection requirements.

16 Access to the Personal Data

16.1 Internal Use

Access to personal data of SIM's data subjects is only granted to relevant staff involved in portfolio management, client relationship management, and to the conducting officers and Board of SIM in order to allow them to fulfil their respective duties (need-to-know basis).

16.2 External Use

Personal data may also be shared with certain third parties, strictly necessary for the performance of their respective legal obligations, such as :

- (Depository) banks for managing bank accounts of data subjects as stipulated in signed mandates;
- Third parties performing governance or legal functions, such as compliance officers, internal and external auditors;
- National or international governing body, courts or related organisations to which SIM is legally obliged to provide information.

These third parties are contractually or legally obliged to guarantee the confidentiality and safety of the personal data thus gathered in accordance with the applicable legislation.

17 Register of treatment of activities

In compliance with GDPR, SIM maintains a detailed register of all processing activities involving personal data, including :

- **Purpose of Processing:** The specific purpose for which the personal data is processed.
- **Categories of Data Subjects:** The types of individuals whose data is being processed.
- **Categories of Personal Data:** The types of personal data being processed.
- **Recipients of Data:** The entities or individuals to whom the personal data is disclosed.
- **Retention Period:** The duration for which the personal data will be retained.
- **Technical and Organizational Security Measures:** The security measures implemented to protect the personal data.
- **Data Transfers outside the EEA and related safeguards:** Any transfers of personal data to third countries or international organizations, including the identification of such countries or organizations and the safeguards in place.

This register is reviewed and updated regularly to ensure accuracy and completeness, demonstrating SIM's commitment to GDPR compliance and facilitating cooperation with supervisory authorities.

	<h2>GDPR Policy</h2>	Date: 17/02/2026 Version N°: V4.0 Status: Validated
---	----------------------	--

18 Appendix: Contacts

Function	Name	Mail	Tel
Data Protection Officer	Sandra Van Vaerenbergh	sv@shelter-im.com	T: +352 206 03 000 80
Head of Portfolio Management	Benedict Peeters	bp@shelter-im.com	T: +352 206 03 000 30
Permanent Risk Management Function	Sandra Van Vaerenbergh	sv@shelter-im.com	T: +352 206 03 000 80