Privacy policy

Arcona Capital Fund Management B.V.

Version:	By:	Action:	Material changes:	Adopted by the Board:
1.0	H. Visscher	Review	Yes	12 May 2021
1.0	Charco & Dique	Review Q2 2022	No	Not applicable
2.0	C&D | M. Blokland Maaike de Mol	Review 2023 English translation	Yes	21 March 2024 18 April 2024

1. Purpose

Arcona Capital Fund Management B.V. (hereafter referred to as **ACFM** or the **Management Board**) processes personal data in its business processes. This includes personal data of participants, UBOs, employees, applicants, and suppliers (hereafter referred to as **Personal Data**).

ACFM considers it of importance that Personal Data are handled carefully and treated confidentially. The processing of Personal Data should be done with the utmost care to prevent damage due to misuse to participants, UBOs, employees, applicants, and suppliers and ACFM itself.

This policy document sets out how ACFM fulfils the rights and obligations under the General Data Protection Regulation (2016/679/EC, hereafter **GDPR**) and related laws and regulations on the protection of Personal Data.

2. Scope and Governance

This policy applies to any processing of Personal Data by ACFM.

The Management Board is responsible for (the implementation of) the policy. The policy is evaluated periodically but at least every two years or if warranted, and revised if necessary. The Compliance Officer (hereafter CO) ensures that actions are taken in accordance with the policy and the laws and regulations relating to this subject.

ACFM has not appointed a privacy officer. These duties have been assigned to the CO. The CO informs and advises on the obligations arising from the GDPR and monitors compliance with this regulation and other laws and regulations on the protection of personal data. The CO has an advisory role in carrying out privacy impact assessments (hereafter PIA).

The CO performs at least the following tasks:

- Inform and advise the Management Board and employees of ACFM on their obligations regarding the obligations under the GDPR and other laws and regulations regarding the protection of Personal Data;
- Oversee compliance with the GDPR, other laws and regulations on the protection of Personal Data and the policy on the protection of Personal Data, including the assignment of responsibilities, awareness and training of staff involved in the Processing
- Cooperate with the Personal Data Authority and other regulators; and
- Contact for the Personal Data Authority in direct consultation with the Executive Board.

3. Definitions

Data Subject: any natural person whose personal data are processed.

Personal Data: any information relating to an identified or identifiable natural person ("the Data Subject"). An identifiable person is any natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more elements characterising the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

Processing: an operation or set of operations involving personal data or a set of personal data, whether or not carried out by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of data.

Processor: a natural or legal person, a public authority, a service, or another body that processes personal data on behalf of ACFM.

Controller: the natural or legal person (in this case ACFM), public authority, agency, or other body which alone, or jointly with others, determines the purposes and means of processing personal data.

Register: the register of processing referred to in article 30 of the GDPR.

CDD: Client Due Diligence

4. Principles of Processing Personal Data

The processing of Personal Data is governed by the following principles:

Lawfulness: Processing of Personal Data is lawful (i.e. takes place only for purposes that can be based on one of the legal bases given in the GDPR).[1]

Fairness and Transparency: Processing of Personal Data is proper and transparent.

Purpose limitation: Personal Data is collected for specified, explicit and legitimate purposes and is not further processed in incompatible ways.

Data minimisation: Personal data are adequate, relevant, and limited to what is necessary for the purposes for which they are processed.

Correctness: Personal data is accurate and will be deleted or rectified if necessary.

Storage limitation: Personal Data will be retained in a form that does not allow for the identification of data subjects for longer than is necessary for the purposes for which the Personal Data are retained.

Integrity and confidentiality: Personal Data will be processed by appropriate technical or organisational measures in a manner that ensures appropriate security.

[1] See Articles 5 and 6 of the GDPR for lawfulness and the bases to be distinguished (including performance of contract, legal obligation or consent of the Data Subject).

Accountability: Personal Data are processed under the responsibility of ACFM which ensures and can demonstrate that processing complies with the provisions of the GDPR.

4.1 Application Principles of Processing Personal Data

The principles of Personal Data Processing are applied at ACFM in the following ways.

Lawfulness: Exclusively those Personal Data are requested by ACFM from Data Subjects that are required by law for identification purposes and that enable ACFM as investment fund manager to conduct business transactions with the Data Subject.

Fairness and transparency: CDD employees shall inform Data Subjects why Personal Data is requested and also the consequences if the Personal Data is not provided by the Data Subject. For example, failure to provide Personal Data may result in ACFM not being allowed to do a payment because the Data Subject(s) or heirs of Data Subject(s) cannot be identified.

Purpose limitation: When Personal Data is requested, the purpose for which the Personal Data will be used is stated. The Personal Data will be processed only for the defined purpose. Personal Data are mostly requested due to legal obligations arising from the Anti Money Laundering / Combating the Financing of Terrorism (hereafter **AML/CFT**).

Data minimisation: CDD employees clearly indicate which specific Personal Data they need to comply with legal requirements. In addition, they also indicate which information can be withheld. Employees request only the Personal Data of Data Subject(s) required by law, applying the principles of necessity, proportionality, and subsidiarity. For example, it often happens that a Data Subject has passed away and ACFM needs to identify the heirs before proceeding with distribution. Initially, internal consultations are carried out to determine whether the heirs' details have not already been communicated in previous correspondence (subsidiarity). If this is not the case or the data is not complete, then it is determined what information is legally required before approaching the Data Subject (necessity and proportionality).

Correctness: Data Subjects themselves have the responsibility to inform ACFM about changes in their Personal Data. Additionally, CDD employees are also actively engaged in retrieving Personal Data if they turn out to be incorrect, for example when (news) letters are returned or e-mails are not received. Incorrect Personal Data is immediately removed and/or updated to the actual data in a shared file.

Storage restriction: outdated Personal Data in the client file are immediately deleted and replaced by the actual Personal Data if a data subject makes a change to the current data.

Integrity and confidentiality: Personal data in digital form is technically secured by access codes and can only be accessed by employees with a relevant function such as CDD analysts. Furthermore, hard copies are kept securely behind closed doors. Further details about the security of Personal Data at ACFM can be found under chapter 8 i.e. Security and Other Management Measures.

Accountability: Multiple measures are taken to ensure that legal requirements from the GDPR are met throughout the data processing process and all parties involved in it. ACFM is supervised by the Authority Financial Markets (hereafter **AFM**). In addition, ACFM has an external Compliance Officer who, together with the CO, monitors that the processing of Personal Data complies with the requirements of the GDPR.

5. Special categories of Personal Data

Special categories of Personal Data are extra-sensitive data such as racial and ethnic origin, political opinion, religious beliefs, trade union membership, health, sexual orientation, and criminal convictions.

In general, special categories of Personal Data may not be processed unless a specific exception applies. This varies for each category of special Personal Data.

Personal Data of a criminal nature (including a VOG) may be processed with the explicit consent of the Data Subject.

The Citizen Service Number (hereafter **BSN**) may only be used for the implementation of the relevant law or for the purposes stipulated by law. ACFM does not request BSN numbers from its business relations. BSN numbers are only processed for the purpose of processing the salary data of personnel and commissioners in office of the funds managed by ACFM. Also, BSN numbers are processed in the Insiders List under the *Market Abuse Regulation*, hereinafter the **MAR**).

From September 2023, identity documents and passports will no longer be stored, digital nor in hard copy. The relevant ID data for the CDD investigation will be stated in an overview, after which the identity cards and passports will be permanently deleted from the servers.

6. Register

The CO maintains a register listing the processing activities for which ACFM is responsible. The register shall contain:

- A description of the categories of Data Subjects and categories of Personal Data;
- The processing purposes;
- The categories of recipients to whom Personal Data has been or will be disclosed, including recipients in third countries or international organisations;
- If applicable, transfers of Personal Data to a third country or international organisation. This will also include the documents on appropriate safeguards;
- The intended time limits for erasing the different categories of data;
- A general description of the technical and organisational security measures.

If the processing activity changes, the Register must be updated accordingly. The CO monitors the content of this Register.

The Register does not store the actual Personal Data of Data Subjects. The Register only provides insight into the Processing Activities through a description. The Register therefore contains a description of the Processing Activities and not the Personal Data itself.

7. Rights of Data Subjects

Right to information about the Processing

If Personal Data are obtained from the Data Subject, information should be provided on the following topics, if requested**:**

- The foundation of the Processing;
- The Processors, and if applicable the intention to share the Personal Data outside Europe;
- The retention period (or provision thereof) and on the Data Subject's other rights (see further below, as well as indication of right of withdrawal, right of complaint); and
- The other purposes of use, if any.

The abovementioned information need not be provided if the Data Subject already has this information.

If the Personal Data was not obtained from the Data Subject itself, the Data Subject will be provided with the following additional information:

- The source from which the data came and whether this source is public;
- If the Personal Data are processed for another purpose, the Data Subject will also have to be provided with the above information.

Again, the information does not have to be provided if the Data Subject already has the information, if providing that information proves impossible or would require disproportionate effort or if the Personal Data must remain confidential.

Right of inspection: The Data Subject has the right to inspect.

Right to restrict Processing: The Data Subject has the right to have his/her Personal Data restricted in a Processing.

Upon receiving a request to this effect, it should be determined in each case whether it can be carried out on legitimate grounds.

Right of portability (data portability): The Data Subject has the right to obtain and transfer the Personal Data relating to him/her that he/she has provided to ACFM in a common form. In such a situation, the Data Subject will receive all data and will transfer it to another Controller or entity collecting Personal Data.

Right to object: The Data Subject has the right to object to the Processing of Personal Data concerning him/her. Upon receiving a request to that effect, it should be determined in each case whether it can be carried out on legitimate grounds.

Right of rectification and erasure of data: The Data Subject has the right to have his/her Personal Data rectified or erased. Upon receiving such a request, it should be determined in each case whether this can be carried out on legitimate grounds.

The GDPR has a notification obligation in case of rectification or erasure of data, and in case of processing restrictions; any recipient to whom Personal Data has been disclosed must be notified of any rectification, erasure of Personal Data or restriction of Processing, unless this proves impossible or requires disproportionate effort.

7.1. Handling requests from the Data Subject

ACFM will comply with the Data Subject's rights as soon as possible and provide information on how the request has been complied with within four weeks of receiving the request at the latest. Depending on the complexity of the requests and the number of requests, this period may be extended, if necessary, by a period of two additional months. Compliance with the Data Subject's request shall be free of charge unless the request is ungrounded or excessive. In the latter case, the request may also be rejected for that reason.

In case of uncertainty as to the identity of the natural person making the request, additional information may be requested to confirm the identity of the Data Subject.

7.2. Complaints and compensation

The Data Subject has the right to file a complaint with the Personal Data Authority if he/she believes that the Processing of his/her Personal Data did not comply with the GDPR.

The Data Subject may be entitled to compensation for damages suffered if his/her Personal Data is breached.

8. Security and other control measures

For each Processing of Personal Data, appropriate technical and organisational management measures as described in the Register shall be observed, taking into account the risks of the processing. The appropriate technical and organisational management measures are periodically evaluated and updated where necessary. During the weekly CDD consultation, the processing and storage of (new) Personal Data is discussed. Consultations are held with the IT manager (I&O Netsys) on need-based Personal Data protection.

With regard to any new Processing or for any change in the Processing of Personal Data, the probability (likelihood) and impact (severity) of the risks of the Processing on Personal Data are determined beforehand, during and afterwards. For risks to the rights and freedoms of Data Subjects that are assessed as high, privacy impact assessments (PIA, also known as data protection impact assessments) are carried out. If it is decided that no measures are taken to mitigate the risks, the Personal Data Authority must be consulted prior to the Processing.

The control measures include security of equipment, access security, information security, awareness, including prevention of unauthorised access to or use of Personal Data and the equipment used for the Processing. In addition, laptops are made secure and only the IT administrator may download or edit programmes with the permission of the contact person at ACFM.

Personal Data collected in hard copies are located in locked cabinets in a room that is locked by (CDD) employees after working hours every day. There are three employees who have keys to this room. This room is located in the office building after the front door and the alarm system.

There is a confidentiality obligation regarding the protection of Personal Data which is known to ACFM employees. When developing new applications, Data Subjects are taken into account and alternatives that are least objectionable to them are chosen according to the principles of 'privacy-by-design' and 'privacy-by-default'.

Employees have access to Personal Data on a need-to-know basis. This means that employees only have access to Personal Data when they need it to perform their duties by virtue of their position. For example, Compliance and/or CDD employees have access to a Compliance folder and data specifically for their work. Asset Management employees, on the other hand, do not have access to a Compliance folder, but rather other files and folders tailored to their work. In addition, to add folders and files on an employee's computer, the IT administrator needs the written permission of one the Board members of ACFM, allowing management to carefully coordinate which employee has access to which folder.

8.1. Data Retention

Personal Data must not be kept longer than is strictly necessary for the purpose for which it was collected. The data retention overview sets out for each category of Personal Data after which time they must be destroyed. ACFM sees to it that agreements are made with outsourcing partners or other business relations who have access to Personal Data about processing Personal Data, which are laid down in processing agreements. Processor agreements have been signed for a number of ACFM's service providers.

9. Transfer of Personal Data to third countries

Personal Data is stored on Sharepoint. Sharepoint concerns a Microsoft platform. Microsoft has several data centres around the world, including 14 within Europe. Personal Data is in most cases stored at the two geographically closest data centres to limit the impact of a natural disaster or service outage. The closest data centres are located in the Netherlands, France or Germany.

ACFM's data is therefore stored on servers within the European Union (hereafter **EU**), obliging Microsoft to apply the EU-US privacy shield framework.[2] This means that Personal Data can be securely shared between the EU and companies in the United States that adhere to the Data Privacy Framework.

If Personal Data is transferred to countries outside the EU (third country or international organisation), similar rules must be complied with as for the protection of Personal Data in the Netherlands/EU. ACFM will only transfer Personal Data in the event of an adequate level of security.

10. Duty to report data breaches

In the event that Personal Data of Data Subject(s) has been unknowingly or unlawfully leaked (data breach), the Personal Data Authority must be notified within 72 hours from the time of detection, if the breach is expected to pose a high risk to the rights and freedoms of natural persons. In addition, a duty may arise to notify the Data Subject of the breach.

[2] https://blogs.microsoft.com/eupolicy/2022/03/25/eu-us-data-agreement-an-important-milestone-for-data-protection-microsoft-is-committed-to-doing-our-part/