GDPR POLICY

October 2025

Document Owner	Corinne Lafaurie-Konter
Approver(s)	Maxime Kahn
Board or Committee Approval Required ?	no

Version No.	Review Date	Author	Approval Date	Comments
1	October 2025	C.Lafaurie-Konter	October 2025	English version & Fund upgrade

Table of Contents

1 REGULATORY REFERENCES

- European General Data Protection Regulation (GDPR) No. 2016/679
- Data Protection Act (CNIL) of January 6, 1978, amended in 2004

2 GOVERNANCE & CONTROL

The policy applies to all processing of personal data carried out by the Company in the context of its activities, including asset management, client relationship management, human resources, and interactions with service providers or regulators.

This policy is updated as needed and reviewed at least annually. The Chief Executive Officer (CEO) of 111 Capital (the Company) ensures that this review is carried out under the responsibility of the Compliance Officer (RCCI).

The CEO is the Data Controller and may act as Data Protection Officer (DPO), unless an external DPO is appointed. The Compliance Officer (RCCI) monitors GDPR compliance within the annual Compliance and Internal Control Plan. The Risk Control Committee receives periodic updates on GDPR compliance, incidents, and risk assessments.

Permanent Control ensures annual compliance with this procedure and with regulations, as part of the annual Compliance and Internal Control Plan. Similarly, Periodic Control ensures compliance on a triennial basis.

3 DATA SUBJECTS

3.1 CLIENTS AND PROSPECTS

111 Capital manages investment strategies on behalf of professional and institutional investors.

In practice, the Company can operate through management by delegation for certain investors 'assets, through a fund or through separated managed accounts .

Personal data processed in this context concern representatives, signatories, or beneficial owners of institutional clients or investors, i.e. the "data subjects".

The Company therefore processes personal data for the following purposes:

- client onboarding and KYC/AML procedures;
- execution and management of investment management agreements;
- administration and valuation of funds and accounts;
- investor and regulatory reporting (AMF, ACPR, tax authorities, etc.);
- communications regarding fund performance, compliance, and governance.

Processing is carried out in compliance with GDPR, based on:

- contractual necessity: performance of a management agreement or fund relationship;

- legal obligations: compliance with AML/KYC, tax, and other regulatory obligations;
- legitimate interest: proper management and oversight of investment activities.

Representatives of clients and investors are informed of their rights, including access, rectification, erasure, objection, restriction, and portability.
Requests should be sent to the Company's GDPR Contact mailbox or directly to the CEO, who acts as Data Controller.

3.2 Employees and Other Data Subjects

111 Capital also collects and processes data relating to its employees, interns or service providers, as well as applicants or interns wishing to join the Company, and finally shareholders (generally employees).

This data is collected mainly to comply with the Company's legal, regulatory, and contractual obligations. In addition, data may also be collected based on the consent of the data subjects, in the context of recruitment (voluntary communication by candidates of their applications).

The personal data collected from employees or interns is only that which is necessary for HR processing, i.e., data relating to academic training and professional experience, personal contact information, as well as any information required for the preparation of employment contracts, internship agreements, payroll management, and administrative management (name, address, nationality, date and place of birth, bank details, etc.).

Regarding personal data voluntarily provided by applicants seeking an internship or job, i.e., data relating to their academic background and professional experience, personal contact details, and any information necessary for reviewing their applications, it is used exclusively for this purpose.

4 Data Access

Within 111 Capital, personal data is stored on the Company secured network and access to it is granted only to employees who need to know it or when necessary for IT system administration.

A review of access rights to the Company's office network, which hosts this data, is carried out at least annually as part of the overall review of employee access, reported to the Risk Control Committee.

Regarding employees, access to this data is specifically limited to Management, in particular the CEO who is responsible for HR management at 111 Capital. Regarding applicants or interns, staff members from different management teams may access this data as needed.

Prospects, client and investor data access is limited to the Management, and in particular to 111 Capital President.

5 Data Transfers

Provided the third parties comply with professional secrecy obligations, certain personal data may be shared, on a strictly need-to-know basis, and transmitted externally:

- to service providers engaged by 111 Capital to manage payroll, accounting, R&D tax credit calculation, as well as internal control and compliance, as well as to administrators, depositaries, auditors, etc...
- to counterparties and institutional investors, when contractually required.
- public authorities and organizations such as the AMF or tax authorities, where legal obligations or official decisions require such disclosure.

These service providers are also subject to GDPR regulations and ensuring confidentiality, security, and cooperation in case of data breach. In case of transfer outside the EU, i.e. international transfers, the data is sent through a secure transmission protocol and/or secured files with password protection.

6 DATA RETENTION

111 Capital processes and retains personal data of data subjects as long as necessary to fulfill legal and contractual obligations. The retention period is specified according to the nature and use of the data in the Data Processing Register maintained by the Company.

When data is no longer necessary for fulfilling obligations, it is archived and/or deleted during a periodic review, at least annually, conducted by the CEO .

Regarding Company employees, personal data is retained while the employee works at the Company and for a maximum of 5 years after their departure. Regarding applicants for internships or jobs, data is retained for the time necessary to review their applications and deleted during the periodic review, at least once a year, conducted by the CEO.

Prospects, client and investor data are retained for the duration of the relationship and for 5 to 10 years thereafter, depending on statutory requirements under AML and financial regulations.

7 GDPR PROCESSING REGISTER

The CEO of 111 Capital is responsible for the regular update, at least annually, of the Personal Data Processing Register for the Company, and for archiving or deleting data when required. It shall be updated in case of new activities (including clients, funds, or managed accounts).

This Register includes in particular the following items: purposes of processing, types of data, legal basis, recipients, retention period, and security controls.

8 RISK ASSESSMENT AND IMPACT ANALYSIS

An annual risk assessment of personal data breach is carried out by the CEO , with conclusions reported to the Risk Control Committee.

The methodology consists in evaluating the processes deployed by the Company for personal data processing according to the following five criteria:

- Volume/type of data collected and processed
- Data sensitivity

- Data security
- Data retention
- Employee GDPR training

The CEO also conducts an annual impact analysis of personal data processing and ensures that new processes involving personal data collection and management are assessed before being implemented.

9 INCIDENT MANAGEMENT

The CEO is responsible for managing potential incidents, and any such incident must be reported to them.

The incident must be documented with the following information:

- nature of the personal data breach,
- assessment of severity, where possible including approximate number of data subjects and records affected,
- potential consequences of the breach,
- measures taken to remedy or mitigate the incident's potential impact.

Based on these elements, a report may be submitted by the CEO to the supervisory authority if deemed necessary by 111 Capital Management, as soon as possible after the incident occurs (if possible within 72 hours, otherwise with justification for delay). This report includes all of the above-listed information. Based on the same elements, the Management also determines whether it is necessary to notify the affected data subject(s), as soon as possible. If deemed necessary, the CEO is responsible for carrying out this notification.

Finally, all incidents are systematically reported to the monthly Risk Control Committee, with the information listed above.

10 EMPLOYEE TRAINING

The Company provides annual training to its employees, in order to raise awareness of GDPR regulations, clarify their roles and responsibilities in ensuring GDPR compliance, specify the applicability of GDPR to 111 Capital, identify those responsible for data protection within the Company, and outline internal processes to be followed.

11 RIGHTS & NOTICES

11.1 RIGHTS OF DATA SUBJECTS

Under the GDPR, it is recalled that each data subject has the right to access their data, request its rectification, erasure, or restriction of processing, or object to its processing. Each data subject also has

the right to data portability. Provisions laid down in the implementing decrees of GDPR by EU Member States also apply.

Likewise, Article 77 of the GDPR provides the right to lodge a complaint with a data protection supervisory authority. Thus, each data subject may file a complaint with the CNIL, either by mail to CNIL - Service des Plaintes - 3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07, or directly online at www.cnil.fr/fr/plaintes.

Any data subject may, at any time, request the exercise of their rights and/or withdraw consent to the processing of their personal data, by notifying 111 Capital. Requests for opposition or rights exercise can be submitted under the subject line "GDPR – Objection/Request to Exercise Rights" to the Company's Contact mailbox, or addressed directly to the CEO , who is responsible for GDPR processing for the Company.

The same rule applies to consent declarations given before the GDPR effective date, i.e., before May 25, 2018. However, data subjects are reminded that withdrawal of consent applies only prospectively, from the date of the withdrawal request, and does not affect the lawfulness of prior processing.

If applicable, the CEO of the Company is responsible for addressing such requests.

If a data subject exercises their right to object, 111 Capital will cease processing their personal data, unless the Company has legitimate grounds overriding the interests of the data subject.

Personal data communicated to the Company in the context of information requests or business proposals via its website, and potentially collected, is not processed or retained by the Company. Only contact made for applications to join the Company may result in potential processing.

11.2 Notice to Data Subjects

A notice summarizing their GDPR rights is provided to clients and investors upon onboarding or subscription.

Employees and interns acknowledge receipt of the Company's Compliance Manual upon joining, which includes the GDPR policy. The processing of their personal data is necessary for the performance of the employment (or internship) contract. Furthermore, for employees, signing the employment contract constitutes notice regarding the processing of their personal data.

Regarding job (or internship) applicants who voluntarily contact the Company via the Contact mailbox, they have access to this same procedure available on the Company's website, which is specifically notified to them via an automatic email reply.