



**C WorldWide Fund Management S.A.**  
**Privacy & Confidentiality policy**



## **Background**

The aim of this document is to describe the way C WorldWide Fund Management S.A. and its Danish Branch (hereafter also CWFM or the Management Company) processes 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”).

### **1. Processing Personal Data**

CWFM may from time to time receive personal information, as described below (the “Personal Data”), 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. 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.

#### **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;
- revenue;
- 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 performed 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 procedures. In order 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;
- 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 to the, 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

## **2. Disclosure of Personal Data to third parties and International Transfer of Data**

The Personal Data and Confidential 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 require 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 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 this 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' Personal Data and Confidential information.

The investor is informed that the Registrar and Transfer agent will in the scope of the delegation of data processing activities, as part of its Transfer and Registrar Agent duties, 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 C WorldWide which, in turn, must be provided by C WorldWide 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 C WorldWide 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.

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- Canada 2- Ireland 3- Luxembourg 4- Malaysia	1- RBC Investor Services Trust (Canada)  2- RBC Investor Services Bank S.A. Dublin Branch  3- RBC Investor Services Bank S.A. (Luxembourg)  4- RBC Investor Services Malaysia Sdn Bhd	- Transfer Agent/Shareholders Services (incl. Global Reconciliation) - Reporting - Client Services Activities



<p>Client Confidential Information including Shareholder Information (except for development and maintainance services)</p>	<p>1- IBM Luxembourg. RBC Canada</p> <p>2- IBM Luxembourg, IBM Poland. RBC Canada</p> <p>3- Canada, India, Luxembourg, Malaysia, United Kingdom</p>	<p>1-IBM Luxembourg s.à.r.l. RBC Investor Services Trust (Canada).</p> <p>2-IBM Luxembourg s.à.r.l IBM POLSKA sp. z o.o RBC Investor Services Trust (Canada)</p> <p>3-RBC Investor Services Trust (Canada). Tata Consultancy Services India. RBC Investor Services Bank S.A. (Luxembourg). RBC Investor Services Malaysia Sdn Bhd. RBC Investor &amp; Treasury Services (UK)</p>	<p>- IT Infrastructure (hosting services)</p> <p>- IT System Management/Operation Services on Infrastructure</p> <p>- IT Services (incl. development and maintenance services) &amp; IT Operations on Business Application</p>
---	---	--	--

The Transfer Agent further committed to CWFM that it will take reasonable technical and organisational 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 will always do this in a way permissible under GDPR rules.



### **3. 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 our booking information is held.

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

### **4. Retention period**

CWFM takes every reasonable step to ensure that the investors' (and related Data Subjects') Personal Data is only processed for the minimum period necessary for the purposes set out in this prospectus.

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.

### **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. Data Subject Rights**

Under certain conditions set out by the Data Protection Laws and/or by 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 to access his/her Personal Data and to know, as it may be, the source from which his/her Personal Data originates and whether it originates from publicly accessible sources;



- Right to have the Personal Data rectified or corrected if he/she deems the Personal Data incomplete or incorrect;
- Right to restrict the use of his/her Personal Data;
- 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 of his/her Personal Data, 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 Personal Data 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.

Where 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.

## **7. Data breaches**

A personal data breach is a breach of security leading to the 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 the confidentiality, the integrity and the availability at the same time, as well as any combination of these three principles.

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

If the data breach results in a high risk to the rights and freedoms of individuals, a notification of the breach to the CNPD is required.

The notification must, 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 point where more information can be obtained;





- describe the likely consequences of the 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](mailto:databreach@cnpd.lu).

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 name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;
- a description of 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. There must be a high probability that they receive the necessary information. If necessary, public communication may be required.

CEFM 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).

Therefore, it is important that any employee who suspects there has been a case of personal data breach, for example that an email containing personal data has been sent to the wrong recipients, immediately reports the incident to the Conducting officers in order for them to take the actions necessary.

## **8. 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 (<http://www.cww.lu/cookiepolitik>)

## **9. Appointment of Data Protection Officer (DPO)**

CWFM has delegated to RBC Investor Services Bank S.A. 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 TA function.

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

## **10. Complaints**

You have the right to lodge a complaint with a supervisory authority.

<https://cnpd.public.lu/en/droits/faire-valoir/formulaire-plainte.html>

Commission nationale pour la protection des données

Service des plaintes

1, avenue du Rock'n'Roll

L-4361 Esch-sur-Alzette

## **11. How to contact us**

If you have any questions about our use of your personal data, please contact us at Funds\_GDPR@cww.lu.