ALMA CAPITAL

POLICIES/ PROCEDURES

Subject:	Personal Data Protection Policy

Owner: Compliance

Approved by:	Board of Directors	Date:	22/07/2025

I. INTRODUCTION

Alma Capital Investment Management S.A. (hereafter "ACIM" or the "Company")) is a Luxembourg-based management company, authorized and regulated by the CSSF, subject to Chapter 15 of the UCI Law of 17 December 2010, and to chapter 2 of the AIFM Law of 12 July 2013 as amended. ACIM is the management company for UCITS and alternative investment funds or sub-funds (the Funds).

Under the freedom of establishment and freedom to provide services in another Member State of the European Union, ACIM has established a branch in France, Alma Capital Investment Management, French branch (the "French Branch"), authorized by the *Autorité des Marchés Financiers* (AMF).

Following the Brexit, ACIM has established a subsidiary in the United Kingdom, Alma Capital London (the Subsidiary), authorized by the Financial Conduct Authority (FCA) to manage UCITS funds. This Subsidiary is fully owned by ACIM and only performs activities that are linked to the funds managed by ACIM (mostly portfolio management and distribution). Also, the Board of Directors of ACL has acknowledged that all policies and procedures applicable to ACIM should also be applicable to ACL, considering that ACL employees only work for ACIM benefits.

This Policy therefore applies to ACIM, including its French Branch, and to its Subsidiary. References in this Policy to "Alma" or the "Company" includes its French Branch and its Subsidiary.

This procedure describes the Data Protection Policy in place within Alma, and will apply to all of the Personal Data of all categories of Data Subjects (investors, suppliers, prospects, customers, staff, etc) as processed by the Company.

II. BACKGROUND AND DEFINITION

ACIM is subject to the European Regulation 2016/679 (as amended or replaced from time to time) ("GDPR") and to all local laws and regulations relating to the processing of personal data and privacy applicable to its respective Funds (together the "Data Protection Law") which apply to all data collected by the Company in the course of their daily business and activity. In this context, this Policy may be supplemented by any separate personal data protection policy applied to the Subsidiary or to any of the respective Funds, providing more specific personal data protection process related to obligations of such non-Luxembourg entities.

GDPR describes how undertakings must collect, process, store and destroy Personal Data. The protection afforded by this regulation applies to the Personal Data of natural persons, regardless of whether data is stored electronically, on paper or on other material.

Under Article 24(1) of the GDPR, ACIM as a data controller should implement an appropriate data protection policy as part of the organizational and technical measures it puts in place to demonstrate compliance with the GDPR ("Data Protection Policy").

This Data Protection Policy furthermore applies to:

- all employees working for Alma;
- all agents working on behalf of Alma;
- all other persons who perform activities on behalf of Alma (such as non-executive Directors, contractors, suppliers, etc.).

This group of individuals working for or performing activities on behalf of Alma will be defined as "Staff" within this Data Protection Policy.

All capitalised terms that are not defined in this Data Protection Policy will have the meanings given to them under the GDPR.

III. DATA PROTECTION POLICY

a. Governance, Policy Review And Ownership

The Board of Directors of ACIM has ultimate responsibility for ensuring that the Company complies with their obligations under Data Protection Law.

Taking into account the circumstances in which a data controller must appoint a Data Protection Officer as set down in Article 37 of the GDPR, the Board has determined that it is not currently necessary to appoint a Data Protection Officer. The Board shall keep this matter under review and should guidance emerge which indicates that ACIM should appoint a Data Protection Officer or should the processing conducted on behalf of ACIM change so as to fall within the scope of Article 37 of the GDPR, ACIM will re-consider the need to appoint a Data Protection Officer.

The Management of ACIM will designate a person having primary responsibility for ensuring compliance with this policy within its Compliance Department based on professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil his/her tasks within Alma (the Designated Person). Main roles and responsibilities of the Designated

Person are detailed below. Also, when needed, they are further detailed in each of the relevant sections of this policy:

- Ensure that the Company is at all time in line with all legal and regulatory requirements and best practice in terms of GDPR, by reviewing and being alert of any new requirement issued by authorities, and review internal policies and procedures to ensure they are in line with those requirements;
- Ensure guidelines provided to the Staff are well communicated, understood and adequately applied by all employees;
- Be responsible for the completion and the update of the Data Register (as defined below) based on collection of information from the Staff;
- Remain always reachable to all Staff who would need instruction, advice, clarification on the applicable rules and what should be done on specific matters;
- Discuss with the Management of ACIM any improvements that would need to be

made within the firm to enhance the quality of data protection;
- Report to the Management of ACIM in case of any breach noted and escalate with the Management of ACIM a plan to ensure authorities are made aware, should this be required.

The Company shall ensure that the Designated Person has the necessary resources (e.g. time, equipment, and information) at his/her disposal to carry out his/her responsibilities properly.

The Designated Person is allowed to have other functions within the Company provided that these functions do not give rise to conflicts of interest. The Designated Person cannot, for example hold a position within the organization that leads him or her to determine the purposes and the means of the processing of personal data.

The Designated Person shall directly report to the Management of ACIM. Consequently, the Designated Person cannot be held personally responsible in case of non-compliance with GDPR. Data protection compliance remains a corporate responsibility of the Company.

This Policy is therefore owned by the Board collectively, with the Management of ACIM, the Compliance Department and the Designated Person.

The Company will inform the Staff of the name and contact details of the Designated Person to ensure that this function is known within the organization.

The Management of ACIM will evaluate on a yearly basis whether the activities of the Designated Person are sufficient and whether they:

- are in accordance with the relevant rules and regulations;
- include all existing processes handling personal data within the Company;
- are in line with the ACIM's risk profile.

If certain changes must be made, the Management of ACIM must ensure that a remediation plan is set up in a timely fashion.

IV. DELEGATION AND SERVICES EXTERNALIZATION

Alma has delegated or externalized certain tasks (central administration, domiciliation, record keeping, brokerage, investment management, payroll, tax, among others) to external service providers (the "Service Providers"). While remaining responsible for the treatments carried out in the context of its activities, Alma as "data controller", has specifically delegated to the Service Providers the implementation and monitoring missions of the data protection regulations for the Company.

Data Processing Agreements

Alma must ensure at all times that it is in compliance with Article 28(3) of GDPR and therefore that it enters into a written agreement with any Service Provider or other data processor of Alma in order to impose the specific obligations set down in Article 28(3) of the GDPR on the relevant Service Providers. In performing their obligations under their contracts with Alma, each Service Provider may process personal data on behalf of Alma and accordingly constitutes a "data processor" of Alma.

Right of Audit and Inspection

Under its agreement with the relevant Service Provider, Alma shall have a contractual right to obtain all relevant information from that Service Provider which is necessary in order for the Service Provider to demonstrate its compliance with the data protection obligations set down in the contract. Furthermore, Alma shall have the contractual right to carry out an audit or inspection of the relevant Service Provider for such purposes. The results of any such audit or inspection will be retained by Alma who may require the relevant Service Provider to take specific actions following completion of the audit.

Due diligence performed on Service Providers

When contracting with a third party data processor, Alma shall conduct appropriate due diligence both at the outset of the relationship and on a periodic basis. The due diligence shall seek to ensure that the third party data processor is capable of complying with the requirements of the written agreement as detailed below.

In particular, Alma shall seek to obtain sufficient guarantees that the relevant Service Provider will implement appropriate technical and organizational measures to ensure that the processing conducted by such Service Provider will meet the requirements of the GDPR.

While performing the initial and ongoing due diligences on such Service Providers, the Designated Person will always ensure that such Service Provider has implemented procedures to ensure they are performing, at a minimum, the specific tasks listed below:

- determining the purposes and means of all processing operations concerning personal data as carried out by Alma;
- monitoring of compliance with GDPR, other EU or member state data protection provisions and with the policies of data processors;
- keeping track of developments in the field of data protection and, if necessary, introducing changes to the policies or procedures to keep all documentation up to date;
- establishing a risk based approach with respect to the processing operations;
- ensuring that the necessary awareness is created within the organization and ensuring that the staff receives the necessary periodic training relating to data protection and developments in the field of data protection;
- maintaining and regularly updating the record of processing operations under the responsibility of Alma;
- developing and maintaining procedures relating to the rights of Data Subjects and ensuring that any requests are handled in accordance with such procedures;
- providing advice and assistance to Alma when carrying out a data protection impact assessment;
- notifying and following up on personal data breaches and, if required, introducing changes to policies or procedures in order to prevent similar breaches in the future;
- acting as a point of contact for internal (employees) or external (investors, board members, shareholders, contractors, suppliers, etc.), and cooperate with the relevant national data protection authority.

Notwithstanding the delegations as mentioned above, Alma remains responsible for the treatments carried out in the context of its activities.

V. PERSONAL DATA

"Personal data" includes any data which relates to a living individual who can be identified:

- from that data; or
- from that data and other information which is in the possession of Alma.

Alma only holds personal data which is directly relevant to its dealings with a given Data Subject. That data will be held and processed in accordance with the Data Protection Law and this Policy.

Processing personal data includes any operation that is carried out in respect of personal data, including, but not limited to, collecting, storing, using, recording, disclosing, transferring or deleting personal data.

In the framework of our activities/services, it may be necessary for us to process this kind of data which may notably include (i) identification details such as your name, surname, date and place of birth; (ii) contact information such as your email address, domicile address or phone number; (iii) any other relevant personal details such as your nationality and citizenship; (iv) government identification numbers such as a copy of your ID card; (v) sound recording; (vi) financial and banking information.

Personal data collected by Alma is generally collected in order to:

- manage and administer shareholdings in Alma or in the Funds;
- comply with legal, tax or regulatory obligations imposed on Alma or on the Funds under applicable law;
- efficiently manage its directors and designated persons and its relationship with its Service Providers;
- conduct marketing efforts and quality control;
- provide customer service, training and related purposes;
- track fees and costs;
- carry out statistical analysis and market research; and
- transfer personal data to third parties such as auditors, regulatory or tax authorities and technology providers in the context of the day to day operations of the Company.

VI. MAIN PRINCIPLES

As a controller of personal data, Alma is bound to certain key principles as how to handle this information during the different stages of the data processes. These key principles relate to:

1. The Collection Of Personal Data

Personal Data can be generally defined as any information relating to an identified or identifiable natural person ("Data Subject").
As a controller of Personal Data, Alma should only process data that is collected for specific, explicit and legitimate purposes. Processing may not take place for purposes other than those that have been specified. The Personal Data collected should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The different categories of Personal Data are set out in the register of processing activities (the Data Register). This will be performed based on information collected from the Staff, in contact

with Personal Data collected, including the Human Resource department regarding Personal Data on employees of Alma.

Prior to the drawing up of the Data Register, ACIM has ensured that it is sufficiently aware of all data flows and that it knows where all Personal Data is being stored.

The Company shall know, be aware and remain aware of:

- The origin of the Personal Data collected;
- The (categories of) Personal Data collected;
- The (categories of) Data Subjects;
- The (categories of) recipients of Personal Data, including recipients in third countries;
- Transfer of Personal Data to third countries.

In the framework of the collection of Personal Data, the Company should also be able to clearly indicate in each processing situation which ground for processing it invokes:

Legal obligation

Where the processing of Personal Data is carried out in accordance with a legal obligation to which Alma or the Funds is subject, the processing should have a basis in Union law or local law.

E.g. when carrying out its activities, Alma should collect certain personal information of its clients

in the framework of the anti-money laundering legislation.

Performance of a contract

Where the collecting and the processing of Personal Data is necessary for the performance of a contract to which the data subject is party, the processing is lawful.

Processing information

Alma should be able to demonstrate that the data subject has been informed of the processing of his or her Personal Data. An e-mail disclaimer inserted in electronic signature of each member of the Staff, clearly and expressly informs the Data Subject on the collection, use and process of their Personal Data received by any mean.

Legitimate interest

In accordance with Article 6(1)(f) of the General Data Protection Regulation (GDPR), the Management Company may rely on legitimate interest as a legal basis for the processing of personal data, where such processing is necessary for the purposes of the Company's legitimate interests or those of a third party, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subjects.

To ensure compliance and accountability, the Company commits to conducting a Legitimate Interest Assessment (LIA) before relying on legitimate interest as a legal basis. The LIA includes the following three steps:

- Purpose Test – Verifying that the processing is necessary and proportionate to achieve a clearly defined legitimate interest.
- Necessity Test – Evaluating whether the processing is essential and whether less intrusive alternatives are available.
- Balancing Test – Assessing whether the data subject's rights and interests override the legitimate interest pursued, taking into account the nature of the data, context of processing, reasonable expectations of the data subject, and potential impact.

The LIA is documented and reviewed periodically or when material changes to the processing activity occur.

This approach is in line with the European Data Protection Board (EDPB) Guidelines 1/2024 on processing personal data under Article 6(1)(f) GDPR, and supports the Company's accountability obligations under Article 5(2) GDPR.

2. The Storage Of Personal Data

Personal Data should be stored in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

As detailed above, Personal Data are saved in secure folders in the server , to which only the Compliance Department and the Human Resources staff, the Management of ACIM and Directors of ACIM have access.

3. The Use Of Personal Data

Given the fact that Alma shall only process data that is collected for specific, explicit and legitimate purposes it also engages itself to only use this limited information when providing its services.

4. The Transfer Of Personal Data

Alma shall ensure that it is at all times aware where (in which country) Personal Data is stored.

a. Transfer of Personal Data to a member country of the European Economic Area (EEA)

Personal Data may be freely transferred between countries in the EEA if the Company still knows where such Personal Data is stored at all times.

Alma may transfer – within the EEA – personal information to the following undertakings or organizations:

- To affiliated companies

Alma may have a legitimate interest in transmitting Personal Data to an affiliated company for internal administrative purposes, including the processing of clients' or employees' Personal Data.

No client data should be transmitted to affiliated companies, unless this is necessary for administrative purposes.

- To public organizations

The Company may furthermore be required, given legal obligations, to provide Personal Data to public organizations, such as e.g. any regulatory body or any social security organization.

- To third parties

The Company may need to transmit client, prospect or employee data to a third party, e.g. in a contractual relationship for services provided to Alma.

Alma will at all times ensure this transmitting of data is preceded by the necessary and appropriate data protection clauses including non-disclosure agreements. Alma will expect the same level of assurance of these third parties with regards to the handling of personal data, as Alma expects from its own staff.

b. Transfer of Personal Data to third countries (outside the EEA)

In case of transfers of Personal Data to other undertakings or organizations or branch located in third countries (outside the EEA), appropriate measures should be taken to ensure that the level of protection as required according to GDPR standards is not undermined. To ensure that personal information does receive an adequate level of protection, it is transferred outside the EEA on the basis of a Data Transfer Agreement.

5. The Access Restriction To Personal Data

In case Personal Data becomes no longer necessary for the regular day-to-day activities of the Company, the access to these Personal Data will be restricted.

6. Data Subject Rights

Alma ensures that Data Subjects can effectively exercise their rights in respect of their Personal Data, which include the right of access, rectification, erasure, restriction of processing of data and a right to object to processing.

These rights could be exercised by writing to the following address: compliance@almacapital.com. The request will be processed immediately.

Dealing with Data Subject Requests

Alma expects that any Data Subject requests made by a shareholder of the Funds will be made directly to Transfer Agent (TA). A specific procedure is implemented by each TA to ensure, when relevant, that such request is forwarded to the Designated Person.

Any Data Subject request made by a director will be made to the Chairperson of the Company and shall be forwarded to the Designated Person for action.

Any Data Subject request made by an employee will be made directly by the employee to the Designated Person for action.

Should any person be dissatisfied with the processing of his/her Personal Data or wish complaining about it, please refer to the Complaints handling procedure published on the website:

https://www.almacapital.com/documentation/

Any Data Subject has a right to lodge a complaint with the competent supervisory authority, being in Luxembourg the *Commission Nationale pour la protection des données* (CNPD).

7. Responsibility

Everyone who works for or with Alma has a responsibility for ensuring that data is collected, processed and stored appropriately. Each team handling identifiable Personal Data must therefore ensure that this information is handled in line with this Data Protection Policy and data protection legislation and principles.

Notwithstanding the above, certain employees / management directors within Alma have key areas of responsibility (next to these of the Designated Person as discussed earlier in this policy):

- The Management of ACIM

The Management of ACIM shall ultimately be responsible for all issues relating to data protection and compliance with the applicable laws. The Management of ACIM shall sign off on any decisions that are to be made and documents that are to be drafted. In addition, the Management of ACIM shall ensure that its organization is on track when it comes to data protection issues.

- Compliance Department

ACIM Compliance is notified by the Designated Person in cases where the customer's request in relation to his Personal Data could lead to a complaint or damage the reputation of the Company. As part of second-line controls, Compliance has access to the 'incident' register on request. In general, Compliance ensures compliance with the procedure.

8. Data Protection Impact Assessment ("Dpia")

Where a certain processing procedure could lead to a high risk to the rights and freedoms of individuals, a full risk assessment needs to be ensured by Alma as a data controller.

A DPIA is not required where:

- the nature, scope, context and purposes of the processing are very similar to processes for which a DPIA has been carried out. In such cases, results of a DPIA for similar processing can be used; and
- the processing operation has a legal basis in Luxembourg (under certain circumstances).

The Designated Person will be establishing a risk assessment with respect to the processing operations.

9. Breach Of Data

Notification process

Under its contracts with the relevant Service Provider, Alma must be notified of any Personal Data Breach (as that term is defined in the GDPR) without "undue delay" after the Service Provider becoming aware of the Personal Data Breach.

All such Personal Data Breaches must be reported to the Board of Directors of ACIM and to the Designated Person who will act as the relevant contact for the incident and will ensure that all relevant information relating to the breach, including the details or the incident, root cause analysis and corrective and preventative action is provided by the relevant Service Provider so as to be able to investigate the incident and determine (i) whether a breach has taken place, (ii)

possible consequences for Data Subjects (iii) what remedial action is required and (iv) whether the Data Subjects and/or the should be notified

If considered necessary, the Board of Directors of ACIM shall convene a board meeting in order to consider the Personal Data Breach further.

Immediate Notification to the CNPD of Data Protection Breaches (where applicable)

The Company must report all relevant Personal Data Breaches to the relevant authority such as the CNPD no later than 72 hours after becoming aware of the Personal Data Breach. If a report is not made within 72 hours then an explanation as to the delay needs to accompany the report.

The Company is not required to report any Personal Data Breach to the CNPD which is unlikely to result in a risk to the rights and freedoms of the relevant Data Subjects. In the event that the Company, taking into account the relevant circumstances, determines that it is not necessary to notify the CNPD of the relevant data protection breach, a full record of the circumstances relating to the breach and the rationale for determining why such notification was not required shall be documented and maintained by the Company.

Notification to the Data Subject

The Board will make an assessment regarding notification of a Personal Data Breach to affected Data Subjects taking into account the criteria set down in Article 34 of the GDPR. The Board will then determine whether affected Data Subjects need to be informed of the Personal Data Breach, and where applicable, will instruct the Designated Person to prepare a notice to Data Subjects.

Logging Issues and Breaches

ACIM maintains a central log for all Personal Data Breach and issues which is maintained by the Designated Person. This is set out in Appendix.

VII. PUBLICATION

The Data Protection Policy will be made available for all Staff.

This Data Protection Policy will be evaluated on a regular basis by the Management of ACIM (with the Designated Person and the Compliance Department) and will be adjusted where necessary. Substantial changes to this policy will be announced internally.

VIII. MONITORING AND EVALUATION

ACIM checks whether Personal Data which has been processed within Alma is handled in accordance with the principles of this Policy. This evaluation will be performed on three levels within ACIM:

- Monitoring at the level of the Designated Person

The Designated Person will perform regular checks as regards the compliance with the principles as included in this Data Protection Policy.

- Monitoring at the level of Compliance Department

The Compliance department will monitor compliance of the relevant departments with this Data Protection Policy. Checks will be performed following a risk-based approach, e.g. by means of random checks of the prospect database.

- Periodic audit

Data Protection will be one of the themes within the scope of the internal audit universe and will be assessed in the context of internal audit activities.

Appendix: Personal Data Security Breach Log

Personal data security breach log							Effective Date [x],			
Details of breach								Measure taken / to be taken		
No.	Date of breach	No of people affected	Nature of breach	Description of breach	How breach was identified	Description of data	Consequence of breach	All individuals informed?	Remedial action	CNPD Informed