C WorldWide Fund Management S.A.

Privacy & Confidentiality policy

2026

Version 8

Date of approval	Version	Update	Author	Approved by
11/2018	Version 1	First version	Compliance function	Conducting Officers
02/2019	Version 2	General update, data breaches, – Layout adjustment	Compliance function	Conducting Officers
6/10/2020	Version 3	Inclusion of the Danish Branch – update of sources of personal data, categories of personal data, purpose of processing personal data and other general updates	Compliance function	Conducting Officers
04/12/2020	Version 3.1	Inclusion of the details concerning data transfer by RBC	Compliance function	Conducting Officers

7/09/2022	Version 4	General update, Notification process, lodging process for complaints	Compliance function, and person responsible for GDPR	Conducting officers
06/11/2023	Version 5	General update, removal of the mentioning of RBC Investor Services Bank and replacement by BNYM	Compliance function, and person responsible for GDPR	Board of Directors
12/06/2024	Version 6	Inclusion of review frequency and Personal Data Processing Register in Appendix 2	Compliance function, and person responsible for GDPR	Board of Directors
18/06/2025	Version 7	General update, annual review	Compliance function, and person responsible for GDPR	Board of Directors
03/09/2026	Version 8	Inclusion of: - Definitions, - Legal basis - Lawful grounds - Processing - Retention policy details - Section related to ROPA and DPIA and update of the register - Sanctions - Information to data subject - Privacy - Responsibilities of the Controller	Compliance function	Board of Directors

Contents

1. Definition and abbreviations

Terms	Definition
Consent	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 PD relating to him/her, art. 4 XI GDPR
Controller	The natural or legal person (…) which, alone or jointly with others, determines the purpose and means of the processing of PD, art. 4 VII GDPR. Joint Controller must define and disclose the relationship against the data subject.
CWW Group	C WorldWide Group
CWFM/ManCo/Management Company/Company	C WorldWide Fund Management S.A.
Data Subject	An identifiable natural person is one 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 factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person, art. 41 GDPR
Data Subjects' rights	Right to demand that the controller provide access to, rectify or erase personal data or to limit processing involving the data subject, or right to object to processing and right to data portability
DR Processing	Any operation or set of operations which is performed on PD or on sets of PD (gathering, storage, use, alteration, distribution, deletion/destruction of PD)
DPIA	Data Protection Impact Analysis
DPO	Data Protection Officer
GDPR	EU Regulation 2016/679/EU dated 27 April 2016 on protection of natural persons with regards to the processing of personal data
Group	CWW Group
ROPA	Record of Processing Activities – Mapping of all Processing Activities of CWFM and its Processors
CNPD	Commission National Protection des Données
Personal Data/PD	Any information relating to data subject, Art. 4 I GDPR. This includes all data directly or indirectly linkable to a data subject like name, address,

	national identification number, health related data, e-mail address, telephone number, political opinion, bank account number, etc.
Processor	A natural or legal person (…) which processes PD on behalf of the Controller, Art. 4 VIII GDPR
Processing/Data processing	Any operation or set of operations which is performed on PD or on sets of PD (gathering, storage, use, alteration, distribution, deletion, destruction of PD)
Recipient	The individual, legal entity, public authority, service or other body which receives personal data, whether a third party or not
Registrar and Transfer Agent/BNYM	The Bank of New York Mellon SA/NV Luxembourg branch

2. Legal Basis

- EU Regulation 2016/679/EU dated 27 April 2016 on protection of natural persons with regards to the processing of personal data (“GDPR”);
- Luxembourg law dated 01 August 2018 on the Organization of the National Commission for Data Protection and implementation of EU Regulation (EU) 2016/679 ("the Data Protection Act) implementing GDPR
- EU directive 2002/58/EU as amended on protection of personal data and the protection of privacy in the electronic communications sector ("E-Privacy Directive")
- Luxembourg Act of 30 May 2005 on the Protection of Privacy in the Context of Electronic Communications ("ePrivacy Act 200S') transposing the E-Privacy Directive
- Law of 17 December 2010 relating to undertaking collective investment, as amended Law of 5 April 1993 on the financial sector, as amended
- CWW Group Directives

3. Background

The aim of this document is to describe the way C WorldWide Fund Management S.A. and its Danish Branch (**“CWFM”** or the **“ManCo”**) process the personal data concerning individuals as Data Controller, pursuant to Regulation (EU) 2016/679 on the protection of natural persons about the processing of personal data and on the free movement of such data (hereafter also **“GDPR”**).
The purpose of the policy is also the management of risks related to data processing and the avoidance of breaches of the applicable regulatory framework.

4. Processing Personal Data

CWFM may from time to time receive personal information, as described below (the “Personal Data” or “PD”), relating to individuals who are employees, counterparties of the agreements in place, (prospective)

investors, or, in the event a counterparty/investor is not a natural person, information relating to officers, directors, partners, members, representatives, contact persons, agents, persons holding a power of attorney, or the beneficial owners (each a "Data Subject"), and may in that context process Personal Data of the Data Subjects. The term "processing" has the meaning ascribed to it in the Data Protection Laws, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, destruction. Personal Data of the `data subjects` is subject to certain legal safeguards specified in the GDPR. The Data Protection Laws prescribe the way in which the Management Company, the Funds and their service providers may collect, retain and handle Personal Data. CWFM is a controller of the `data subjects' Personal Data for purposes of the GDPR (the "Data Controller"), and will process, or arrange the processing of the Data subjects' Personal Data by service providers.
CWFM is also Processor with regards to Personal Data collected from counterparties other than investors.

Processing activities by CWFM	Possible activities
Collection of PD	Collection from Data Subjects or third party in physical or electronic form
	Recording in physical or electronic form
Storage	(Re-) Structuring
	Storage in physical or electronical fomr
Use	Adaption or alternation
	Retrieval
	Consultation
	Immediate use
	Combination
	Alignment
(Cross border) Transfer	Disclosure of PD by transmission to an adequate jurisdiction and with an implemented lawful transfer mechanism
	Dissemination
Retention & Destruction	Destruction
	Erasure
	Restriction
(Sub-) Outsourcing services (implying a transfer of relevant information to a third party)	Disclosure by transmission

All Processing activities by CWFM must comply with the following key principles:

- Processing must be lawful, fairly and transparent to the Data Subject;
- PD is only allowed to be collected for specific and legitimate purposes;
- PD has to be kept up to date and accurate;
- CWFM avoids or reduces the use of PD whenever it can;
- CWFM will not misuse collected PD for further illegitimate processing.

As CWFM uses Processors, which act on its behalf, it has to ensure in advance that each Processor has implemented appropriate technical and organizational measures to comply with the GDPR.
This compliance-check is part the initial and ongoing Due Diligence of CWFM on the Processors.

Processing activities of CWFM's Processors must be defined in written agreements and contain the following rules:

- Processor acts only on documented instructions of CWFM as Controller;

- Sufficient guarantee of the Processor that technical and organizational measures are implemented to meet the conditions of the GDPR;
- Processor uses no Sub-Processors without previous authorization of CWFM/ the Funds;
- Confidentiality conformation of all persons with access to PD;
- Confirmation of Processing security;
- Assistance to CWFM as the Controller to fulfil its obligations with appropriate technical and organizational measures
- Safeguard data security requirements under Art. 32 GDPR;
- Assist CWFM with notifications to the CNPD;
- Assist CWFM to communicate data breaches to the Data Subject;
- Follow the instructions of CWFM, in particular with regard to exercise the Data Subject's rights;
- Make all information available and allow inspections by CWFM as Controller to demonstrate the compliance with the GDPR;
- Inform the CWFM/ the Funds as Controller about all infringements related to PD;
- Forward all obligations to the Processor's sub-delegates dealing with PD of CWFM/ the Funds;
- Cooperation with the National Commission on information request;
- Keep records about the Processing activities up to date.

a. Source of Personal Data

CWFM collects Personal Data, subject to applicable law, from a variety of sources as follows:

- when employees/management provide data to CWFM. When they apply for a position at CWFM, consequently, when they are hired or appointed to cover specific role and when they perform personal transactions (personal data, extract of criminal records, details on personal transactions performed);
- when counterparties of the agreements in place with CWFM provide personal data to the Management Company. When AML controls are performed on each counterparty or when counterparties are identified;
- when the investor provides data to the fund or CWFM (e.g., where he/she contacts CWFM via email or telephone, or by any other means);
- in the ordinary course of the relationship (e.g., during managing transactions or investment in managed funds);
- through the financial advisor or dealer that intermediates the operation;
- when investor access CWFM website. When he/she visits a site, his/her device and browser may automatically disclose certain information (such as device type, operating system, browser type, browser settings, IP address, language settings, dates and times of connecting to a Site and other technical communications information), some of which may constitute Personal Data.

b. Categories of personal data processed:

- identification data, for example: Name, identification number/social security number, details from the passport such as the passport number, and further information including photograph, date and place of birth.
- contact data (address, telephone number, email address), sample signature;
- bank account details;
- bank statements and payment instructions;
- information relating to the investor’s subscription in the Fund as well as to redemptions, including transactions data;
- proof of the investor’s eligibility to purchase units in the Fund;
- revenues;

- wealth and its source;
- telephonic or electronic recordings; and
- information used in "cookies" and similar technologies on websites, mobile applications and in emails to recognize a Data Subject, remembering the respective Data Subject's preferences;
- extract of criminal records;
- information related to transactions carried out by the employees.

c. Purposes of processing Personal Data

Personal data will be processed for the following purposes:

- managing and administrating holdings of investors in the Fund on an on-going basis; informing investors who wish so, of events such as the general assembly of investors, etc.
- to ensure the ability of CWFM to perform the obligations under the subscription agreement, the Fund's constitutional documentation and further documents which together form the basis of the investor's contractual relationship with CWFM (where applicable), and certain required pre-contractual steps;
- operational purposes and statistical analysis (including behavior analysis for anti-money laundering ("AML") assessment);
- processing certain information about the investor or the investor's directors, officers and employees and beneficial owners (if applicable) in order to carry out AML checks and related actions which CWFM considers appropriate to meet any legal obligations imposed on CWFM relating to the prevention of fraud, money laundering, terrorist financing, bribery, corruption, tax evasion and to prevent the provision of financial and other services to persons who may be subject to economic or trade sanctions, on an on-going basis, in accordance with CWFM's AML policy and procedure. To conduct due diligence, CWFM, or the Registrar and Transfer agent acting on its behalf may also screen against publicly available government and/or law enforcement agency sanctions lists;
- processing certain information about the other counterparties or counterparties' directors, officers and employees and beneficial owners (if applicable) in order to carry out AML checks and related actions which CWFM considers appropriate to meet any legal obligations imposed on CWFM relating to the prevention of fraud, money laundering, terrorist financing, bribery, corruption, tax evasion and to prevent the provision of financial and other services to persons who may be subject to economic or trade sanctions, on an on-going basis, in accordance with CWFM's AML policy and procedure. To conduct due diligence, CWFM may also screen against publicly available government and/or law enforcement agency sanctions lists;
- to report tax related information to tax authorities in order to comply with a legal obligation;
- to update the shareholder/unitholder register of the Funds;
- to update and maintain records regarding subscriptions and / or redemptions in the Fund;
- to provide the investor with information about products and services which may be of interest, and which processing is necessary to perform a relevant contract with the investor;
- to retain AML records of individuals to assist with subsequent screening of them, including in relation to investment in other funds;
- to disclose information to a governmental, tax or regulatory body, financial market, broker or other intermediaries, counterparties, court, auditors or other third parties and to conduct compliance activities, where CWFM considers this to be in the Fund's best interest, or the interest of another person, but where such disclosure is not required by the laws of the European Union member states;
- where this is in the legitimate interests of CWFM to manage and administer the Fund's business and to provide information to its service providers to allow them to comply with their legal and regulatory obligations, especially where these derive from the laws of countries outside the European Economic Area ("EEA");

- to establish, exercise or defend legal claims and in order to protect and enforce CWFM's rights, property, or safety, or to assist the investors in the Fund or others to do the same, and to investigate and respond to any complaints and disputes;
- to ensure that the hiring is made according to applicable professional standing and experience criteria and according to AML requirements as well;
- to ensure the respect of the requirements concerning the execution of personal transactions by employees and management of CWFM; and
- to comply with any applicable law and regulatory requirements, including for instance any regulatory or legal tax reporting requirements, auditing or financial reporting requirements, or disclosure requirements from regulatory, tax or other governmental or public authorities.

5. Confidentiality

CWFM employees are bound by the applicable law (GDPR) and by the Code of Business Conduct and Ethics for C WorldWide Group in respecting applicable confidentiality rules and never using confidential information about our clients or their business activities or other circumstances in an undue manner.

6. Privacy by Default and Privacy by Design

Privacy by default means that *per se preferences* have been chosen to limit Processing activity.
Protection measures by default ensure that only necessary PD for a specific purpose and lawful grounds are processed. The data flows are of principle limited on the necessary quantity, available to the necessary persons, stored for the necessary period of time and accessible only for the necessary people or data recipients. Only PD which is necessary for the specific purposes will be processed. Privacy by Default concerns mainly the amount of collected data, the extent of the Processing, the period of storage or the limitation of access to the PD.
Privacy by Design concerns the early implementation of technical data protection measures during the development of new processes and at the time of Processing. The Controller is required to implement appropriate and organizational measures like the minimization, anonymization and other technical/operational measures to reduce risks for the data subjects.
For each new Processing CWFM takes both principles into account and has established a process flow, which is detailed in Appendix 1 ("Checklist New Processing of Personal Data', which is managed and stored by the Compliance function of CWFM.
The Conducting Officer who requests the implementation of a new DP relevant process submits a request to the other Conducting Officers and to the Compliance function. A detailed description of the new activity is needed on this stage and a DP-Analysis (DPIA see Appendix 2) needs to be performed. It will be checked if the Processing will be carried by a valid justification.
Furthermore, the Conducting Officers check the Data Processing roles and the risks for the Data Subject and CWFM.
Based on the analysis performed, the Conducting Officers decide on the new Processing activity and the decision is formalized in the meetings' minutes. Significant risks associated to new processing activities shall be reported to the Board of Directors.

7. Lawful grounds

The DP is only lawful when it is based on one or more legal grounds of Art 6 ff. GDPR. These grounds are:

- consent of the Data Subject;

- performance of a contract;
- compliance with legal obligations;
- vital interest of the Data Subject or another natural person (not the Processor or Controller);
- public interest or exercise or official authority;
- legitimate interest of the Controller or a third party overriding the interest of the Data Subject;

Processing of data for new/other purposes than the ones for which the data had been collected, must be based on valid lawful ground. A change of the lawful ground has to be disclosed to the Data Subject when the Data Subjects has not already this information.

Where the DP is performed on the base of consent provided by the Data subject, the data subjects consent must be freely given, it must specifically refer to the data to be processed and showing the matters for the consent. The purpose of the DP must be disclosed clearly and in an easily understandable wording. The data subject has to be advised that it has the right of withdrawing the consent at any time in an easy way. A withdrawal does not make the former processing unlawful.
This consent must be expressed for profiling the data subject or when sensitive data is processed.

In relation to the DP performed to ensure compliance with legal obligations, CWFM is obliged to identify and verify the identity of its investors/ business partners/ contractual counterparties and to have KYC documentation in place (e.g. Law 2004, CSSF regulation 12-02, Law 2010). Insofar the collection of PD is justified as long as it does not exceed the legally required information and the purpose has not changed. The ground includes the gathering of PD before the relationship is established as required by the applicable regulation.

The performance of a contract demands amongst other the clarification of the counterpart's identity including the identity of the representatives.
In some cases, the legitimate interest of the Controller may justify a Processing activity, however the interest and fundamental rights of the involved data subject must be considered as well and usually the rights of the data subject prevail. The interest of the Controller must be based on a valid, fact-based reasons at the time the data processing starts.

8. Disclosure of Personal Data to third parties and International Transfer of Data

The Personal Data and Confidential Data may be shared by CWFM in compliance with and within the limits of the Data Protection Laws with the following categories of third parties for the following reasons. CWFM requires that such third parties agree to process such Personal and Confidential Data based on given instructions and requirements consistent with this prospectus and with the relevant service provider agreements.

- the Registrar and Transfer Agent, Distributor/sub-distributor, and Information Technology providers, and such of their affiliates and other sub-processors as may be necessary for the aforementioned categories of service providers to provide their services;
- Regulatory or tax authorities, governmental or law enforcement agencies, and other governmental or public agencies or authorities, in order to comply with legal or regulatory obligations or at their request;
- advisors (e.g., auditors, legal counsel and tax advisors) to CWFM in relation to or in connection with the investors' investment in the Fund;
- banking institutions and other financial service providers to the Fund.

The above third parties may use the services of their affiliates or service providers to process the investors'

Personal Data where necessary or appropriate. CWFM requires that third parties processing Personal Data on behalf of CWFM agree by contract to process the Personal Data appropriately and based on given instructions and requirements consistent with the prospectus and the relevant service provider agreement.

The transfer of Personal Data to third parties set out above may involve the transfer of data to third countries outside of the EEA. Such countries may not have a comparable level of data protection as the investor's jurisdiction. When Personal Data is transferred to countries which are not deemed as equivalent in terms of Data Protection Laws, it is legally required that CWFM, the Registrar and Transfer Agent or any other agent provides for appropriate safeguards in order to ensure the appropriate protection of the investors'/other counterparties' Personal Data and Confidential information.

The investor is informed that the Registrar and Transfer agent will be delegated for data processing activities, as part of its Transfer and Registrar Agent duties, and if it will enter into outsourcing arrangements with third party service providers in- or outside the Transfer Agent group (the Sub- contractors). As part of those outsourcing arrangement, the Transfer Agent may be required to disclose and transfer personal and confidential information and documents about the investor and individuals related to the investor (the Related Individuals) (the Data transfer) (such as identification data – including the investor and/or the Related Individual's name, address, national identifiers, date and country of birth, etc. – account information, contractual and other documentation and transaction information) (the Confidential Information) to the Sub-contractors. In accordance with Luxembourg law, the Transfer Agent is due to provide a certain level of information about those outsourcing arrangements to CWFM which, in turn, must be provided by CWFM to the investors.

Confidential Information may be transferred to Sub-contractors established in countries where professional secrecy or confidentiality obligations are not equivalent to the Luxembourg professional secrecy obligations applicable to the Transfer Agent. In any event, the Transfer Agent is legally bound to and has committed to CWFM that it will enter into outsourcing arrangements with Sub-contractors which are either subject to professional secrecy obligations by application of law or which will be contractually bound to comply with the Data Protection Luxembourg Laws. Investors may obtain a copy of the mentioned agreements by contacting the following email address: Funds_GDPR@cww.lu.

A description of the purposes of the said outsourcing arrangements, the Confidential Information that may be transferred to Sub-contractors thereunder, as well as the name of the service provider and the country where those Sub-contractors are located is therefore set out in the below table.

Activity	Location
Input and authorization of subscriptions and redemptions, transfers, and switches	BNY Mellon - India BNY Mellon - USA BNY Mellon – Singapore & Hong-Kong BNY Mellon – UK & Ireland BNY Mellon – Poland
Payment Processing, including Retrocession processing	BNY Mellon - India BNY Mellon - USA BNY Mellon – Singapore & Hong-Kong BNY Mellon – UK & Ireland BNY Mellon – Poland
Release of Contract Note to Shareholders	BNY Mellon - India BNY Mellon - USA BNY Mellon – Singapore & Hong-Kong BNY Mellon – UK & Ireland BNY Mellon – Poland

Account opening/AML/Static Data Maintenance	BNY Mellon - India BNY Mellon - USA BNY Mellon – Singapore & Hong-Kong BNY Mellon – UK & Ireland BNY Mellon – Poland
End of day processing (including daily cash flow reporting to Fund Managers and release of Contract Note to Shareholders).	BNY Mellon - India BNY Mellon - USA BNY Mellon – Singapore & Hong-Kong BNY Mellon – UK & Ireland BNY Mellon – Poland
Investor Servicing	BNY Mellon - USA BNY Mellon – ASIA / EAST (Singapore, Hong-Kong, Japan) BNY Mellon – UK & Ireland BNY Mellon – Poland
Hosting of transaction monitoring tool	BNY Mellon - USA
Processing and sending (fax, email, post) of: - Dealing Contract Notes - Distribution Vouchers - Statements (Dealing & Retrocession) - Ad-hoc mailings	Capita Business Services Limited 71 Vitoria Street, Westminster GB/London SW1H 0XA
Scanning of physical post/documents including PSDC (prestataire de services de dematerialisation ou de conservation / in English: digitization or e-archiving service provider)	LAB Luxembourg S.A. Digital Transition Hub 3 rue Elvire Engel L-8346 GRASS - Luxembourg

Activity	Location
Vendor of the application that enables recording and end to end process of regulatory breaches and complaints / including Rackspace UK where the servers used by SSAL are hosted	STRATEGIC SOFTWARE APPLICATIONS LTD (SSAL) Warnford Court 29 Throgmorton Street London EC2N 2AT United Kingdom
Technology provider of the Mutual Fund Transfer Agency system / including their sub-contractors TIBCO & Vodafone	Bravura Solutions PTY Limited

Type of information transmitted to the Service Provider	Country where the Service Provider is established	Name of the Service Provider	Nature of the outsourced activities

Client Confidential Information including Shareholder Information	1- India 2- UK & Ireland 3- Luxembourg 4- Singapore & Hong-Kong 5- USA 6- Poland	1- BNY Mellon- India 2- BNY Mellon – USA 3- BNY Mellon – Singapore & Hong-Kong 4- BNY Mellon – UK & Ireland 5- Bank of New York SA/NV Poland Branch	- Transfer Agent/Shareholders Services (incl. Global Reconciliation) - Reporting - Client Services Activities

The Transfer Agent further committed to CWFM that it will take reasonable technical and organizational measures to ensure the confidentiality of the Confidential Information subject to the Data Transfer and to protect Confidential Information against unauthorised processing. Confidential Information will therefore only be accessible to a limited number of persons within the relevant Sub-contractor, on "a need to know" basis and following the principle of the "least privilege". Unless otherwise authorised/required by law, or in order to comply with requests from national or foreign regulatory authorities or law enforcement authorities, the relevant Confidential Information will not be transferred to entities other than the Sub-contractors.

When sharing Personal Data with third parties located in third countries, as laid out above, the Management Company and the Registrar and Transfer Agent commit to ensure compliance with GDPR rules.

9. Data Protection

CWFM protects personal data against unauthorized access, unlawful use, accidental loss, corruption or destruction.

CWFM uses technical measures such as encryption and password protection to protect data and the systems they are held in. CWFM also uses operational measures to protect the data, for example by limiting the number of people who have access to the databases in which booking information is conducted.

CWFM keeps these security measures under review and refers to industry security standards to keep up to date with current best practice.

10. Retention period

CWFM takes every reasonable step to ensure that the investors' and other counterparties (and related Data Subjects') Personal Data is only processed for the minimum period necessary for the purposes set out in the prospectus, the agreement or any other binding document.

The Personal Data of data subjects and their related parties, where applicable, will be retained for a maximum duration of up to five (5) years following the end of the business relationship between the respective data subjects and CWFM.

Personal Data may be retained for a longer duration if this is required under applicable law, or by a

regulatory or tax authority, a law enforcement agency or other governmental or public body or considered necessary in order to allow CWFM and the Fund's key service providers or their affiliates to comply with their legal obligations.

Once the period referred to above has expired, to the extent that this is applicable, the following actions will be carried out, at the respective Data Subject's choice:

- permanent deletion or destruction of the relevant Personal Data; or
- return of the Personal Data to the respective Data Subject.

The purge will be performed on an annual basis as long as no special legal reason requires an earlier action. Since the entire IT infrastructure is delegated to the Group, the rules for electronical data purging is also outsourced to CWW Group and follow the rules set up at group level. In the framework of the periodical due diligence on the delegate, CWFM verifies the alignment of the data protection rules applied by the delegate to the requirements applicable to CWFM and the respect of the policies.

For the purge of physical PD, once a year the Conducting Officers must provide the Compliance function the details:

- which kind of PD has been identified for purge;
- the deletion of the selected data.

All staff are required to keep a high discipline while gathering and storing PD and to only store PD in dedicated folders adequately protected and accessible only by authorized people.
In the case that employees store their own PD on electronical drives or on the hard drive of the workstation it is on the sole responsibility and risk of the employee. Each employee should consider that CWFM is entitled to replace the company devices, workstations or to delete the content of the drives at any time without any announcement or justification.
In addition, each Conducting Officer must consider security measures to limit the access to and dissemination of PD. Usually, this is done by:

- clean desk procedure;
- lockable cabinets for each employee;
- limited access to folders;
- removing access rights when not necessary;
- limited distribution of PD in physical form or by email only on a need-to-know basis.

11. Data Subject Rights

Under Data Protection Laws and/or applicable guidelines, regulations, recommendations, circulars and requirements issued by any local or European competent authority, such as the Luxembourg data protection authority (the "Commission Nationale pour la Protection des Données" CNPD) or the European Data Protection Board, each Data Subject has the following rights:

- Right of information, therefore the right to request from the Controller the information linked to the Processing of his/her PD, including the source from which his/her Personal Data originates and whether it originates from publicly accessible sources;
- Right to access his/her PD;
- Right to have the PD rectified or corrected if he/she deems the Personal Data incomplete or incorrect;
- Right to restrict the use of his/her PD;
- Right to request that his/her Personal Data be erased, unless there is a legitimate reason to justify storing it;
- Right to object to processing his/her PD, unless a legitimate reason prevails over his/her interests

and rights;
- Right to data portability (in certain specific circumstances), i.e. the right to receive the PD in a structured format.

Further details regarding the above rights are provided for in Chapter III of the GDPR and in particular Articles 15 to 21 thereof.

Whereas the Management Company requires data subjects' personal information in order to comply with AML or other legal or regulatory requirements, failure to provide this information will result in the Management not being able to accept the investor's investment in the Fund or the business relationship with the data subject.

Each Data Subject has the right to place a complaint with a data protection authority in the country where he/she is located or where CWFM is located or where the rights of the Data Subjects have been infringed. The authority keeps in this case the complainant informed.

The Data Subject is entitled to ask for compensation for material and immaterial damages caused by the Processing of PD by the Controller. Joint controllers are jointly liable against the Data Subject.

12. Responsibilities as Controller

CWFM has to ensure the implementation of appropriate technical and organizational measures to protect all PD against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and unlawful forms of Data Processing. This leads to the following obligations:

- Prevent all PD against the access of unauthorized persons to the facilities used for data processing (monitoring of entry to facilities);
- Prevent PD from being read, copied, amended or moved by any unauthorized person (monitoring of media);
- Prevent the unauthorized introduction of any PD into the information system, as well as any unauthorized knowledge, amendment or deletion of the recorded data (monitoring of memory);
- Prevent Processing systems from being used by unauthorized persons (monitoring of usage);
- Guarantee that persons when using an automated DP system access only data that are within their competence (monitoring of access);
- Check the identity of third parties to whom the PD can be transmitted (monitoring of transmission);
- Guarantee that the identity of the persons with access to the PD can be checked and recorded ex post (monitoring of introduction);
- Prevent PD from being read, copied, amended or deleted in an unauthorized manner when data are disclosed and data media transported (monitoring of transport);
- Safeguard PD by creating backup copies (monitoring of availability);
- Ensure Data Process is done in a way which is lawful, fair and transparent to the Data Subject ("lawfulness, fairness, transparency");
- Ensure that DP is performed for purposes which are specified, explicit and legitimate and may not be subsequently processed in anyway which is incompatible with these purposes (purpose limitation);
- Ensure that DP is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (data minimization);
- Keep PD accurate and, where necessary, up to date; every reasonable step must be taken to ensure that personal data, which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay ('accuracy');
- Keep PD in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed ('storage limitation').

The Conducting Officer in charge of Compliance of CWFM oversees the implementation of the above-mentioned principles.

13. Register of Processing activities (ROPA)

CWFM is obliged to keep written records of the processing activities and responsibilities, art. 30.1 of GDPR. For this reason, CWFM has assessed all flows of PD and mapped them in an inventory, which is kept up to date annually by the Compliance Function. The inventory contains:

- Name and contact details of the Controller/joint Controller, its representatives and the DPO (if applicable);
- Purpose of the processing;
- Description of the categories of Data subjects;
- Description of the categories of PD;
- Description of the categories of Recipients of PD;
- Cross border transfers;
- Time limits for data purging;
- Technical description of organizational security measures.

14. Data Processing Impact Analysis (DPIA)

New processing activities have to be subject of a DPIA which has to be executed in advance of the activity. The DPIA shows risks for the Data Subject and potential shortcomings. It helps to manage the risks linked to a Processing and gives flexibility for the mitigation of risks. It clarifies if a Processing activity needs to be disclosed to the CNPD. The Compliance function is in charge of the assessments and ensures compliance with the rules of the GDPR. The assessment has to contain at minimum:

- the systematic description of the planned activity;
- the purposes of the processing, including the legitimate interest of the Controller to implement the activity;
- an assessment on necessity and proportionality in relation to the pursued purposes;
- an assessment of the risks for the Data Subject's rights;
- detailed description of the measures to exclude or minimize the risks;
- in doubt CWFM will seek for the Data Subjects view on the risks linked to the new activity and take this position into account;
- the assessment has to be reviewed when the circumstances/ facts change

The Conducting Officer responsible for Compliance is responsible for having the assessment finalized and all the Conducting Officers are responsible to take the result of the assessment into account before a new process has been approved and implemented.
The initial DPIA of CWFM has been conducted on a risk-based approach and focusses on the most important Processing activities for the identified Data Subjects.
The DPIA process considers the following work steps:

- Description of the envisaged processing;
- Assessment of the necessity and proportionality;
- Measures envisaged to demonstrate compliance;
- Assessment of the risks to the rights and freedoms;
- Measures envisaged to address the risks;
- Documentation;
- Monitoring and review.

15. Data breaches

A personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data breaches can be categorized according to the three well-known principles of information security:

- Breach of confidentiality: in the event of disclosure or unauthorized or accidental access to personal data;
- Violation of availability: in case of loss /accidental or unauthorized destruction of personal data;
- Violation of integrity: in case of accidental or unauthorized modification of personal data;

Depending on the circumstances, a breach may concern confidentiality, integrity and availability at the same time, as well as any combination of these three principles.

In case of data breach, CWFM, as controller, shall determine whether the personal data breach presents a high risk to the rights and freedoms of the data subjects.

The data breach should be notified to both CNPD and data subject.

a) Notification to the CNPD:

If the data breach results in a risk to the rights and freedoms of individuals, CWFM, as data controller, must notify the breach to the CNPD without undue delay and, where feasible, not later than 72 hours after having become aware of it. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

The notification should be performed through the "Breach notification form" and should, at least:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact points from whom further information can be obtained;

- describe the likely consequences of personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The notification of the violation shall be sent to the email address databreach@cnpd.lu.

The Compliance function documents any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken and informs the other Conducting Officers; significant breaches must be reported to the Board of Directors.
Any notification to the CNPD must be approved by the Conducting Officers and the Board of Directors.

b) Notification to the data subject:

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least:

- the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact points from whom further information can be obtained;
- likely consequences of personal data breach;
- the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The means of communication used to contact the data subjects must be effective meaning that there must be a high probability that they receive the necessary information. If necessary, public communication may be required.

CWFM documents any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken (including data breaches not notified to the CNPD).

Any employee suspecting a case of personal data breach, (i.e., sending of an email containing personal data to the wrong recipients) reports immediately the incident to the Compliance function in order for them to take the necessary actions.

16. Information to investors, business partners and employees about rights under the GDPR

Based on section 2 of the GDPR, CWFM is obliged to inform all Data Subjects for which it processes PD about its relevant activities.
CWFM identified 3 categories of data subjects which are in scope: Investors, representatives of business partners and staff members.
CWFM informs the Data Subjects in particular about:

- the identity and the contact details of CWFM;
- purposes of the Processing and the legal ground for the processing, in particular the legitimate interest of CWFM as Controller;
- recipients of the PD;
- transfer PD to a third country and the existence or absence of an adequacy decision by the National Commission.

Investors which are already invested will be informed about the GDPR, the processing activities and the rights with written letters. The letters contain the GDPR relevant wording of the prospectuses.
Prospect investors receive all necessary information by means of the disclosure included in the prospectus and in the subscriptions forms. The documents will be available in different languages.
Business partners of CWFM subject of a Due Diligence will be informed via email or written letters.
(Future) Staff members are informed by e-mail prepared or by a written letter.
A summary of the data protection policy in place at CWFM is available on the website of the Company.

17. Outsourcing

In the case that CWFM has outsourced the Processing to third parties, e.g. to the appointed Register Agent, marketing agents, portfolio managers, it must ensure that the third party has data security measures, policies and controls in place. These measures, policies and controls shall be defined in the agreement between both parties to bind the Processor.
The criteria for the selection of the outsourcing partner include among others its professional expertise,

location, reputation, ability to provide the services to be outsourced as well as the guarantee for permanent provision of such services, available financial and human resources and also the effective protection of PD.
The main risks associated with the outsourcing must be identified, monitored, quantified and controlled systematically.
During the entire life of the relationship with the third party, the department in charge of the monitoring of the relationship must ensure that the counterparty has in place and maintains systems and procedures that are adequate to safeguard the security (confidentiality, integrity and
availability) of information, taking into account the nature of the information in question and the correct recording and retention of data.

18. Cookies

A cookie is a data file which is saved on your computer when opening a website. It allows websites to recognize your computer and allows for the gathering of information on which websites and functions you visit with your browser. Cookies cannot see who you are, what your name is or where you live. Nor can they see whether the computer is used by one or more persons. A cookie cannot spread computer virus or other harmful programs.

We may Process your Personal Data through cookie technology as described into the Cookies policy in force at C WorldWide Asset Management Fondsmæglerselskab A/S who makes available our website; the Cookies policy is available on the homepage of our website (https://www.cww.lu/cookie-policy/)

19. Appointment of Data Protection Officer (DPO)

CWFM has delegated to Bank of New York Mellon S/A, Luxembourg Branch the Transfer Agent activities. Also, CWFM has delegated the Distribution function to C WorldWide Asset Management, therefore the criteria laid down in art. 37 of GDPR to define the cases where the data controller or the data processor shall designate a DPO are not applicable:

1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity – criteria not applicable;

2. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale – the systematic processing of KYC/sanctions and AML related data could be considered as matching the criteria in terms of type of processing, but the activity has been externalized to an appointed Transfer Agent (data processor);

3. the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10 – not applicable as the data referred in article 9 are not treated and the data referred in article 10 could be treated but at the processor level, being outsourced the Transfer Agent function.

Based on the analysis above, CWFM decides not to appoint a DPO

20. Sanctions

The CNPD or another data protection authority can impose administrative fines against CWFM in any case

of infringements of the GDPR. A fine depends mainly on:

- The nature, gravity and duration of the infringement;
- Intentional or (only) negligent character of the infringement;
- Mitigation measures already taken;
- Degree of responsibility between Controller and Processor or other aspects previous infringements;
- Cooperation with the supervisory authority responsible for data protection;
- Manner how the infringement came to the attention of the authority and behavior of the Controller.

Each staff member must take into consideration that breaches may lead to strict fines for non-compliance, reaching up to €20 million, or 4% of the worldwide annual revenue, whichever is higher.

21. Complaints

Data subjects have the right to lodge a complaint with a supervisory authority, namely the CNPD of Luxembourg using the following link:

Complaint form - Individuals - National Data Protection Commission - Luxembourg (public.lu)

Commission nationale pour la protection des données
Service des réclamations
15, Boulevard du Jazz
L-4370 Belvaux

22. How to contact CWFM as data Controller

If Data subjects have any questions about the processing of their personal data, they should contact Funds_GDPR@cww.lu.

This policy, together with the Register of Processing Activities (see Appendix 3), should be reviewed by the Board of Directors of the Management Company at least annually and/or when needed.

Approved by the Board of Directors on September 3, 2026.

WORLDWIDE

Appendix 1 – Checklist New Processing of Personal Data

ID	Area	Questions	Answer
1	PD Scope	PD for	New processing activity
2	General information	Affected data subject	
3		Data status	
4		Data category	
5		Data Access Restricted – Need-to-know	*Yes/no*
6		Owner	*Please provide a user or department*
7		DPIA required	*Yes/no*
8	Main processing purpose	Consent by data subject	*Yes/no*
9		Performance of contract	*Yes/no*
10		Legal obligation	*Yes/no*
		If yes, please specify	
12		Protect vital interest of data subject	*Yes/no*
		If yes, please specify	
13		Public interest	*Yes/no*
		If yes, please specify	
14		Other legitimate interests	*Yes/no*
		If yes, please specify	
15	Data processing	Affected services	
16		Impacted core processing activities	
17		Data purge approach	For electronic data the CWW Group approach is applied Specify approach for physical documents
18		Retention time	For electronic data the CWW Group approach is applied Specify approach for physical documents
19		Cross border (if affected, specify reason for location in scope)	
20	Roles	Controller location	
21		Controller department	
22		Processor location	
23		Processor department	
24	Associated risk	Specify risk	
25	Data protection measures	Technical Measures	
26		Organisational measures	
27		If Cross-border is set at yes, other measures	

WORLDWIDE

Appendix 2 - DPIA Template

Criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:

- a systematic description of the processing is provided (Art. 35 VII (a):
  - nature, scope, context and purposes of the processing are taken into account:
  - PD, recipients and period for which the PD will be stored are recorded;
  - a functional description of the processing operation is provided:
  - the assets on which PD rely (hardware, software, networks, people, paper or paper transmission channels) are identified.
  - compliance with approved codes of conduct is taken into account (Article 35 VIII):
- necessity and proportionality are assessed (Article 35 VII (b)):
  - measures envisaged to comply with the Regulation are determined (Article 35 VII (d) and recital 90), taking into account:
    - measures contributing to the proportionality and the necessity of the processing on the basis of
      - specified, explicit and legitimate purposes) (Article S I (b));
      - lawfulness of processing (Article 6);
      - adequate, relevant and limited to what is necessary data (Article S I (c)):
      - limited storage duration (Article 5 T (c));
  - measures contributing to the rights of the Data Subjects:
    - information provided to the data subject (Art 12, 13 and 14):
    - right of access and portability (Art. 15, 20);
    - right to rectify, erase, object, restriction of processing (Art. 16 to 19 and 21):
    - Recipients:
    - Processor(s) (Art. 28);
    - safeguards surrounding international transfer(s) (Chapter V):
    - prior consultation (Art. 36).
- risks to the rights and freedoms of data subjects are managed (Art. 35 VII (c)):
  - origin, nature, particularity and severity of the risks are appreciated (cf recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
    - risks sources are taken into account (recital 90);
    - potential impacts to the rights and freedoms of data subjects are identified in case of illegitimate access, undesired modification and disappearance of data;
    - threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
    - likelihood and severity are estimated (recital 90)
  - measures envisaged to treat those risks are determined (Art. 35 VII (d) and recital 90):
- interested parties are involved:
  - the advice of the DPO (if applicable) is sought (Art. 35 II);
  - the views of data subjects or their representatives sought (Art. 35 IX).

Appendix 3 – Record of Processing Activities

gdpr-personal data processing register 2