Mercer

welcome to brighter

Mercer Investment Solutions Europe

Data Protection and Confidential Information Policy

August 2025

Contents

1. Introduction I

2. Obtaining and Using Personal Data II

3. Storage and Security of Personal Data V

4. Retention Periods V

5. Breach Notifications VI

6. Privacy Impact Assessments VII

7. Transfers of Personal Data VIII

8. Data Access Requests IX

9. Other Data Subject Rights X

10. Appointment of a Data Protection Officer XII

Mercer Investment Solutions Europe Data Protection and Confidential Information Policy last updated in August 2025

Introduction

In the ordinary course of its business, Mercer Global Investments Management Limited ("**MGIM**") acts as management company or alternative investment fund manager, Mercer Global Investments Europe Limited ("**MGIE**") acts as investment manager and distributor, and Mercer Limited ("**Mercer Limited**") acts as sub-distributor, to MGI Funds plc, Mercer PIF Fund plc, Mercer QIF Fund plc, Mercer QIF CCF and Mercer UCITS Common Contractual Fund (collectively the "**Funds**") (together with MGIE, MGIM, and Mercer Limited, the "**Companies**").

The Companies collect and process Personal Data (as defined below) of natural persons (including natural persons connected to such individuals) who are clients, prospective clients, and investors and prospective investors in, and service providers to, the Funds, as well as Personal Data relating to its and, as appropriate, their respective directors, officers, employees, agents, representatives and personnel ("**Individuals**"). The Companies are the entities involved in providing Mercer Investments Solutions.

For the purposes of this policy, **"Personal Data"** includes any personal information (whether or not it is sensitive) which relates to an identified or (directly or indirectly) identifiable living Individual, including without limitation name, address(es), email address, date of birth, identification documents, anti-money laundering related information, account numbers, bank account details, tax and other public or social security identifiers, and residency information, and online identifiers, and may include personal information, contracts and related documents between the Companies and shareholders or prospective investors (whether or not Individuals), and between the Companies and / or between the Companies and the service providers to the Funds, MGIM or MGIE ("**Service Providers**").

The Companies are obliged to adhere to relevant data protection laws relating to Personal Data as applicable. In addition, the Companies have contractual confidentiality obligations which are owed to shareholders, prospective investors and the Service Providers, amongst others.

The Funds and MGIM act as joint data controllers, in obtaining and using Personal Data in connection with clients, shareholders, prospective clients and investors, and employees and representatives of Service Providers. MGIE and Mercer Limited are separate controllers of the Personal Data of Individuals for the purposes the provision of investment services (such as discretionary portfolio management and/or investment advice related to investment into the Funds) directly to professional investors.

The Personal Data may be held electronically, processed via automated processes, or held in general files, and where processed on the Companies' behalf by Service Providers, will be subject to written contracts governing that processing and setting out the security and confidentiality measures which the Service Providers have committed to implement.

This document sets out the Companies' policies and guidelines with regard to the processing of Personal Data as data controller. Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection,

recording, organisation, structuring, storage, adaption, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The Board of each Company has also adopted the MMC Global Information Security Policy, which addresses the Companies' policy with regard to cyber security and IT risk. In the event of any conflict between the information security policy and this policy, this policy shall prevail insofar as any cyber security or IT incident impacts Personal Data.

For the avoidance of doubt and notwithstanding anything to the contrary in this policy, nothing in this policy shall prevent the Companies from complying with any legal or regulatory obligation to disclose Personal Data in accordance with applicable law.

Obtaining and Using Personal Data

Current law requires that Personal Data may only be processed if the data controller has a legal basis, such as data subject consent, or if the processing is necessary for the performance of a contract to which the data subject is party, for the taking of other pre-contract measures at his / her request, or where processing is otherwise necessary for compliance with legal obligations, to protect the vital interests of the data subject; or is otherwise necessary for the data controller's legitimate interests or on public interest grounds.

Specifically, it is a requirement that Personal Data must be processed in accordance with the principles of data protection which are:

- **Lawfulness, fairness & transparency**: Personal Data must be processed fairly and lawfully, in a transparent manner.
- **Purpose limitation**: Personal Data must be collected for specified, explicit and legitimate purposes, and not further processed in a manner which is incompatible with those purposes.
- **Data minimisation**: In addition, Personal Data must be adequate, relevant and limited to what is necessary in relation to such purposes.
- **Accuracy**: Furthermore, Personal Data must be accurate and, where necessary, kept up to date.
- **Storage limitation**: Personal Data must also be in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the Personal Data was collected.
- **Integrity & confidentiality**: The Companies are required to ensure that Personal Data is processed in a manner that ensures appropriate integrity, confidentiality and security of the

Personal Data, including against unauthorised or unlawful processing and against accidental loss or destruction or damage, using appropriate technical and organisational measures. In addition, the Companies impose confidentiality obligations on the Service Providers, and is subject to confidentiality obligations with regard to investors and Service Providers.

- **Accountability**: The Companies are responsible for demonstrating compliance with the data protection principles.

Accordingly:

- Only Personal Data, which is strictly necessary for the purpose of a subscription into the Funds and / or the contract between the Companies and a client or shareholder, prospective client or investor, or Service Provider (as relevant), should be requested or obtained from the client or shareholder, prospective client or investor, Service Provider or relevant Individual.

- Through the application forms, privacy statement(s) (current copies of which are available at Mercer Investment Solution Europe Privacy Statement.pdf) and prospectus of the Funds, the Companies make shareholders, prospective investors, Service Providers and relevant Individuals aware of:

  - the identity and contact details of the Companies;

  - contact details of the data protection officer;

  - the purposes of the processing for which the Personal Data are intended;

  - the legal bases for processing; and

    - where that legal basis is a legitimate interest of a Company or a third party, a description of those legitimate interests and the right to object to the processing; and

    - where the legal basis is consent, the right to withdraw consent;

  - the recipients or categories of recipients (if any) of the Personal Data;

  - where applicable, details of any intended transfer of Personal Data to a third country or international organisation;

  - details of storage and retention periods;

  - details of any automated decision-making, including any profiling;

  - the right of Individuals to get access to their Personal Data, to rectify or erase any such Personal Data, and their other rights under applicable data protection laws;

  - details on where the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and consequences of failure to provide Personal Data; and

- the right to lodge a complaint with the local Data Protection Authority ("**DPA**") (for example, in Ireland the Data Protection Commission) (the "**DPC**").

- The Companies will not use Personal Data other than for the purposes which have been brought to the attention of the relevant Individual and, if consent is required, to which the relevant Individual has consented.

- Where Service Providers process Personal Data for a Company pursuant to contracts between the relevant Company and a Service Provider, the Service Provider acts as data processor of the relevant Company. The relevant Company will therefore ensure that:

  - appropriate due diligence is undertaken on such Service Providers to confirm that the Service Providers provide sufficient guarantees to implement appropriate technical and organisational security measures so as to meet the requirements of applicable law and to ensure the protection of the rights of the Individuals with regard to their Personal Data;

  - where a Service Provider will transfer Personal Data outside of the European Economic Area ("**EEA**") (with the exception of the UK and other third countries deemed adequate, at the time of the transfer, by the European Commission), appropriate due diligence must be carried out in the form a transfer impact assessment to determine if the laws and practices of the country of transfer will afford a level of data protection to Personal Data which is of essential equivalence with the data protection laws in the EEA. Supplemental measures of a contractual, organisational or technical nature may need to be agreed with the Service Provider. Where a Service Provider is proposing to transfer Personal Data to the United States, in reliance on the EU-US Data Privacy Framework ("**DPF**"), the relevant Company must verify that the data importer has successfully self-certified under the DPF (see here);

  - any contracts with such Service Providers impose obligations on the Service Providers which are required under applicable law and which assist the Company in complying with its own obligations under applicable law; and

  - any contracts with such Service Providers acting as data processors include data processing clauses required by the General Data Protection Regulation (EU) 2016/679.

- Where Service Providers are dealing with existing shareholders, the Service Providers have confirmed that they have procedures in place to verify on behalf of the Funds that all existing Personal Data held relating to those existing shareholders is accurate and up to date.

Storage and Security of Personal Data

Each of the Companies and the Service Providers is obliged to implement appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, or accidental loss, alteration, unauthorised disclosure or access. This applies particularly where such Personal Data will be transmitted over a network.

Generally, the Companies shall, and where they appoint the Service Providers, shall ensure that the Service Providers shall:

- taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of Individuals, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, which shall include, as appropriate:
    - pseudonymisation and encryption;
    - the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems, procedures and services;
    - the ability to restore availability and access in a timely manner in the event of a technical incident;
    - a process for regular testing, assessing and evaluating the effectiveness of those measures;
- take all reasonable steps to ensure that employees and other agents are aware of and comply with the security measures which have been implemented, including training of their respective relevant employees and agents;
- ensure that technical security controls are implemented to limit access to the Personal Data on a “need to know” basis; and
- ensure that all hard copies of Personal Data are securely stored and are only accessed on a “need to know” basis.

Retention Periods

The Companies are obliged to retain certain Personal Data to ensure accuracy, to help maintain quality of service and for legal, regulatory, fraud prevention and legitimate business purposes.

Each Company is obliged by law to retain AML related identification and transaction records for five years from the end of the relevant investor relationship or the date of the transaction respectively.

Other information, including Personal Data of the directors and business contact information, will be retained for no longer than is necessary for the purpose for which it was obtained by the relevant Company or as required or permitted for legal, regulatory, fraud prevention and legitimate business purposes. In general, the Companies (or their Service Providers on their behalf) will hold this Personal Data for a period of seven years from the termination of the relevant business relationship, unless the relevant Company is obliged to hold it for a longer period under law or applicable regulations. Certain director information may be held indefinitely where it forms part of the statutory books and records of the relevant Company.

The Companies (or their Service Providers on their behalf) will also retain records of telephone calls and any electronic communications for a period of five years and, where requested by the Central Bank of Ireland, for a period of up to seven years from the date of such call or communication.

Breach Notifications

In accordance with applicable data protection laws, the Companies will be obliged to notify the local DPA of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data transmitted, stored or otherwise processed (each a "**personal data breach**") within 72 hours of becoming aware of same, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of Individuals. Furthermore, the Companies will need to communicate with any impacted Individuals without undue delay where a personal data breach is likely to result in a high risk to the rights and freedoms of those Individuals.

In the event of a personal data breach:

- the impacted Companies shall give immediate consideration to the likely risks arising from the personal data breach, taking into account the nature and scope of the Personal Data in question, the extent of the breach, the period of the breach, and any security measures which may militate against risk, such as encryption. In doing so, the potential consequences for the affected Individuals will be considered;

- any reportable personal data breach will be reported to the DPC within 72 hours of the relevant Companies becoming aware of the incident. Where a report is made to the DPC, the relevant Company will provide such information and detail as is required under applicable data protection laws and / or as the DPC may request, which shall include:

    - a description of the nature of the personal data breach, including where possible, the categories and approximate numbers of impacted Individuals, and the categories and approximate number of Personal Data records concerned;

    - a description of the likely impact of the personal data breach;

- a description of measures to address the breach including to mitigate possible adverse effects;

- reporting to the DPC may be conducted in phases where the full extent of the personal data breach is not known within 72 hours of the relevant Company becoming aware of same. Any such phased reporting will be conducted in consultation with the DPC; and

- any incidents which are likely to result in high risk to Individuals will be communicated to the impacted Individuals without undue delay unless this would involve: (a) disproportionate effort; (b) the Personal Data were encrypted or unintelligible; or (c) the relevant Company has taken subsequent measures which ensure the high risk to the rights and freedoms of the Individuals concerned is no longer likely to materialise. In the case that the communication would involve disproportionate effort, a public communication or similar equally effective notification measure shall be implemented by the relevant Company.

Where, having considered the matter, the Company comes to a determination that no notification is required to be made to the DPC and / or the affected data subjects, the Company shall in any event keep a summary record of each incident which has given rise to the risk of unauthorised disclosure, loss or alteration of Personal Data, including its effects and any remedial action taken, which will include an explanation as to why the Company did not consider it necessary to inform the DPC.

Records may be made available to the DPC on request (e.g. security incident reports, record of processing activities, etc.). This means all steps taken to deal with a personal data breach need to be clearly documented by the relevant Company.

The Companies shall make all reasonable efforts to ensure that the Service Providers notify the Companies without delay of any security incident and provide all reasonable assistance to the relevant Company to enable it to comply with its obligations under applicable data protection laws with regard to notification of personal data breaches.

Privacy Impact Assessments

The Companies may be required to undertake privacy impact assessments in relation to the processing of Personal Data in certain circumstances and will undertake an impact assessment where the processing in question, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of Individuals.

Without limitation, the following may be indicative of high risk processing:

- a significant change to the processing operations relating to the Personal Data, including where implemented by one of the Service Providers;

- processing involving evaluation, scoring, monitoring or profiling of Individuals;

- Combining of two or more data sets arising from separate processing operations conducted for different purposes; and

- Innovative use of technologies or of organisational measures to protect Personal Data.

Any privacy impact assessment shall include:

- a systematic description of the envisaged processing operations and the purposes of the processing, including where applicable the legitimate purposes pursued by the relevant Company;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to Individuals; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure protection of Personal Data and to demonstrate compliance with applicable data protection laws taking into account the rights and legitimate interests of Individuals.

The relevant Companies shall consult with the DPC where necessary in accordance with applicable data protection laws, and where appropriate shall seek the views of Individuals or their representatives.

The relevant Companies shall ensure that the Service Providers notify the relevant Companies without delay of any new processing or change in processing arrangements (including implementation of any new technology) to facilitate the relevant Companies in determining whether the processing is likely to result in high risk to Individuals and shall provide all reasonable assistance to the relevant Companies to enable it to comply with its obligations under applicable data protection laws with regard to undertaking a privacy impact assessment.

Transfers of Personal Data

The cross-border processing of Personal Data outside of the EEA ("**transfer**"), whether to an entity related to the Companies or any of the Service Providers, or to a third party, is restricted, and is only permitted in limited circumstances. Particular restrictions and limitations apply to the transfer of Personal Data to countries outside of the EEA, where such countries do not have equivalent levels of data protection to that afforded to Personal Data under Irish law.

Appropriate due diligence must be carried out in the form a transfer impact assessment to determine if the laws and practices of the non-EEA country of transfer will afford a level of data protection to Personal Data which is of essential equivalence with the data protection laws in the EEA. Supplemental measures of a contractual, organisational or technical nature may need to be agreed with the entity related to the Companies or Service Provider.

In the event that a Company or a Service Provider wishes to transfer Personal Data to a country outside the EEA or outside the UK, it will in general be necessary for the relevant Company to have in place a written agreement with the third party to whom the Personal Data is transferred (the "**Importer**") which will:

- limit the scope of use of that Personal Data to specified and permitted purposes;
- prohibit further processing without the express consent of the relevant Company and / or MGIM and / or the relevant Individual or entity to whom the Personal Data relates;
- contain an undertaking from the Importer to comply with policies and guidelines similar to those to which the relevant Company and / or MGIM is subject; and
- contain an undertaking from the Importer that it will implement adequate technical and organisational safeguards to protect the Personal Data.

Where processing is occasional and non-repetitive, it may be possible for the relevant Company to transfer Personal Data outside the EEA and the UK where such transfer is necessary for the performance of a contract between the Company and an Individual, or where the Individual has explicitly consented to the transfer.

The Companies may transfer Personal Data to other companies in the Marsh McLennan group of companies in accordance with the binding corporate rules adopted by the Marsh McLennan group (as approved by a competent data protection authority (such as the DPC)).

A relevant Company, as data controller, may also impose a contractual obligation on the Service Provider to put in place Module 3 of the European Commissioner's approved standard contractual clauses (2021) where that Service Provider is appointing a sub-processor in a country outside the EEA which is not subject to a European Commission adequacy finding. However, in no case will Personal Data be transferred outside Ireland or the UK without the relevant Company's knowledge.

Where it is proposed to transfer Personal Data to the United States, in reliance on the DPF, the relevant Company must verify that the Importer has successfully self-certified under the DPF (see here).

Data Access Requests

In the event that an Individual makes a data subject access request in writing or otherwise, there is an obligation on a data controller to provide certain information to the data subject along with a copy of the Individual's Personal Data.

Accordingly, upon receipt of any data subject access request, the relevant Company shall respond without undue delay and in any event within one month of receipt of the request. This period may be extended by up to two further months where necessary, taking into account the complexity and number of requests.

Where the Company has reasonable doubts concerning the identity of the individual making the request, it may request additional information necessary to confirm the data subject's identity. In such cases, the response period shall commence upon receipt of the additional information.

In its response, the Company shall:

- inform the Individual as to whether the data processed by or on behalf of the relevant Companies (and MGIM in the case of the Funds) includes Personal Data relating to the Individual, and where it does, to provide access to such Personal Data including a description of:
    - the categories of the Personal Data;
    - the purposes for which they are being or are to be processed;
    - the recipients or categories of recipients to whom they are or may be disclosed;
    - information as to source, where not obtained directly from the Individual;
    - where possible, the envisaged storage period, or alternatively the criteria used to determine that period;
    - the right to lodge a complaint to the DPC;
    - details of any automated decision making or profiling (if applicable);
    - the existence of the right to request rectification or erasure of Personal Data or restriction of processing of Personal Data or to object to such processing;
    - the appropriate safeguards with regard to international data transfers (e.g. standard contractual clauses).
- provide the Individual with a copy of their Personal Data; and
- provide the relevant information to the Individual free of charge, in an easily visible, intelligible and clearly legible manner within one month of a proper request from the data subject, unless an exception applies under applicable data protection laws (meaning certain Personal Data can be withheld or redacted from the access request response).

If the relevant Company does not intend taking action at the request of the data subject, the Company shall inform the Individual without delay and the reasons for not taking action, as well as the right of the Individual to complain to the DPC.

The relevant Company shall ensure that the Service Providers notify the relevant Companies (and MGIM in the case of the Funds) without delay of any data subject access request and provide all reasonable assistance to the relevant Company to enable them to comply with their respective obligations under applicable data protection laws in relation to any data subject access requests.

Other Data Subject Rights

Individuals also have the following rights, in certain circumstances:

- the right to rectify inaccurate Personal Data

- the right to restrict processing

  An Individual may request that the Companies restrict processing of his / her Personal Data where:

  - its accuracy is contested, to allow the Companies to verify its accuracy; or
  - the processing is unlawful, but the Individual does not want it erased; or
  - it is no longer needed for the purposes for which it was collected, but the Individual still need it to establish, exercise or defend legal claims; or
  - an Individual has exercised the right to object, and verification of overriding grounds is pending.

  With the exception of storing Personal Data, following a request for restriction, Personal Data may only be processed by the relevant Company with the Individual's consent or to establish, exercise or defend legal claims or to protect the rights of another natural or legal person or for reasons of public interest.

- the right to object to processing

  An Individual can object to any processing of his / her Personal Data which is based on the Companies' legitimate interests, if that Individual believes his / her fundamental rights and freedoms outweigh the Companies' legitimate interests. The Companies will, however, have an opportunity to demonstrate that it has compelling legitimate interests which override the Individual's rights and freedoms. An Individual can also object to processing of his / her Personal Data for direct marketing purposes.

- the right to be forgotten

  An Individual can also request that the Companies erase his / her Personal Data in limited circumstances where:

  - it is no longer needed for the purposes for which it was collected; or
  - the processing was based on consent and consent has been withdrawn; or
  - following a successful right to object to processing based on legitimate interests (see above); or
  - it has been processed unlawfully; or
  - to comply with a legal obligation to which the Companies are subject.

The Companies are not required to comply with a request to erase Personal Data if the processing of the Personal Data is necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims.

- the right to data portability

  An Individual has the right to request Personal Data be provided or be transferred directly to another data controller, in a structured, commonly used, machine-readable format, but only where the processing is based on consent or on the performance of a contract with the individual, and the processing is carried out by automated means.

- the right not to be subject to automated decision making, including profiling

  An Individual shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. This shall not apply if the decision is necessary for entering into, or performance of a contract with the Individual, is authorised by European Union or Member State law, or is based on the Individual's explicit consent.

The Companies shall comply with applicable data protection laws in honouring Individual rights as set out above. However, if a Company does not intend taking action at the request of the data subject, the relevant Company shall inform the Individual without delay and the reasons for not taking action, as well as the right of the Individual to complain to the DPC.

The Companies shall ensure that the Service Providers notify the relevant Company without delay of any data subject requests to enforce the above rights and provide all reasonable assistance to the relevant Company to enable them to comply with their obligations under applicable data protection laws in relation to any data subject requests.

Appointment of a Data Protection Officer

The Marsh McLennan group has appointed a Group Data Protection Officer ("**DPO**") for all the Marsh McLennan companies. Any queries regarding the use of the Personal Data by the Companies and / or the exercise of individual rights should be addressed to Mercer at privacycoordinator@mercer.com or the group DPO at privacy@mmc.com.

Last updated August 2025

Version:	Prepared by:	Reviewed by:	Approved by:	Version Date:
1	Matheson (Anne Marie Bohan)	LCPA	MGIE and MGIM board	Versions 2018 to 2021
2	William Fry (Patricia Taylor)	LCPA	MGIE and MGIM board	June 2022
3	William Fry (Patricia Taylor)	LCPA (AB)	MGIE and MGIM board	June 2023

4	William Fry (Patricia Taylor)	LCPA (AB) & Technology (Mike Burke)	MGIE Board MGIM Board	August 2023 November 2023
5	William Fry	LCPA (AB)	MGIE Board MGIM Board	August 2025