STRICTLY PRIVATE AND CONFIDENTIAL

CIBUS CAPITAL LLP: DATA PROTECTION POLICY

This Summary is not exhaustive, supersedes any earlier procedures, is current as of the above date and may be varied or amended by management from time to time as circumstances dictate.

This document is confidential, provided for informational purposes only and is not legally binding on Cibus or any of its affiliates. Cibus accepts no responsibility to any third person in connection with, and no third person shall have any right to enforce, any performance or non-performance of any of the provisions of this document.

In no event shall this document constitute or be considered as advice or solicitation to invest in any specific investment or fund advised by Cibus or its affiliates, nor should this document be relied upon in making any investment decision. The information contained in this document shall not be considered as legal, tax or other advice.

This document is liable to change at any time, without notice.

CIBUS
CAPITAL
LLP

Data Protection Policy

Cibus Capital LLP

Adoption Date:	11 November 2025
Approved By:	Jeremy Alun-Jones
Owner:	DPO and Legal Team

1. **DEFINITIONS**

"Automated Decision-Making" means when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

"Automated Processing" means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing, as are many uses of artificial intelligence (AI) where they involve the processing of Personal Data.

"Consent" means agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

"Controller" means the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. The LLP is the Controller of all Personal Data relating to its Company Personnel and Personal Data used in its business for the LLP's own commercial purposes.

"Criminal Convictions Data" means personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

"Data Subject" means a living, identified or identifiable individual about whom the LLP holds Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

"Data Privacy Impact Assessment" or "DPIA" means tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

"Data Protection Officer" or "DPO" means Jeremy Alun-Jones.

"Explicit Consent" means consent which requires a very clear and specific statement (that is, not just action).

"UK GDPR" means the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK GDPR.

"LLP" means Cibus Capital LLP.

"Personal Data" means any information identifying a Data Subject or information relating to a Data Subject that the LLP can identify (directly or indirectly) from that data alone or in combination with other identifiers the LLP possesses or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

"Personal Data Breach" means any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that the LLP or its third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

"Privacy by Design" means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

"Privacy Notices" or "Privacy Policies" means separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of:

- general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy); or
- stand-alone, one-time privacy statements covering Processing related to a specific purpose (for example, the VC Newsletter Privacy Notice).

"Processing" or "Process" means any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

"Pseudonymisation" or "Pseudonymised" means replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.

"Related Policies" means the Company's policies, operating procedures or processes related to this Policy and designed to protect Personal Data.

"Special Categories of Personal Data" means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

"Staff" means members/partners, employees, workers, contractors, consultants, agency workers, consultants, directors and others.

2. INTRODUCTION

2.1 This policy applies to the **LLP** and its **Staff**.

2.2 This policy (the **"Policy"**) was adopted on 11 November 2025.

2.3 This Policy is reviewed annually and may be amended on an ad hoc basis if required.

2.4 This Policy sets out how the LLP handles the Personal Data of its Staff, business contacts and other third parties.

2.5 This Policy applies to all Personal Data that the LLP Processes, regardless of the media on which that data is stored or whether it relates to past or present Staff, business contacts or any other Data Subject.

3. **SCOPE**

3.1 The LLP recognises that the correct and lawful treatment of Personal Data will maintain trust and confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that the LLP takes seriously at all times.

3.2 The LLP could be exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the UK GDPR.

3.3 All Staff are responsible for ensuring compliance with this Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

3.4 The DPO is responsible for overseeing this Policy.

3.5 Staff should contact the DPO with any questions about the operation of this Policy or the UK GDPR or if they have any concerns that this Policy is not being or has not been followed. In particular, Staff must always contact the DPO in the following circumstances:

(a) if they are unsure of the lawful basis on which they are relying to process Personal Data (including the legitimate interests used by the LLP) (see paragraph 4);

(b) if they need to rely on Consent or need to capture Explicit Consent (see paragraph 5);

(c) if they need to draft Privacy Notices (see paragraph 6);

(d) if they are unsure about the retention period for the Personal Data being Processed (see paragraph 10);

(e) if they are unsure what security or other measures they need to implement to protect Personal Data (see paragraph 11);

(f) if there has been a Personal Data Breach (paragraph 12);

(g) if they are unsure on what basis to transfer Personal Data outside the UK (see paragraph 13);

(h) if they need any assistance dealing with any rights invoked by a Data Subject (see paragraph 14);

(i) whenever they are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see paragraph 18) or plan to use Personal Data for purposes other than for which it was collected (see paragraph 7);

(j) if they plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see paragraph 19);

(k) if they need help complying with applicable law when carrying out direct marketing activities (see paragraph 20); or

(l) if they need help with any contracts or other areas in relation to sharing Personal Data with third parties (including the LLP's suppliers and consultants) (see paragraph 21).

4. PERSONAL DATA PROTECTION PRINCIPLES

4.1 The LLP adheres to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

(a) processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);

(b) collected only for specified, explicit and legitimate purposes (purpose limitation);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation);

(d) accurate and where necessary kept up to date (accuracy);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (storage limitation);

(f) processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality);

(g) not transferred to another country without appropriate safeguards in place (transfer limitation); and

(h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (data subject's rights and requests).

4.2 The LLP is responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

5. LAWFULNESS, FAIRNESS AND TRANSPARENCY

5.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.2 Staff may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts the LLP's actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that the LLP Processes Personal Data fairly and without adversely affecting the Data Subject.

5.3 The UK GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given their Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet its legal compliance obligations;

(d) to protect the Data Subject's vital interests; or

(e) to pursue the LLP's legitimate interests (or those of a third party) for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which the LLP processes Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

5.4 Staff must identify and document the legal ground being relied on for each Processing activity with the DPO and the LLP's legal team before undertaking the relevant Processing activity.

6. CONSENT

6.1 A Controller must only process Personal Data on one or more of the lawful bases set out in the UK GDPR, which include Consent.

6.2 A Data Subject consents to Processing of their Personal Data if they clearly indicate agreement to the Processing.

6.3 A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if the LLP intends to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.4 When processing Special Category Data or Criminal Convictions Data, the LLP will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, a Privacy Notice must be issued to the Data Subject to capture Explicit Consent.

6.5 Staff will need to evidence Consent captured and keep records of all Consents, so that the LLP can demonstrate compliance with Consent requirements.

7. TRANSPARENCY (NOTIFYING DATA SUBJECTS)

7.1 The UK GDPR requires a Controller to provide detailed, specific information to a Data Subject depending on whether the information was collected directly from the Data Subject or from elsewhere. The information must be provided through an appropriate Privacy Notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

7.2 Whenever the LLP collects Personal Data directly from a Data Subject, including for HR or employment purposes, the LLP must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and DPO, and how and why the LLP will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

7.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), the LLP must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. The LLP must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates its proposed Processing of that Personal Data.

7.4 If a member of Staff is collecting Personal Data from a Data Subject, directly or indirectly, then the Data Subject must be provided with the relevant Privacy Notice.

7.5 If the relevant Privacy Notice does not exist, please contact the DPO and the LLP's Legal Team so that a Privacy Notice can be drafted based on the facts and circumstances.

8. PURPOSE LIMITATION

8.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

8.2 Staff cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless the Data Subject has been informed of the new purposes and they have Consented where necessary.

8.3 If Staff want to use Personal Data for a new or different purpose from that for which it was obtained, please contact the DPO for advice on how to do this in compliance with both the law and this Policy.

9. DATA MINIMISATION

9.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

9.2 Staff may only Process Personal Data when performing your job duties requires it and cannot Process Personal Data for any reason unrelated to your job duties.

9.3 Staff may only collect Personal Data that they require for their job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

9.4 Staff must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised.

10. ACCURACY

10.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay once a member of Staff becomes aware that it is inaccurate.

10.2 Staff must ensure that the Personal Data the LLP uses and holds is accurate, complete, kept up to date and relevant to the purpose for which the LLP collected it. Staff must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. All reasonable steps must be taken to destroy or amend inaccurate or out-of-date Personal Data.

11. STORAGE LIMITATION

11.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

11.2 The LLP will maintain retention policies and procedures to ensure Personal Data is deleted after an appropriate time, unless a law requires that data to be kept for a minimum time.

11.3 Staff must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which the LLP originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements. For example, if an underlying data set needs to be retained but the identities of who the data has come from is no longer needed then the data set should be Pseudonymised.

11.4 Staff will take all reasonable steps to destroy or erase from the LLP's systems all Personal Data that the LLP no longer requires. This includes requiring third parties to delete that data where applicable. For example, once a recruitment process has been completed, Staff should ensure that all CVs and Personal Data of unsuccessful applicants is deleted from the LLP's systems.

11.5 Staff will ensure Data Subjects are provided with information about the period for which data is stored and how that period is determined in any applicable Privacy Notice.

12. SECURITY INTEGRITY AND CONFIDENTIALITY

12.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

12.2 The LLP will develop, implement and maintain safeguards appropriate to the LLP's size, scope and business, available resources, the amount of Personal Data that the LLP owns or maintains on behalf of others, and identified risks (including use of encryption and Pseudonymisation where applicable).

12.3 The LLP will regularly evaluate and test the effectiveness of those safeguards to ensure security of its Processing of Personal Data. Staff are responsible for protecting the Personal Data the LLP holds. Staff must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. Staff must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

12.4 Staff must follow all procedures and technologies the LLP puts in place to maintain the security of all Personal Data from the point of collection to the point of destruction. Staff may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

12.5 Staff must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) **Confidentiality:** only people who have a need to know and are authorised to use the Personal Data can access it (for example, Personal Data relating to HR matters should only be accessible to those members of Staff directly involved in providing HR services);

(b) **Integrity:** Personal Data is accurate and suitable for the purpose for which it is processed; and

(c) **Availability:** authorised users are able to access the Personal Data when they need it for authorised purposes.

12.6 Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the LLP implements and maintains in accordance with the UK GDPR and relevant standards to protect Personal Data.

13. REPORTING A PERSONAL DATA BREACH

13.1 The UK GDPR requires Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject.

13.2 The LLP has put in place procedures to deal with any suspected Personal Data Breach and will notify the Data Subject or any applicable regulator where the LLP is legally required to do so.

13.3 If a member of Staff knows or suspects that a Personal Data Breach has occurred, they should not attempt to investigate the matter themselves and should immediately contact the DPO and the LLP's Operations Team. Staff should preserve all evidence relating to the potential Personal Data Breach.

14. TRANSFER LIMITATION

14.1 The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. Staff transfer Personal Data originating in one country across borders when they transmit, send, view or access that data in or to a different country.

14.2 Staff must comply with the Company's guidelines on cross-border data transfers.

14.3 Staff may only transfer Personal Data outside the UK if one of the following conditions applies (as determined in consultation with the DPO and the LLP's Legal Team):

(a) the UK has issued regulations confirming that the country to which the LLP transfers the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the UK GDPR including:

(i) the performance of a contract between us and the Data Subject;

(ii) reasons of public interest;

(iii) to establish, exercise or defend legal claims;

(iv) to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and

(v) in some limited cases, for its legitimate interest.

15. DATA SUBJECT'S RIGHTS AND REQUESTS

15.1 A Data Subject has rights when it comes to how the LLP handles their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Controller's Processing activities;

(c) request access to their Personal Data that the LLP holds (including receiving a copy of their Personal Data);

(d) prevent the LLP's use of their Personal Data for direct marketing purposes;

(e) ask the LLP to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) object to Processing which has been justified on the basis of its legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the UK;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority; and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

15.2 Staff must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

15.3 Staff must immediately forward any Data Subject request they receive to the DPO and the LLP's Legal Team.

16. ACCOUNTABILITY

16.1 The Controller must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

16.2 The LLP must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Policy or Privacy Notices;

(d) regularly training Company Personnel on the UK GDPR, this Policy, Privacy Notices, and data protection matters including, for example, a Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

17. RECORD KEEPING

17.1 The UK GDPR requires the LLP to keep full and accurate records of all its data Processing activities.

17.2 The LLP must keep and maintain accurate corporate records reflecting its Processing. These records should include the name and contact details of the Controller and the DPO as well as description of the type of Personal Data held and Processed by the LLP.

17.3 All Staff are deemed to have given their informed Consent to the Processing of their Personal Data upon receipt of the Employee Privacy Notice. The LLP shall ensure all Staff receive the Employee Privacy Notice upon commencement of employment and are notified of any updates to the Employee Privacy Notice during the course of their employment. For all Data Subjects other than Staff, Consent is obtained through the inclusion of appropriate data

protection provisions with the relevant contractual documentation governing the relationship between the LLP and such Data Subject.

18. TRAINING AND AUDIT

18.1 The LLP is required to ensure all Staff have undergone adequate training to enable them to comply with data privacy laws. The LLP must also regularly test its systems and processes to assess compliance.

18.2 Staff must undergo all data privacy-related mandatory training.

18.3 Staff must regularly review all the systems and processes under their control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

19. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

19.1 The LLP is required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

19.2 The LLP must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data.

19.3 The Controller must also conduct a DPIA in respect to high-risk Processing.

19.4 Staff should conduct a DPIA with the LLP's Legal Team (and have the findings signed off by the DPO) when implementing major system or business change programs involving the Processing of Personal Data including but not limited to:

(a) use of new technologies (programs, systems or processes, including the use of AI), or changing technologies (programs, systems or processes);

(b) automated Processing including profiling and ADM;

(c) large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data; or

(d) large-scale, systematic monitoring of a publicly accessible area.

20. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

20.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

20.2 If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds (b) or (c) will not be allowed. However, the Special Categories of Personal Data and Criminal Convictions Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

20.3 If a decision is to be based solely on Automated Processing (including profiling), then the Data Subject must be informed when they first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

20.4 The LLP must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and the envisaged consequences, and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

20.5 A DPIA must be carried out with the LLP's Legal Team (and signed off by the DPO) before any Automated Processing (including profiling) or ADM activities are undertaken.

20.6 Where Staff intend to use any generative AI tool that involves profiling or ADM, they must also comply with the LLP's AI Policy.

21. DIRECT MARKETING

21.1 The LLP is subject to certain rules and privacy laws when engaging in direct marketing to third parties (including any limited partners or prospective limited partners of funds advised by the LLP) (for example, when sending marketing emails).

21.2 A Data Subject's prior consent is generally required for electronic direct marketing (for example, by email, text or automated calls). The limited exception is for existing third parties that have provided explicit consent or have made a "soft opt-in" which allows an organisation to send marketing texts or emails without consent if it:

(a) has obtained contact details in the course of a sale to that person;

(b) is marketing similar products or services; and

(c) gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent marketing message.

21.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

21.4 A Data Subject's objection to direct marketing must always be promptly honoured. If a third party opts out of marketing at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

21.5 Staff must consult the DPO and the LLP's Legal Team before undertaking any direct marketing.

22. SHARING PERSONAL DATA

22.1 Generally, the LLP is not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

22.2 Staff may only share the Personal Data the LLP holds with another employee, agent or representative of the Cibus group (which includes funds advised by the LLP and their portfolio companies) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

22.3 Staff may only share the Personal Data the LLP holds with third parties, such as the LLP's service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place;

(d) the transfer complies with any applicable cross-border transfer restrictions; and

(e) a fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.