CORUM Butler Asset Management Limited

(the "Company")

GDPR Policy

4 December 2025

Version	Date	Comment
1.0	31 July 2019	Board Approval
2.0	25 March 2020	Annual review
3.0	8 September 2021	Annual review
4.0	6 September 2022	Annual Review
5.0	6 September 2023	Annual Review and enhancement to include, inter alia, DPO appointment
6.0	22 May 2024	DPO change
7.0	19 November 2024	DPO change and general refresh
8.0	4 December 2025	Annual review

Contents

1. Definitions and key concepts

GDPR - Regulation (EU) No. 2016/679 replaces Directive 95/46/EC ("General Data Protection Regulation").

Breaches – breaches of the regulations must be reported to the Data Protection Commissioner within 72 hours. Also, the Regulations give rise potential fines for breaches of the Regulations up to a total of €20m (or 4% of total annual global turnover, whichever is greater).

Data Controller - Natural or legal person which determines the purposes and means of the Processing of Personal Data.

Data Processor - Natural or legal person which Processes Personal Data on behalf of the Data Controller.

DPO – Data Protection Officer.

DPA – Data Protection Authority (Data Protection Commissioner in Ireland).

DPIA – the Data Protection Impact Assessment is the process identifying and mitigating data protection risks. If a processing activity is likely to result in a high risk to individuals, a DPIA will be performed with the main goal of minimising the identified and predicted risks of the processing activity.

Data Subject consent – clear, unambiguous, specific and freely given indication of the data subject's agreement to the processing of personal data relating to them. The provision of consent must also be easily evidenced by the data controller.

Data Subject Rights – their right to access information held, data portability, right to be forgotten i.e. withdrawal of consent for which the data controller must provide information on action taken to comply with that request.

ICAV's - Company' Funds under Management

Personal Data – any information relating to an identifiable natural person ("data subject") who can be identified from that data.

Processing - Any operation which is performed on Personal Data including but not limited to collecting, storing, using, recording, disclosing, transferring or deleting personal data.

Timelines – Data controllers must comply with requests from data subjects within a shorter timeframe (no undue delay and must be concluded within one month).

2. Introduction

This policy sets out the process for adherence to the provisions of the GDPR by the Company and its employees.

As a Data Controller, the Company must comply with all applicable laws and regulations relating to the processing of personal data and privacy, including the Data Protection Act 1998-2018 (as may be amended or supplemented from time to time) and from 25 May 2018, the EU's General Data Protection Regulation 2016/679 (the "GDPR") (together the "Data Protection Legislation").

Under Article 24(1) of the GDPR, the Company as a Data Controller, should implement an appropriate data protection policy as part of the organisational and technical measures it puts in place to demonstrate compliance with the GDPR.

This Policy describes how personal data must be collected, handled, stored, disclosed and otherwise "processed" to meet the Company's data protection standards and to comply with the Data Protection Legislation.

The Company is responsible for and shall be in position to demonstrate compliance with this Policy. This includes ensuring that Fund Service Providers (as defined below) who process personal data on its behalf are acting in accordance with Data Protection Legislation.

3. Data Controller/Data Processor

The Company operates a model where the majority of services are delegated to Service Providers who confirm their own compliance with GDPR. Each Service Provider has been classified as either a Data Controller or a Data Processor. A Data Controller determines the purpose and means of data processing, while a Data Processor simply processes the personal data on behalf of the Company

The Company is the Data Controller and as Data Controller, the Company must ensure the following with respect to personal data:

- It is processed lawfully, fairly and transparently;
- It is only collected for specific and legitimate purposes;
- It must be adequate, relevant and limited the minimum data necessary for the purpose for which it is collected;
- It is only kept for such period as is necessary e.g. at least 6 years following the cessation of relationship with that data subject;
- It must be processed with due care and be protected against any unlawful use, accidental loss or damage.

The Company may also transfer personal data to a Fund Service Provider which such Fund Service Provider may process on its own behalf in the capacity of a data controller provided that it has a lawful basis for that processing. In such circumstances, the Company will seek assurances from the relevant Fund Service Provider that it is processing the relevant personal data for its legitimate interests or in order to comply with a legal obligation to which it is subject.

Agreements currently in place between the Company and the Fund Service Providers reflect the provisions of GDPR where necessary.

When contracting with a third-party data processor, the Company shall conduct appropriate due diligence both at the outset of the relationship and on a periodic basis. The annual due diligence requirement will be scheduled as an event in the annual Compliance Calendar of the Board of the Company. The due diligence shall seek to ensure that the third-party data processor is capable of complying with the requirements of the written agreement as detailed below under "Article 28(3) Data Processing Agreements". In particular, the Company shall obtain sufficient guarantees that the relevant Fund Service Provider will implement appropriate technical and organisational measures to ensure that the processing conducted by such Fund Service Provider will meet the requirements of the GDPR.

Each Service Provider shall provide confirmation on their GDPR processes to the Company on at least an annual basis (e.g. in occasion of the annual Due Diligence with the Delegates/Service Providers). The Company's escalation procedures have been updated to allow for the notification of requests from data subjects to the various Fund Service Providers to be reported to the Board.

4. The Register of Processing Activities

In accordance with Article 30 if the GDPR, the Company shall maintain a register of personal data held by it or on its behalf by one of the appointed Fund Service Providers ("**the Register**"). The Register will contain, among other info, the following:

- What personal data is held;
- For what purpose is the data held and is it lawful under GDPR;
- Where that data is held;
- The description of the categories of the data subject and of the categories of personal data;
- Whether data is transferred, if so, to whom and if it is transferred to entities outside the EEA*;
- How long data is held for;
- The security measures applicable for the protection of the data;
- The envision time limits for erasure for different categories of data.

Where data is transferred outside the EEA, measures are taken to ensure equivalent safeguards are in place. This register is maintained and updated at least on an annual basis by the Compliance Function and validated by the DPO.

The Compliance Function will keep the register up to date and document a DPIA whenever the updates made to the register make a DPIA necessary.

5. DPO Role and Responsibilities

The DPO, appointed at Group Level, assists the Company in its role as Data Controller in managing the protection of personal data. In particular, the DPO must:

- inform and advise the Data Controller and/or Data Processor, as well as their employees, of their obligations under data protection legislation;
- monitor Compliance of the organisation with all legislation in relation to data protection, including in audits, awareness-raising activities as well as a mandatory training for all new employee ;
- provide advice where a DPIA has been carried out and monitor its performance;
- act as a point of contact for requests from data subjects regarding the processing of their personal data and the exercise of their rights;
- cooperate with DPAs and act as a contact point for DPAs on issues relating to the processing.

The DPO reports directly to the Board of Directors of the Company and shall present an annual report including all activities performed during the year and those planned for the following year.

6. Data Subject Communication/Data Privacy Notice

The data subjects within the Company employees and Directors, have been notified of the GDPR impact to their data held by the Company and their rights in that regard, including the legal basis for the processing of their data, their rights under GDPR e.g. right to complain or to withdraw their consent and the time frame in which their data will be retained.

The Company or any Service Provider who receives a data request from a data subject in relation to personal data which they process on behalf of the Company will notify the Data Protection Coordinator immediately. The Data Protection Coordinator shall then immediately inform the DPO who will then notify the Board and will ensure that such requests from a data subject requesting information on data held are appropriately responded to within 1 month of receipt of that request.

For new investors to the underlying ICAV's, this information is included in, but not limited to an updated subscription document. Existing investors who will not necessarily have sight of the updated subscription document and prospectus have been sent a Data Privacy Notice on behalf of the underlying ICAV's advising them of the new information relevant to the Regulations.

7. Data Retention & Disposal

GDPR data retention rules, in general, require any personal data that is collected or processed by the Data Controller and Data Processor to be kept only for the necessary time period required to achieve the purpose for which the information was collected.

The Company, in its role as Data Controller, should ensure that personal information is securely deleted or returned when it is no longer required. In accordance with art. 39 of the GDPR, the Data Controller is required to establish time limits for data retention and to ensure the erasure of records when they are no longer required.

Under certain circumstances, personal data may be retained for longer time periods, even though the information is no longer required for its original purpose, such as to ensure compliance with additional regulatory requirements. In this respect, a dedicated Records and Retention Policy is in place within the Company and shall be read in conjunction with this Policy.

In order for data to be erased, the Data Controller must know and map all personal data treated and where these are stored. The Company's Register of Processing Activities, in section 4, includes the aforementioned information.

Data disposal is the process of securely removing or destroying personal data when it is no longer needed. To avoid improper disposal, which may lead to breaches of individual's privacy, the Data Controller must ensure to have in place a robust disposal mechanism for physical (e.g. paper documents stored in loco) and digital (IT Service outsourced at Group Level) type of personal data retained.

8. Breaches

The Company and the Company's Fund service providers have in place procedures to identify breaches of data protection and, where such breach occurs in connection with personal data which they process on behalf of the Company, will notify the Company of any such breaches without undue delay. The Company will ensure all data breaches in relation to personal data of investors or Fund Service Providers and their affiliates (or their respective employees, partners, officers, agents and service providers), for which the Company is a Data Controller, is recorded on the companies Data Protection Breach Log and shall be communicated to the DPO and upon the determination of the DPO will notify to the Data Protection Commissioner within 72 hours of that breach being identified. The Company shall appoint a contact (Data Protection Coordinator) for all relevant correspondence within the Company and with the DPO. The DPO will be responsible for all communication with the Data Protection Commission. Contact details for the DPO and Data Protection Coordinator are noted in Section 9 below.

9. Escalation

Any Service Provider of the Funds under management or third parties providing services to the Company, who become aware of a Data breach in connection with Personal Data which they process on behalf of the Company and/or Fund shall without undue inform the Company's Data Protection Coordinator (the Company's Head of Compliance Function), who will then inform the DPO who will then inform the Board. The DPO, who will co-ordinate notification to the Data Protection Commissioner, shall gather all relevant information concerning the breach.

Data subjects may also use the below contacts for any data requests. These will be processed with undue delay.

Company GDPR Email: DPO@corumbutler.com

DPO: Marine Marois (DPO at Group Level)

Employees of the Company becoming aware of any Personal Data Breach, will follow the procedure in Appendix 1. Same escalation process will follow then.

10. Compliance with Regulation

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 Company's organizational structures/business practices/Service Providers are properly reflected in the Policy.

All changes made will be communicated to and confirmed by the Board.

The Board of Directors of the Company has ultimate responsibility for ensuring that the Company complies with its obligations under Data Protection Legislation.

Appendix 1 – Internal process

List of internal processes:

- Procedure for data breach
- Procedure for handling rights requests
- Procedure for retention of customer and prospect data
- Procedure for securing communications
- GDPR Group internal policy

All procedures are detailed on the Intranet. You can have access here.