

**Guggenheim Global Investments plc**

**Data Protection Policy**

<b>Version</b>	<b>Approved By</b>	<b>Date</b>
<b>1</b>	<b>Board of Directors</b>	<b>25 May 2018</b>

## 1 Introduction

- 1.1 Guggenheim Global Investments plc (the "**Company**") has adopted this data protection policy (the "**Policy**") to ensure it meets its obligations under the EU data protection regime introduced by the General Data Protection Regulation (Regulation 2016/679, the "**Data Protection Legislation**").
- 1.2 This Policy describes how Personal Data must be collected, handled, stored, disclosed and otherwise "Processed" to meet the Company's data protection obligations and to comply with the Data Protection Legislation.
- 1.3 The purpose of this Policy is to ensure that everyone involved in the processing of Personal Data at the Company is fully aware of, and complies with, the requirements of the Data Protection Legislation.
- 1.4 A "Privacy Notice" exists which provides information for external individuals as to how their Personal Data is being processed.
- 1.5 In preparing the Policy, the Company has taken into account the nature, scale and complexity of its business and in particular the fact that it relies broadly on an outsourced model and the support of its delegates and affiliates for the performance of its functions. As the Company does not regularly and systematically monitor Data Subjects on a large scale, it has not appointed a data protection officer. The Company's board of directors (the "**Board**") is ultimately responsible for ensuring that the Company meets its legal obligations and operates in full compliance with the Data Protection Legislation.

## 2 Definitions

- 2.1 "**Data Controller**" means any natural or legal person, which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data (in this case, the Company).
- 2.2 "**Data Processor**" means a natural or legal person who processes Personal Data on behalf of the Data Controller such as a fund administrator, distributor and/or other delegates that receive Personal Data.
- 2.3 "**Data Subject**" means an identified or identifiable natural person who is the subject of Personal Data.
- 2.4 "**Personal Data**" means any information relating to a Data Subject, such as name, residential address, email address, contact details, corporate contact information, signature, nationality, place of birth, date of birth, tax identification, credit history, correspondence records, passport number, bank account details, source of funds details and details relating to an investor's investment activity.
- 2.5 "**Privacy Notice**" means the data protection disclosure statement prepared in respect of the Company outlining the Company's data protection obligations and the data protection rights of Data Subjects investing in the Company, as required under the Data Protection Legislation.
- 2.6 "**Processing**" means performing any operation or set of operations on Personal Data, whether or not by automatic means, including collecting, recording, organising, storing, amending, using, retrieving, disclosing erasing or destroying it. The rules around the Processing of Personal Data apply whether the activity takes place in the European Union ("**EU**") or not, where the Processing activities are related to (i) the offering of goods and services to Data Subjects that are in the EU; or (ii) the monitoring of their behaviour which takes place within the EU.

## 3 The Company as Data Controller

- 3.1 The Company is a Data Controller and shall comply with its obligations as such under the Data Protection Legislation.

3.2 When Processing Personal Data, there may also be times where other service providers to the Company (including the administrator) will be required to use Personal Data for purposes they have determined to be lawful and necessary, in which case they may be characterised as Data Processors or (joint) Data Controllers under the Data Protection Legislation.

#### 4 **Data Protection Principles**

4.1 Personal Data shall be:

- (a) processed fairly, lawfully and transparently;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- (c) limited to what is required for the stated purpose or purposes;
- (d) accurate, complete and up to date;
- (e) retained for not longer than is necessary for the stated purpose or purposes;
- (f) kept safe and secure;
- (g) provided to a Data Subject on request (please see Section 5); and
- (h) not transferred to people or organisations situated in countries without adequate protection.

4.2 Fair and transparent Processing

Fairly obtained Personal Data requires that the Data Controller, at the time the Personal Data is collected, makes the Data Subject aware of the following:

- (a) the identity and contact details of the Data Controller;
- (b) the purpose in collecting the Personal Data as well as the legal basis for Processing;
- (c) the legitimate interests of the Data Controller or third party and an explanation of those interests (where Processing is based on this ground);
- (d) the persons or categories to whom the Personal Data may be disclosed;
- (e) where applicable, details of any transfers outside of the European Economic Area ("**EEA**"), safeguards in place and the means by which to obtain a copy of them;
- (f) the period for which the Personal Data will be stored or the criteria used to determine that period;
- (g) the Data Subject's right to rectify or request erasure of Personal Data;
- (h) the Data Subject's right to the portability of their Personal Data;
- (i) the Data Subject's right to withdraw consent; and
- (j) the Data Subject's right to lodge a complaint with the Data Protection Commission.

The Company generally meets these requirements through the provision to Data Subjects of the Privacy Notice (contained in the application form) and a summarised disclosure contained in its prospectus. The Privacy Notice has been circulated to all existing Data Subjects of the Company immediately prior to the Data Protection Legislation taking effect.

The Company will ensure that all information and communications relating to the Processing of Personal Data will be clear, concise, transparent, intelligible, easily accessible and easy to understand using clear and plain language. The Company will ensure that these transparency requirements are adhered to at all stages of the collection and Processing of Personal Data.

If any of the information described above changes after it has been provided to the Data Subject, the Data Subject shall be provided with an update to the information.

#### 4.3 Lawful Processing

The Company can process Personal Data lawfully to the extent that at least one of the following applies;

- (a) where the Data Subject has given consent to the Processing;
- (b) where this is necessary for the performance of the contract with the Company;
- (c) where this is necessary in order to protect the vital interests of the Data Subject or another natural person;
- (d) where this is necessary for the performance of a task carried out in the interest or in the exercise of official authority vested in the Data Controller;
- (e) where this is necessary for compliance with a legal obligation to which the Company is subject; and/or
- (f) where this is necessary for the purposes of the legitimate interests of the Company or a third party and such legitimate interests are not overridden by the Data Subject's interests, fundamental rights or freedoms.

#### 4.4 Purpose Limitation

The Company will only collect and process Personal Data for purposes that are specific, explicit and for legitimate purposes. The Company will process Personal Data for the following purposes;

- (a) to reflect an investor's ownership of shares in the Company (i.e. where this is necessary for the performance of the contract to purchase shares in the Company or to process redemption, conversion, transfer and additional subscription requests or the payment of distributions);
- (b) to discharge its anti-money laundering obligation to verify the identity of its customers (and, if applicable their beneficial owners) or for prevention of fraud or for regulatory or tax reporting purposes or in response to legal requests or requests from regulatory authorities (i.e. where this is necessary for compliance with a legal obligation to which the Company is subject); and/or
- (c) for direct marketing purposes (that is, the provision of information to Data Subjects on products and services) or for quality control, business and statistical analysis or for tracking fees and costs or for customer service, training and related purposes (i.e. where this is necessary for the purposes of the legitimate interests of the Company or a third party and such legitimate interests are not overridden by the Data Subject's interests, fundamental rights or freedoms and provided that the Company is acting in a fair, transparent and accountable manner and has taken appropriate steps to prevent such activity having any unwarranted impact on the Data Subject, noting the right of the Data Subject to object to such uses, as discussed below).

The Company will not process Personal Data in a manner that is incompatible with the purposes communicated to Data Subjects.

#### 4.5 Personal Data Minimisation

The Personal Data collected will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is being processed.

#### 4.6 Accurate Records

The Company will ensure that the Personal Data held is accurate and kept up to date. The accuracy of any Personal Data will be checked at the time of collection and at regular intervals or triggers thereafter. The Company will take all reasonable steps to amend inaccurate or out-of-date Personal Data.

#### 4.7 Storage Limitation

The Company will not keep Personal Data longer than is necessary for the purpose or purposes for which it was collected. It will take all reasonable steps to erase all Personal Data which is no longer required. The Company will be clear when informing the Data Subject about the length of time for which Personal Data will be kept and the reason why the information is being retained.

#### 4.8 Security

In processing Personal Data, the Company shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, 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 natural persons. In particular, the Company shall take all appropriate security, technical security and organisational measures to address the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

The Company will seek assurances from any service providers that act as Data Processors for the Company that they have implemented appropriate information security measures which comply with the relevant conditions of the Data Protection Legislation.

#### 4.9 Transferring Personal Data to a country outside the EEA

The Company itself will not transfer Personal Data but anticipates that its Data Processors may transfer Personal Data to entities located outside of the EEA.

Data Processors may only transfer Personal Data outside of the EEA (a) with the written consent of the Company; or (b) where required to do so by EU or the law of an EU member state to which the relevant Data Processor is subject.

Any such transfer of Personal Data by the relevant Data Processor shall be subject to the provision by the Data Processor of appropriate safeguards and subject to the availability of rights and effective legal remedies for Data Subjects, or shall otherwise be in accordance with the requirements of the Data Protection Legislation.

### 5 **Data Subject Rights**

#### 5.1 Right to Access

The Data Subject shall have the right to obtain confirmation from the Company as to whether or not Personal Data concerning them is being processed.

Where the Company is Processing their Personal Data, the Data Subject will have the right to access such Personal Data and the following information;

- (a) the purpose of the Processing;
- (b) the categories of Personal Data concerned;
- (c) the persons or categories of persons to whom the Personal Data may be disclosed, in particular recipients in third countries or international organisations;

- (d) the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
- (e) the existence of the right to request from the Company rectification or erasure of the Personal Data or restriction of Processing of Personal Data concerning the Data Subject or to object to such Processing;
- (f) the right to lodge a complaint with the Data Protection Commission;
- (g) where the Personal Data is not collected for the Data Subject, any available information as to their source; and
- (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

Where Personal Data is transferred to a third country or an international organisation, the Data Subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

The right to obtain a copy of the Personal Data undergoing Processing will not adversely affect the rights and freedoms of others, meaning the relevant information will be redacted where necessary.

The Company will not charge a fee for complying with the Data Subject's access request unless it can demonstrate that the request is excessive in nature, having regard to the number of requests made by the Data Subject. In such cases a reasonable fee based on administrative costs may be charged.

The information must be provided without delay and within at least one month<sup>1</sup>. Where requests are complex, the Company will be able to extend the deadline for providing the information to a total of three months. However, it must still respond to the request within a month, explaining why the extension is necessary.

The Company may refuse to act upon a request that is manifestly unfounded or excessive in nature, in which case it will inform the Data Subject of its reasons as soon as practicable in writing and inform the Data Subject of their right to lodge a complaint with the Supervisory Authority.

A request may be made by an individual, such as an investor or a director, and may be made in electronic format as well as by written request.

## 5.2 Right to be forgotten

The Data Subject shall have the right for Personal Data to be erased without undue delay in certain contexts including, but not limited to, where the Personal Data has been Processed unlawfully or where the Personal Data is no longer necessary in relation to the purposes for which it was collected or otherwise.

Given the specific nature for which the Company uses the Personal Data it collects, this is not likely to be applicable to the Data Subjects of the Company.

## 5.3 Right to the restriction of Processing

Data Subjects have the right to require that the Company restrict Processing of Personal Data in certain circumstances including, but not limited to, where the Personal Data is inaccurate, is no longer required in light of the purposes of the Processing or the Data Subject has exercised their right to object (pending verification of any legitimate grounds of the Company which overrides those of the Data Subject).

Where Processing has been restricted, such Personal Data shall, with the exception of storage, only be processed with the Data Subject's consent. The Company will inform the Data Subject before the restriction of Processing is lifted.

---

<sup>1</sup> Article 12(3)

#### 5.4 Right to object

The Data Subject shall have the right to object, on grounds relating to their particular situation, at any time to Processing of Personal Data concerning them where the Processing is based on the legitimate interests pursued by the Company.

The Company shall no longer process the Personal Data unless the Company demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

Data Subjects shall have the right to object to the Processing of Personal Data for direct marketing purposes at any time. Where the Data Subject objects to Processing for direct marketing purposes, the Personal Data shall no longer be processed for such purposes.

### 6 **Third Party Service Providers**

6.1 Where the Company instructs a third party to process personal data its behalf (a third party Data Processor), the Data Processor must enter into a written agreement with the Company that:

- (a) provides details of the processing of Personal Data that they are being instructed to carry out;
- (b) requires the third party to process the Personal Data only in accordance with the Company's written instructions and to the extent necessary for them to fulfil their obligations to the Company under the agreement;
- (c) requires the third party to implement appropriate technical and organisational measures and controls to ensure the confidentiality and security of the personal data; and
- (d) imposes any additional data processing obligations required by the Data Protection Legislation.

6.2 The data processing agreement should be signed by both parties before any Personal Data is transferred to the Data Processor.

6.3 Any party making amendments or unable to adhere to the data processing agreement should be referred to the Board before the agreement is signed.

6.4 When contracting with a Data Processor, it is important that the Company conducts appropriate due diligence both at the outset of the relationship and on a periodic basis. The due diligence should ensure that the Data Processor is capable of complying with the requirements of the written agreement as detailed above.

### 7 **Co-operation with supervisory authorities**

7.1 The Company shall cooperate, on request, with the relevant supervisory authority in the performance of its tasks.

7.2 The relevant supervisory authority for the Company is the Data Protection Commission in Ireland (the "**Supervisory Authority**").

### 8 **Keeping records of all Processing**

8.1 The Company shall maintain accurate and complete records of all the Processing activities it undertakes directly. This requires that the Company determine what Personal Data it holds, where it came from and who the Company shares it with. Similarly each Data Processor will be required to maintain accurate and complete records of all Processing activities it undertakes directly.

8.2 A record of the Company's Processing activities is contained in Appendix I.

8.3 The Company will retain Personal Data for a period of up to seven years following the Data Subject's disinvestment from the Company or at the point from when the business relationship with the Company has ceased. Information may be retained for a longer period where this is necessary for compliance with a legal obligation or for the establishment, exercise or defence of a legal claim. The Company and its duly authorised delegates will refrain from collecting any further Personal Data and shall take appropriate steps to dispose of any records containing Personal Data, to the extent that this is operationally feasible and proportionate.

## 9 **Reporting of Personal Data breaches**

9.1 If the Company detects and records a Personal Data breach, it shall notify the Supervisory Authority without delay, and in any case not later than 72 hours, unless the breach is unlikely to result in a risk to the rights of the Data Subject. A notification template is set out in Appendix II.

9.2 Each Data Processor shall notify the Company without undue delay after becoming aware of a Personal Data breach and shall include in any such notification the applicable information referred to in the Data Protection Legislation (as set out in Appendix II) and shall provide all reasonable assistance to the Company in connection with any such Personal Data breach, including in particular facilitating the Company communicating details of any Personal Data breach to the relevant Data Subject if required, as described at sub-paragraph 9.4.

9.3 The Company shall document all Personal Data breaches, comprising the facts relating to the Personal Data breach, its effects and the remedial action taken.

9.4 Unless one of the conditions set out in sub-paragraphs (a) to (c) below are met, the Data Subject must also be notified without undue delay if the Personal Data breach is likely to result in a high risk to their rights and freedoms. The notification shall describe in clear and plain language the nature of the breach, the name of the contact point where more information can be obtained, the likely consequences and measures taken to mitigate or address the breach.

Notification to the Data Subject is not required in any of the following circumstances:

- (a) where the relevant Personal Data is encrypted/protected in a manner making it unintelligible to unauthorised persons;
- (b) where the Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the Data Subject resulting from the breach is no longer likely to materialise;
- (c) where an individual notification would involve disproportionate effort (e.g. public communication or similar is sufficient).

## 10 **Board Oversight and Updates to this Policy**

10.1 The Board will be responsible for the oversight of compliance with this Policy. It will review the appropriateness of this Policy annually and will ensure that it is operating as intended. It will also review this Policy to ensure that it continues to be compliant with applicable national and international regulations, principles and standards.

10.2 This Policy shall be reviewed and updated as necessary on at least an annual basis or as and when is required or deemed necessary by the Company. Material changes to this Policy will be approved by the Board.



**Appendix I – Records of Processing activities in accordance with Article 30 of the Data Protection Legislation**

**The Data Controller**

Name and contact details of Data Controller	Guggenheim Global Investors plc and CorporateDataPrivacy@GuggenheimPartners.com.
The purposes of Processing	As outlined in the Privacy Notice
The categories of Data Subjects	Individual investors and individuals connected to institutional investors that provide the Company with Personal Data (for example directors, trustees, employees, representatives, shareholders, investors, clients, beneficial owners or agents)
The categories of Personal Data	Name, residential address, email address, contact details, corporate contact information, signature, nationality, place of birth, date of birth, tax identification, credit history, correspondence records, passport number, bank account details, source of funds details and details relating to investment activity.
The categories of recipients in the EU	<ul style="list-style-type: none"> <li>- the administrator, BNY Mellon Fund Services (Ireland) Designated Activity Company;</li> <li>- Duff &amp; Phelps (Ireland) Limited and its affiliates;</li> <li>- the distributor, Guggenheim Investment Advisors (Europe) Limited;</li> <li>- the auditor, KPMG;</li> <li>- the company secretary, MFD Secretaries Limited;</li> </ul> and their respective affiliates and delegates.
The categories of recipients in third countries	<ul style="list-style-type: none"> <li>- the investment manager, Guggenheim Partners Investment Management LLC;</li> </ul> and their respective affiliates and delegates.
The categories of recipients who are international organisations	N/A
Suitable safeguards in the case of transfers in line with Article 49(1) of the Data Protection Legislation	N/A
Time limits for erasure of Personal Data	Refer to the Privacy Policy, " <i>Our Retention of your Personal Data</i> "
A general description of the technical and organisational security measures in place	N/A – no data held directly by the Company.

**Appendix II – Notification Letter Template (required information under Article 33 of the Data Protection Legislation)**

Data Protection Commission  
Canal House  
Station Road  
Portarlinton  
Co. Laois

[insert date]

Dear [ ]

**Notification of Breach**

[Insert a description of 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].

[Insert the name and contact details of the data protection officer or other contact point where more information can be obtained].

[Insert a description of the likely consequences of the Personal Data breach].

[Insert a description of the measures taken or proposed to be taken by the Data Controller to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects].

Yours sincerely