abrdn III ICAV
Data Protection Policy
September 2022

1. Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) (the **"GDPR"**) replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46EC. Its purpose is to protect the rights and freedoms of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge.

The GDPR and supplemental national data protection laws in Ireland, which consist primarily of the Data Protection Acts 1988 to 2018, will be collectively referred to as the "Data Protection Legislation" that apply to the Company.

Adherence to Data Protection Legislation on its own is not sufficient, companies must be able to demonstrate their compliance with Data Protection Legislation in order to fully comply.

abrdn III ICAV (the "Fund") is regulated by the Central Bank of Ireland and has adopted this data protection policy (the "Policy") to describe its obligations under the Data Protection Legislation and its internal procedures to ensure that it respects the rights of data subjects of the Fund, with regard to the way in which their personal data is handled.
For the avoidance of doubt, the Fund has adopted the Policy and not abrdn plc's data protection policy.

As a regulated entity, the Fund and its delegates and affiliates have to collect, store and process certain Personal Data about investors, beneficial owners, directors, employees, trustees, service providers and other third parties for the purposes of its operations and adhering to its legal and regulatory obligations.

The Fund's Data Protection Manager maintains a data inventory of all data processing activities that are carried out by and on behalf of the Fund.

The Board has ultimate responsibility for ensuring that the Fund complies with its obligations under Data Protection Legislation and as such this Policy will be reviewed at least annually by the Board to ensure appropriateness. Additional updates and ad hoc reviews may be performed as and when required to ensure that any changes to the Fund's organisational structures / business practices / Fund Service Providers or changes in Data Protection Legislation are properly reflected in the Policy.

This Policy should be read in conjunction with associated and supporting documents as produced by the Fund from time to time. It should also be read in conjunction with all other relevant policies of the Fund, including in particular the Cyber Security Policy of the Fund.

2. Definitions

"Controller" means a natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of personal data. The Fund generally acts as a Controller of personal data.

"**Processor**" means a natural or legal person who processes personal data on behalf of the controller such as a fund administrator, distributor and/or other delegates of the Fund.

"**Data Subject**" means an identified or identifiable natural person from whom or about whom personal data is processed such as an investor in the Fund.

"**Personal Data**" means any information relating to an identified or identifiable natural person. For example, 'Know Your Client' documentation which may include personal data such as residential addresses, email addresses, places of birth, dates of birth, bank account details and details relating to investor investment activity, including business and personal information of individuals to the extent relevant to such activity.

"**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, including collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing, disseminating, erasing or destroying it.

3. Data Protection Principles

The Fund adheres to core data protection principles, namely:

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

In addition, the Fund adheres to the accountability principle, by taking responsibility for, and being able to demonstrate compliance with, obligations under applicable Data Protection Legislation.

3.1 Lawful, fair and transparent Processing

The Fund is required to process Personal Data lawfully, fairly and in a transparent manner in relation to the data subject.

The Fund generally meets these requirements in relation to investors through a privacy notice contained in the application form and a summarised disclosure contained in its prospectus. For other categories of data subjects, such as employees and officers of the Fund, the Fund meets these requirements via privacy notices made available to them, for example when they join the Fund.

The Fund ensures that all information and communications relating to the Processing of Personal Data are clear, concise, transparent, intelligible, easily accessible and easy to understand using clear and plain language[1]. The Fund ensures that these transparency requirements are adhered to at all stages of the collection and Processing of Personal Data.

The Fund generally relies on performance of a contract, legal obligation and legitimate interests as its main lawful bases for Processing of Personal Data. Where relying solely on legitimate interests, the Fund will conduct an assessment to ensure that the processing activity is necessary; and balanced against the rights and freedoms of the Data Subject. The Fund generally does not intend to rely upon consent as the lawful basis for the processing of personal data. Under Article 9 of the GDPR, where the Fund processes any special categories of Personal Data (such as health data), it must have a legitimising condition for doing so under Article 9 or relevant provisions of the Data Protection Act 2018. The Fund generally does not collect or process any special categories of Personal Data, except limited quantities of health data in relation to the Fund's own personnel to the extent that this is relevant to their relationship with the Fund (e.g. in connection with absence from work due to illness). Where the Fund processes special categories of Personal Data, it does so in compliance with applicable provisions in the GDPR and the Data Protection Act 2018.

3.2 Purpose Limitation

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

a) where this is necessary for the performance of the contract to purchase shares in the Fund;
b) where this is necessary for compliance with a legal obligation to which the Fund is subject (such as the anti-money laundering obligation to verify the identity of the Fund's customers (and, if applicable their beneficial owners) or the prevention of fraud); and/or

c) where this is necessary for the purposes of the legitimate interests of the Fund or a third party (such as direct marketing and analysing Personal Data for quality control, business and statistical analysis, tracking fees and costs, training and related purposes). Such legitimate interests are not overridden by a Data Subject's interests, fundamental rights or freedoms.

The Fund will not process Personal Data in a manner that is incompatible with those communicated with Data Subjects. If the Fund is considering any new activity or implementing any new initiative that will involve changing the way that the Fund processes Personal Data, it will decide whether a data protection impact assessment or privacy impact assessment should be carried out in accordance with Data Protection Legislation and related guidance.

3.3 Data Minimisation

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

3.4 Accuracy

The Fund will take reasonable steps to 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 Fund will take all reasonable steps to amend inaccurate or out-of-date Personal Data without delay upon becoming aware of this.

3.5 Storage Limitation

The Fund 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 Fund will be clear when informing the Data Subject about how it determines the length of time for which Personal Data will be kept and the reason why the information is being retained. The Fund will take into account any required statutory retention periods that give rise to an obligation to retain a Data Subject's Personal Data for fixed periods and ensure that Personal Data is retained in line with such statutory requirement(s).

3.6 Integrity and Confidentiality

Processing will be conducted in a manner that ensures appropriate security and confidentiality of Personal Data. The Fund must secure Personal Data from unauthorised access by third parties, alteration, disclosure, accidental loss, destruction or any form of computer corruption. The Fund will seek assurances from any service providers that act as Processors for the Fund that they have implemented appropriate information security measures which may include, but are not limited to:

- Access to IT servers is restricted in a secure location to a limited number of staff;
- Access to systems is password protected;
- A back up procedure is in operation;
- Manual files containing Personal Data, financial information or Fund confidential information are not viewable; and
- A strong emphasis is placed on the security of Personal Data when it is held on portable devices.

3.7 Accountability

The Fund takes its responsibility to comply with applicable Data Protection Legislation seriously and maintains this Policy and the practices referred to in this Policy for this purpose. The Fund also ensures that it can demonstrate its compliance with its obligations under applicable Data Protection Law. The Fund achieves this by maintaining applicable records, policies and procedures which demonstrate its compliance.

4. The Fund as Controller

The Fund is a Controller and takes appropriate measures to comply with its obligations as such under Data Protection Legislation. The Fund often engages third parties to process Personal Data on behalf of the Fund and when they do so, such third parties generally act as Processors.

Where two or more controllers jointly determine the purposes and means of processing, they will be joint controllers.

When Processing Personal Data, there may also be times where service providers to the Fund (for example, the administrator) will be required to use Personal Data for their own, in which case they will be characterised as other Controllers of that Personal Data.

4.1 Fund Service Providers

The Fund operates on a delegated model under which the Fund's Service Providers are appointed to provide certain services to the Fund. In the provision of the services to the Fund, the Fund Service Providers process personal data on behalf of the Fund and as a result constitute "processors" of the Fund.

It is the Fund's policy to ensure that Processors have implemented appropriate technical and organisational measures to ensure there are appropriate safeguards to comply with the GDPR.

The Data Protection Manager on an ongoing basis keeps the Fund's Board of Directors (the **"Board"**) apprised of updates in relation to data protection legislation and guidance relevant to the Fund's operations issued by the Data Protection Commission ("**DPC**"). and the European Data Protection Board ("**EDPB**"). Further details regarding the Data Protection Manager's role are set out below.

The Fund ensures that it has a written agreement with each Fund Service Provider that acts as a Processor on behalf of the Fund which contains appropriate contractual provisions governing the processing of Personal Data by that Fund Service Provider on behalf of the Fund as required under Data Protection Legislation. These provisions include a contractual right to obtain all relevant information from that Fund Service Provider which is necessary in order for the Fund Service Provider to demonstrate its compliance with the data protection obligations set down in the contract. Furthermore, the Fund may carry out an audit or inspection of the relevant Fund Service Provider for such purposes.

5. Data Subject Rights

A Data Subject has the following rights under the GDPR:

5.1 Right to be Informed

Right to obtain, at the point data is first collected, information about the identity and contact details of the controller or representative, contact details of the Data Protection Officer "DPO," purposes of processing, legitimate interests where applicable, recipients of the data, retention period, data subject rights, lawful basis, and details of any automated decision-making or profiling.

5.2 Right of Access

Confirmation from the Fund as to whether or not Personal Data concerning them is being processed. Where the Fund is Processing their Personal Data, the Data Subject has the right to access such Personal Data as well as the purpose of the Processing, the categories of Personal Data concerned; the persons or categories of persons to whom the Personal Data may be disclosed, in particular recipients in third countries or international organisations; the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period, the existence of their data subject rights, and the right to lodge a complaint with the Data Protection Commission or another competent data protection authority.

The Fund will not charge a fee for complying with a Data Subject's access request unless it can be demonstrated that the cost will be excessive. In such cases, a reasonable fee may be applied.

The information shall be provided without delay and within one month. Where requests are complex, the Fund may extend the deadline for providing the information by a further two months. However, it shall in any event respond to the request within a month, explaining why the extension is necessary.

A request may be made by an individual, such as an investor or a director of a Fund and may be made in electronic format as well as by written request to the privacy contact at the Fund.

5.3 Right to rectification

A Data Subject has the right to have inaccurate personal data that the Fund holds in relation to them rectified. The Fund will comply with any valid request for rectification without undue delay.

5.4 Right to be forgotten

A Data Subject has 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. The Fund will comply with any valid request for erasure, subject to applicable exemptions provided for in Data Protection Legislation.

5.5 Right to the restriction of Processing

A Data Subject has the right to require that the Fund restricts Processing of their 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.

Where Processing has been restricted, such Personal Data shall, with the exception of storage, only be processed with the Data Subject's consent and the Fund is required to inform the Data Subject before the restriction of Processing is lifted. The Fund will comply with any valid request for restriction of Processing, subject to applicable exemptions provided for in Data Protection Legislation.

5.6 Right to object

A Data Subject has 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 legitimate interests pursued by the Fund or a third party.

In such circumstances the Fund shall no longer process the Personal Data unless it 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. The Fund will comply with any valid objection to the Processing of Personal Data, subject to applicable exemptions provided for in Data Protection Legislation.

A Data Subject has the right not to be subjected to processing which is wholly automated and which produces legal effects or otherwise which significantly affects an individual, unless one of a limited number of exemptions applies.

The Fund does not envisage engaging in any such automated decision making.

In addition to the above, Data Subjects have the right to lodge a complaint with the Data Protection Authority.

6. Personal Data Breaches

The GDPR defines a personal data breach as a 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.

Whether any data security incident ("**Data Incident**") giving rise to a suspected Personal Data Breach involves Personal Data must be determined on a case-by-case basis. If a Data Incident does not involve Personal Data, it is not a Data Breach. Furthermore, not all Data Incidents involving Personal Data will be Data Breaches, for example where:

- Personal Data is securely encrypted or anonymised such to make the Personal Data unintelligible; and/or

- There is a full, up-to-date back up of the Personal Data (in cases of accidental destruction).

Article 33 of the GDPR requires that all Personal Data Breaches must be reported by a Controller (i.e. the Fund) to the DPC without undue delay and where feasible not later than 72 hours after the Fund having become aware of the Personal Data Breach unless it is unlikely to result in a risk to the rights and freedoms of the affected Data Subjects. Where a Personal Data Breach is notified to the DPC but not within such 72 hour period, it shall be accompanied by reasons for the delay.

Article 34 of the GDPR requires that any Personal Data Breach that is likely to result in a high risk to the rights and freedoms of the affected Data Subjects must be communicated to those individuals without undue delay.

Where any actual or potential Personal Data Breach involving Personal Data in respect of which the Fund acts as a Controller occurs, in addition to seeking to mitigate the impact of the incident, the Fund will need to assess the incident and determine:

- Whether it is a Personal Data Breach;
- Whether it must be notified to the DPC; and
- Whether it must be communicated to the affected individuals.

When doing so, the Fund will take into account Data Protection Legislation and related guidance regarding the assessment of risk to the affected individuals (both to determine whether the Personal Data Breach must be notified to the DPC and to determine whether it must be communicated to the affected individuals).

The Fund needs to ensure that Processors that are processing the Personal Data on behalf of the Fund have agreed to notify the Fund as soon as possible of any Personal Data Breaches so that the Fund can decide what it needs to do in relation to such incidents. It is the Fund's policy to include appropriate contractual obligations on Processors to notify the Fund of such incidents promptly.

Details of any actual or potential Personal Data Breach involving Personal Data in respect of which the Fund acts as a Controller should be sent to the following email address to allow the Data Protection Manager and the Fund to review the nature of the breach and to determine next steps:

gdprservice@carnegroup.com

The Data Protection Manager and the Board will assess whether a Data Breach has reached the threshold to be reported to the DPC. If a Personal Data Breach must be notified to the DPC, specific details must be provided to the DPC by completing and submitting an online form. The type of information required to be provided includes:

- Date and time breach occurred;
- Date and time breach was identified/reported;
- Details of the Data Subjects affected by the Breach;
- Details of the types of Personal Data contained in the Breach e.g. amount of data, any sensitive data;
- Explanation of the breach and details of what caused it to happen;
- Technical and Organisation measures in place at time of breach and subsequently; and
- Summary of actions taken to remediate or mitigate risks to the Data Subjects affected.

The DPC has published a guide regarding notifying it of Personal Data Breaches, which is available at www.dataprotection.ie/en/guidance-landing/breach-notification-practical-guide

The Data Protection Manager and the Board will assess whether Data Subjects should be notified of a Personal Data Breach taking into account the criteria set down in Article 34 of the GDPR.

The Data Protection Manager will maintain on behalf of the Fund a register of all Data Incidents and Personal Data Breaches.

Where a Personal Data Breach occurs, the Data Protection Manager will work with the Board and where necessary, the relevant Fund Service Provider, to implement measures to avoid a similar Personal Data Breaches occurring in the future.

7. Transferring Personal Data to a country outside the EEA

Under Data Protection Legislation, Personal Data generally may not be transferred outside the European Economic Area unless an exception to this general prohibition can be relied on. The permitted exceptions include: (a) where the third country to which the Personal Data is to be transferred is the subject of an adequacy decision by the European Commission, which allows the free flow of Personal Data from the EEA to that third country. A list of Adequacy decisions can be found on the Commission's website https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, or
(b) where the transferring Controller or Processor has provided appropriate safeguards for Personal Data and there are enforceable Data Subject rights and effective legal remedies available to Data Subjects; or
(c) where limited derogations apply, such as where the explicit consent of the Data Subject has been obtained, or where the transfer is necessary for the performance of a contract with the Data Subject, or for the exercise of legal claims or for important reasons of public interest.

Appropriate safeguards may be provided for, in part, by:

- Standard Contractual Clauses between the data exporter and the data importer: the Commission has adopted three sets of model clauses which are available on the Commission's website https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en;
- Binding corporate rules: these are legally binding data protection rules approved by the competent data protection authority which apply within a corporate group;
- Approved codes of conduct together with binding and enforceable commitments of the controller or processor in the third country;
- Approved certification mechanisms together with binding and enforceable commitments of the controller or processor in the third country.

The Fund anticipates transferring Personal Data to entities located both within and outside of the EEA and authorised delegates such as the Fund's administrator, investment manager, distributor and their respective affiliates, some of which may include entities located outside of the EEA. Any transmission of Personal Data by the Fund outside the EEA shall be in accordance with the requirements of the Data Protection Legislation.

8. Responsibility for Data Protection Matters

The Fund has determined that as it does not regularly and systematically monitor Data Subjects on a large scale, it is not currently required to appoint a Data Protection Officer. However, in order to ensure the Fund's compliance with its obligations under the Data Protection Legislation, the Fund has determined to appoint a Data Protection Manager to act as primary contact and coordinate actions required in respect of the Fund's obligations under Data Protection Legislation. The decision not to appoint a Data Protection Officer will be kept under review and a data protection officer may be appointed in the future to the extent required.

8.1 The Role of Carne as the Data Protection Manager

Sinead Phelan has been appointed to act as Data Protection Manager to the Company. Ms Phelan is an employee of Carne Global Financial Services Limited ("Carne") and her role and responsibilities are set out below and also within the Engagement Letter – Data Protections Support Services between the Company and Carne.

In general terms, Data Protection Support in respect of the Fund includes:

- Assist the Fund with the completion and maintenance of a record of processing activities (often referred to as a data inventory);
- Assist the Fund with creating and maintaining a data protection policy;
- Carrying out due diligence on the key Processors engaged by the Fund (e.g. Administrator) to ensure that the processing carried out on the Fund's behalf is done in line with the agreements in place and in line with GDPR;
- Reporting of Personal Data Breaches to the DPC where required under Data Protection Legislation;

- Maintenance of a Data Breach Register;
- Assisting the Board with any requests from Data Subjects (such as Data Subject access requests);
- Reporting to the Board on a quarterly basis including details of any breaches, status of due diligence, policy updates and regulatory guidelines and industry best practice;
- Providing data protection guidance to the Board where required.

8.2 Training

The Data Protection Manager will provide guidance to the Board in respect of any updated guidance or training materials from the DPC and EDPB as required as part of the regulatory updates at each Board meeting. Processors are required to provide appropriate data protection training to their staff to ensure that they handle Personal Data in line with the GDPR requirements.