Prescient

FUND SERVICES (IRELAND)

Data Protection Policy

Version	Date	Created by	Reviewed and approved	Approved date
1	August 2026	PFSI Compliance, Legal and Data Protection Officer	PFSI Board	12 August 2026

Table of Contents

1. Introduction

1.1 **T**he European Union's General Data Protection Regulation ("GDPR") regulates the way in which all personal data is held and processed. 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 GDPR and applicable data protection legislation including the Data Protection Acts 1988-2018 (as amended). The meaning of the terms "personal data" and "processing" are provided in sections 4 and 5 below. This policy is to be read in conjunction with the Prescient Group Data Protection Policy and Prescient Group Artificial Intelligence ("AI") Usage Framework.

1.2 Prescient Fund Services (Ireland) Limited (the "Company") is a private company limited by shares incorporated in Ireland. The Company is authorised and regulated by the Central Bank of Ireland as a UCITS management company and as an alternative investment fund manager, and provides management, administration and related services to a range of collective investment schemes (each a "Fund"). The Company is a data controller in respect of personal data it obtains and/or has obtained from current and former: (i) investors in the Funds (including related personnel), (ii) service providers, delegates, counterparties and governmental and regulatory authorities, (iii) directors of the Company (the "Directors") and employees of the Company, and (iv) clients and prospective clients of the Company, including the promoters and boards of the Funds. The Company may also act as a data processor in its role as fund administrator. PFSI is responsible for ensuring that it uses the personal data of such persons in compliance with GDPR.

1.3 The Company regards the lawful and correct treatment of personal data as integral to the successful operations of the Company, and to maintain the confidence of the people it works with, including investors in the Funds.

1.4 The Company further treats AI governance and privacy governance as a single, integrated obligation. Although AI regulation is not privacy law, AI systems often involve the processing of personal data, therefore such processing activities may be subject to both the EU AI Act (Regulation (EU) 2024/1689) and the European Union's General Data Protection Regulation ("GDPR"). Prescient considers these regimes to be complementary, the EU AI Act governing the safe development, deployment and use of AI systems on a risk-based basis, while GDPR governs the lawful, fair and transparent processing of personal data. Compliance with one regime does not discharge the requirements of the other.

1.5 To this end, the Company fully endorses and adheres to the principles of GDPR.

2. Purpose

2.1 As a data controller, the Company is required to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR.

2.2 The purpose of this policy is to ensure that:

(A) the Directors, employees and anyone else involved in the processing of personal data by the Company are fully aware of, and comply with, the requirements of GDPR; and

(B) data subjects (a "data subject" being a person to whom personal data relates), are aware of their rights under GDPR.

3. Scope

3.1 The Directors, employees and any other authorised third parties who have access to any personal data held by or on behalf of the Company must adhere to this policy.

4. Personal Data

4.1 In this policy, "personal data" includes any data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the Company or its representatives or service providers. In addition to factual information, it includes any expression of opinion about an individual and any indication of the intentions of the Company or any other person in respect of an individual. References to a "data subject" are to an individual whose data is being used.

4.2 Certain personal data is considered to be particularly sensitive and is subject to stricter rules regarding its processing. These categories of personal data are referred to as "sensitive personal data" and include any personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; their physical or mental health condition; details of criminal offences or criminal convictions (including the commission or alleged commission of any offence, any proceedings for any offence committed or alleged to have been committed and the disposal of such proceedings or the sentence of any court in such proceedings) and genetic and biometric data.

4.3 Examples of personal data that the Company might hold include:

(A) information provided to the Company by: (i) investors in the Funds (including related personnel), (ii) service providers, delegates, counterparties and governmental and regulatory authorities, and (iii) Directors and employees of the Company. This might include names and addresses (including proofs of name and address), contact details, dates of birth, gender, nationality, photographs, signatures, occupational history, job titles, income, assets, other financial information, bank details, investment history, tax residency and tax identification information, and, in the case of employees, remuneration, performance and disciplinary records. Such information might be provided in a document, face-to-face, by telephone, by email or otherwise;

(B) information that the Company collects or generates: this might include emails (and related data), and call recordings; and

(C) information that the Company obtains from other sources: this might include information obtained for the purpose of the Company's know-your-client procedures (which include anti-money laundering procedures, counter-terrorist financing procedures, politically-exposed-person checks, sanctions checks, among other things), information from public websites and other public sources.

4.4 The Company only holds personal data which is directly relevant to its dealings with a given data subject. That data will be held and processed in accordance with GDPR and this policy.

5. Processing Personal Data

5.1 The word "process" (and any derivative term) includes any operation that is carried out in respect of personal data, including but not limited to collecting, storing, using, disclosing, transferring or deleting personal data.

5.2 Personal data collected by the Company is generally collected in order to:

(A) assess and process applications for interests in the Funds and other dealings in respect of such interests, including to perform know-your-client procedures, issue

and redeem or withdraw interests, receive payments from and make payments to investors, calculate net asset value, and oversee these processes;

(B) carry out the Company's general business administration, including communicating with investors in the Funds, communicating with service providers and counterparties, accountancy and audit services, risk monitoring, the administration of IT systems, human resources administration (including recruitment, payroll and performance management) and monitoring and improving products and services;

(C) comply with legal and regulatory obligations and industry standards, including know-your-client procedures, the automatic exchange of tax information, legal judgments and the Central Bank of Ireland's fitness and probity regime (including the assessment of individuals performing controlled functions and pre-approval controlled functions); and

(D) share information with the Company's group undertakings, including Prescient Holdings (Pty) Ltd, its subsidiaries and its affiliates (together, the "Prescient Group"), and with the boards, promoters, delegates and other service providers of the Funds, in order that they can undertake business activities relating to the Funds, such as investor relations, discussions with service providers and counterparties, decision-making in relation to the Funds, and business strategy, development and marketing.

5.3 An explanation of the lawful grounds for which personal data may be processed by the Company is provided in section 8 below.

5.4 The Company may not process personal data for any reason other than for the lawful purposes for which it was collected and is being processed.

6. <u>The Data Protection Principles</u>

6.1 Any person processing personal data must comply with the following core principles:

(A) **Lawfulness, fairness and transparency.** Personal data must be processed fairly, transparently and lawfully. The Company must not process an individual's personal data unless it has a lawful ground for doing so and it must inform a data subject of how and why it will process their personal data upon or before collecting it.

(B) **Purpose limitation.** Personal data must be processed only for specified and lawful purposes. Personal data must not be processed in any manner which is incompatible with those purposes.

(C) **Data minimisation.** The personal data that is processed must be adequate, relevant and limited to the minimum data necessary for the lawful purposes for which it is processed.

(D) **Accuracy.** Personal data must be accurate and, where appropriate, kept up-to-date. Any personal data which is incorrect must be rectified as soon as possible.

(E) **Data retention.** Personal data must be kept for no longer than is necessary in light of the lawful purpose(s) for which it is processed.

(F) **Rights of data subjects.** Personal data must be processed in accordance with the rights of data subjects. Data subjects will have the right to see copies of their personal data, to have inaccuracies corrected and to object to the processing of their personal data or to have their personal data deleted if it is no longer required by the Company for another important reason.

(G) **Security.** Personal data must be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures.

(H) **International data transfers.** Personal data must not be transferred to a country or territory outside of the European Economic Area (the "EEA") unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

(I) **Accountability.** The Company and its third party service providers are responsible for and must be able to demonstrate their compliance with this policy including maintaining appropriate governance, oversight and documented decision-making processes in respect of personal data processing.

7. Consent

7.1 Personal data must only be processed if the purpose of the processing satisfies one of the lawful grounds permitted under GDPR. There are various legitimate reasons for which personal data can be collected and used. One such reason is that the individual has consented to the use of their data. Other applicable reasons are described in section 8 below.

7.2 If consent is being relied on to justify using a person's personal data, it must satisfy each of the following criteria:

(A) the consent must be limited to specific processing activities;

(B) the data subject must have been informed the about the processing activities in sufficient detail so as to be able to fully understand what they are consenting to;

(C) the consent must be "freely given". In other words, the data subject must have a genuine free choice as to whether they give the consent. Consent will not be freely given where there is a "significant imbalance of power" such that the individual does not really have a free choice about giving consent;

(D) the performance of a contract or delivery of a service cannot be made conditional upon the data subject giving their consent to the data processing, unless the data processing is required in order to perform the contract or deliver the service;

(E) the consent must be given by way of an unambiguous statement or some other clear, active communication by the data subject, such as signing a form. Consent cannot be inferred from silence or inactivity (for example, the use of pre-ticked boxes); and

(F) the consent to the processing of personal data must be clearly distinguished from other matters that the data subject is asked to agree to (for example, it should not be buried within the terms of a broader contract that the data subject is asked to sign).

7.3 It is important to note that a data subject has the right to withdraw its consent at any time and it must be as easy for a data subject to withdraw consent as it was for it to provide it in the first place. It is important that there are appropriate processes in place to promptly action any withdrawal of consent.

7.4 The Company will not generally seek or obtain consent to the processing of personal data. The Company and its data processors will therefore generally only process personal data in accordance with the other grounds listed in section 8 or, where that is not possible, obtain consent to processing as required. Where consent is obtained, a record of consents will be retained by the Company to evidence that it has been authorised to carry out the processing of a data subject's personal data.

8. Grounds for Processing Personal Data

8.1 As noted above, consent is not the only basis on which personal data can be collected and used and the Company will not generally seek or obtain consent to the processing of

personal data. There are other lawful grounds for processing personal data that the Company will generally seek to rely upon that are described in this section 8.

Non-sensitive personal data

8.2 The legal grounds for processing non-sensitive personal data include:

(A) where the data subject has given its consent to the processing of its personal data. The requirements for obtaining a valid consent are explained in section 7 above;

(B) where the processing is in the Company's legitimate interests and does not cause unwarranted prejudice to the data subject;

(C) where the processing is necessary for the performance of a contract to which the data subject is a party, or for the taking of steps (at the request of the data subject) with a view to entering into a contract; or

(D) where the processing is required by law.

8.3 This section describes the lawful grounds for processing which are most likely to be relevant to the Company's processing activities:

(A) where an applicant for interests in a Fund enters into an investment contract in respect of that Fund and the Company's processing is necessary for the performance of that contract, or is done at the applicant's request prior to entering into that contract, in the Company's capacity as management company, administrator and/or alternative investment fund manager to the relevant Fund;

(B) where processing is necessary to discharge a relevant legal or regulatory obligation;

(C) where processing is necessary for the legitimate business interests of the Company, a Fund, the investment manager, depositary or distributor of a Fund (each a "Fund Service Provider"), or another person, provided that, in each case, the Company undertakes and documents an appropriate assessment (including, where relevant, a legitimate interests assessment) to ensure that such interests are not overridden by the rights and freedoms of the data subject; such as:

(1) carrying out the ordinary or reasonable business activities of the Company, a Fund or a Fund Service Provider, or other activities previously disclosed to investors in the Funds;

(2) ensuring compliance with all legal and regulatory obligations and industry standards, and preventing fraud;

(3) establishing, exercising or defending legal rights or for other purposes relating to legal proceedings; and

(4) ensuring the security of information systems; and

(D) where processing any sensitive personal data falling within special categories, such as any personal data relating to the political opinions of a politically exposed person, the processing will be necessary for reasons of substantial public interest.

Sensitive personal data

8.4 Sensitive personal data is subject to stricter legal controls and the circumstances in which it can be processed are more limited than in respect of other personal data. The legal grounds for processing sensitive personal data include:

(A) where the data subject has given its explicit consent;

(B) where the processing is necessary for the purposes of carrying out the obligations and exercising rights of the Company or the data subject in the field of employment law or social security law;

(C) for the purposes of occupational health or the assessment of the working capacity of an employee;

(D) for equal opportunity purposes, where the processing is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; or

(E) where the processing is necessary for the purpose of, or in connection with, any legal proceedings, obtaining legal advice, or establishing, exercising or defending legal rights.

8.5 The Company does not generally expect to process sensitive personal data, save that: (i) in its capacity as management company, administrator and/or alternative investment fund manager, the Company may receive information relating to the political opinions of any individual classified as a "politically exposed person" in the context of know-your-client procedures for the Funds, which may be received by the Directors and, in certain circumstances, transmitted to a Fund Service Provider; and (ii) the Company may process limited health-related personal data in respect of its employees, for example in connection with sick leave, occupational health assessments or reasonable accommodations.

8.6 The Company will only process sensitive personal data (including transfers to third parties) where it has a lawful basis to do so, for example, where necessary for reasons of substantial public interest (such as the performance of enhanced due diligence on politically exposed persons) or, in respect of employee health data, where necessary for the purposes of employment law or occupational health.

9. High Risk Processing Activities

9.1 It is not expected that the processing of personal data by the Company or its data processors is likely to result in a "high risk" to the data subject as determined under GDPR. The monitoring or profiling of data subjects and the processing of sensitive personal data on a large scale are examples of processing activities that might present a high-risk.

10. Fair Processing Information

10.1 Any forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed.

10.2 Regardless of how personal data is obtained (whether it is obtained from the data subject or from a third party), the data subject must be provided with certain information about the processing of its personal data by the Company. This information must be provided at or before the time at which the personal data is collected (or, if the personal data is obtained from a third party, within a reasonable time of obtaining the personal data or at the time of the first communication with the data subject, whichever is earlier).

10.3 The information provided to the data subject must include the following:

(A) the identity and contact details of the Company;

(B) the categories of personal data collected in relation to the data subject;

(C) if the personal data is not obtained from the data subject, the source(s) of the personal data;

(D) the purpose(s) for which personal data will be processed, including the legal ground for the processing (see section 8 above). If the legal ground involves "legitimate interests", a description of those legitimate interests must also be provided;

(E) if personal data is processed based on the data subject's consent, an explanation of the data subject's right to withdraw their consent at any time;

(F) the categories of personal data that may be disclosed to third parties and the reasons for these disclosures;

(G) if the data processing is a contractual requirement, whether the data subject is obliged to provide the personal data on that basis, and the possible consequences of a failure to provide the information;

(H) any intention to transfer the personal data outside the EEA and information about the level of protection that will be afforded to the transferred data (including details of how the legal requirements for the transfer will be satisfied);

(I) information about the existence of any automated decision making (for example, profiling) undertaken by the Company based on the personal data, including details of the logic involved and its impact on the data subject;

(J) the period for which the personal data will be retained, or (if it is not possible to provide a specific time period) the criteria that will be used to determine the retention period;

(K) a general description of the Company's policies and practices with respect to protecting the confidentiality and security of personal data;

(L) the existence of the data subject's rights; and

(M) any other information that is necessary to guarantee that the processing of the personal data is fair in the circumstances.

10.4 This information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language that will be easy for the data subject to understand.

10.5 This policy is published on the Company's website (www.prescient.ie) and constitutes the privacy notice through which the Company provides the data protection information described in this section 10 to data subjects.

10.6 If any of the information described in the privacy notice changes after it has been provided to the data subject, the data subject must be provided with an updated copy of the information.

11. **Third Party Service Providers**

11.1 Where the Company instructs a third party to process personal data on its behalf (referred to as a "data processor"), the third party 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 law.

11.2 The data processing agreement should be approved by the Company and signed by both parties before any personal data is transferred to the data processor.

11.3 The Company's agreements with its data processors contain the requirements set out in section 11.1 above, and any further agreement entered into between the Company and a data processor will include similar terms in compliance with GDPR.

11.4 When contracting with a data processor, it is important that the Company conduct appropriate due diligence both at the outset of the relationship and on a periodic basis thereafter. Such oversight may include as applicable ongoing monitoring, periodic review of controls, and assurance that the data processor continues to meet applicable data protection and information security standards to ensure that the data processor is capable of complying, and does comply, with the requirements referred to in paragraphs (B)–(D) above.

11.5 Where a contracted data processor appoints another entity to process personal data, that entity should be treated and documented as a sub-processor through the contractual chain. The Company should obtain confirmation and, where appropriate, provide instructions to ensure that GDPR, standard contractual clauses and other applicable transfer requirements are fulfilled, and should complete appropriate due diligence on the sub-processor arrangements.

12. Disclosure of Data

12.1 The Company must ensure that personal data is not disclosed to unauthorised third parties. This section does not apply to data processors, which are addressed in section 11 above.

12.2 Personal data should not be disclosed orally or in writing to third parties without the consent of the data subject and approval from the Company.

12.3 In some circumstances, GDPR permits the disclosure of personal data without needing to obtain the prior consent of the data subject. Such disclosures might (depending on the circumstances) be permitted where this is:

(A) necessary to safeguard national security;

(B) necessary for the prevention or detection of crime, in the substantial public interest, and where obtaining consent from the data subject would prejudice that purpose;

(C) necessary for the administration of justice;

(D) necessary to comply with applicable law; or

(E) necessary to protect the vital interests of the data subject (this refers to life and death situations), but only where its consent cannot be obtained.

12.4 Requests for personal data from third parties must be supported by appropriate paperwork and any disclosures must be approved by the Company.

12.5 The Company will only share personal data with third parties where essential to its business objectives, where commercial risk factors have been fully considered and where the personal data involved is protected lawfully. Accordingly, the Company may from time to time disclose personal data to other parties including: (i) professional advisers such as law firms and accountancy firms, (ii) Fund Service Providers and other Prescient Group entities, including technology providers, (iii) counterparties and (iv) courts and regulatory, tax and governmental authorities, including the Central Bank of Ireland.

13. International Transfers of Personal Data

13.1 Specific legal requirements apply to the transfer of personal data out of the EEA. The "transfer" of data includes sending data to another country or allowing that data to be accessed remotely in another country, regardless of whether the Company transfers personal data outside the EEA itself or a data processor does so when acting on the Company's behalf.

13.2 Personal data must not be transferred outside the EEA unless the recipient country ensures an adequate level of protection for the rights and freedoms of data subjects. This requirement can be satisfied where:

(A) the European Commission has determined that the recipient country, territory or applicable framework provides an adequate level of protection, including, among others, Andorra, Argentina, Brazil, Canada (commercial organisations only), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, the Republic of Korea, Switzerland, the United Kingdom, the United States (in respect of organisations certified under the EU-US Data Privacy Framework), Uruguay and certain international organisations;

(B) the entry into a data transfer agreement between the Company and the non-EEA recipient of the personal data which contains standard contractual clauses that have been approved by the European Commission; or

(C) where applicable, reliance on an adequacy decision (including the EU-US Data Privacy Framework) or the implementation of appropriate safeguards such as standard contractual clauses.

13.3 The Company will ensure that any transfer outside the EEA will be subject to appropriate safeguards or is otherwise permitted under applicable law.

13.4 For transfers to non-EEA countries that are not covered by an adequacy decision, the Company must complete a transfer impact assessment and ensure that appropriate safeguards are in place, such as the European Commission standard contractual clauses. If the transfer impact assessment identifies concerns, supplementary technical or organisational measures, such as encryption or anonymisation, must be implemented before the transfer proceeds. Consent alone is not sufficient to legitimise such transfers.

14. **Retention and Disposal of Data**

14.1 Personal data must not be retained for longer than is necessary for the lawful purposes for which it is processed. To achieve this, each category of personal data processed by the Company must be subject to a retention period which can be justified by reference to those lawful grounds. Retention periods must be monitored and, upon their expiry, the relevant personal data must be deleted or anonymised (so that it is no longer possible to identify the data subject to whom the personal data relates).

14.2 For example, once an investor has redeemed or withdrawn all of its interests in the relevant Fund, it will not be necessary to retain all the information held on them because much of this is only required to administer the investor relationship, such as bank details for payment of redemption or withdrawal proceeds. Some data will need to be kept for longer periods than others, for example where it is necessary to retain certain records in order for the Company to comply with its legal obligations.

14.3 Personal data must be disposed of securely in a way that protects the rights and privacy of data subjects and ensures the permanent erasure of the data (e.g. shredding, disposal as confidential waste, or secure electronic deletion). Hard drives of redundant PCs should be wiped clean before disposal.

15. **Data Protection and Data Security**

15.1 It is critical that the Company protects the personal data in its possession or control by applying appropriate technical and organisational security measures to protect the data.

15.2 When processing and / or transmitting personal data:

(A) personal data, whether held electronically or in paper form, must be kept securely at all times. The Company and authorised third parties of the Company must

ensure that appropriate technical and organisational measures are in place to prevent unauthorised or accidental access, use, disclosure, loss or damage when personal data is being processed (including but not limited to when it is at rest or in transit). Technical measures, for example, include using encryption tools to protect personal data held in electronic form. Organisational measures, for example, include storing paper records containing personal data in locked cabinets;

(B) it is essential that if personal data is lost, damaged, compromised, misdirected or stolen, or otherwise processed in an unauthorised manner, that it is reported to the Company;

(C) care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data in accordance with section 14 above.; and

(D) personal data should not be disclosed except in accordance with sections 11 and 12 above.

15.3 In the event that personal data has been lost, damaged or become subject to unauthorised third party access, the Company will (without undue delay and, where feasible, within 72 hours after having become aware of such a data security breach) notify the Data Protection Commission, unless the data security breach is unlikely to result in a risk to the rights and freedoms of the individual(s) to which the personal data relates (in most cases, it will be difficult to say with certainty that there will be no such risk). Where relevant, the Company will also assess whether the breach constitutes an operational incident requiring notification to the Central Bank of Ireland in accordance with the Company's regulatory obligations. The Company will also maintain appropriate internal incident response procedures to ensure that any data security breach is identified, escalated, assessed and managed in a timely and effective manner. Where the data security breach is likely to result in a "high risk" to the rights and freedoms of the individual(s) to whom the personal data relates, the Company will also notify the affected individual(s) without undue delay in clear and plain language. In addition, the Company will document the data security breach, comprising the facts related to the breach, the scope and nature of the breach, its likely effects and the remedial action taken.

16. **Data Subject Rights**

16.1 Data subjects are entitled to exercise certain rights in respect of their personal data. These rights include access to the personal data held by the Company about them, the right to require the rectification of their data (where it is incorrect) and in certain circumstances the right to object to the processing of their personal data or to require it to be erased.

16.2 Data subjects have a number of legal rights in relation to their personal data. These rights include:

(A) the right to obtain information regarding the processing of their personal data and access to the personal data which the Company holds about them (or which is held on the Company's behalf);

(B) the right to receive a copy of any personal data which the Company processes about them;

(C) the right to request that the Company rectify their personal data if it is inaccurate or incomplete;

(D) the right to request that the Company erase their personal data in certain circumstances. This may include (but is not limited to) circumstances in which:

(1) it is no longer necessary for the Company to retain their personal data for the purposes for which it was collected it; or

(2) the Company is only entitled to process their personal data with their consent (i.e. because no other lawful ground for processing the personal data applies), and the data subject withdraws their consent;

(E) the right to lodge a complaint with an EU data protection regulator, such as the Data Protection Commission, if the data subject thinks that any of their rights have been infringed by the Company:

(F) the right to data portability in circumstances where processing is based on consent or contractual necessity; and

(G) the right to restriction of processing in certain circumstances.

16.3 Requests to exercise these rights will be considered by the Company as soon as practicable following receipt.

16.4 **Contact Us**

16.5 Data subjects who wish to exercise any of the rights described in this section 16, submit a subject access request, or raise any other query regarding this policy or the Company's processing of personal data, should contact the Company using the details below.

16.6 Data Protection Contact: Data Protection Officer: Nadia Galloway

16.7 Email: informationofficer@prescient.co.za / IREcompliance@prescient.ie

16.8 If a data subject is not satisfied with the Company's response, they also have the right to lodge a complaint with the Data Protection Commission (www.dataprotection.ie).

17. Record Keeping

17.1 Accurate and up to date records of the processing activities carried out by the Company must be maintained within the organisation. These records must include:

(A) the purposes of the processing;

(B) the categories of data subject;

(C) the categories of recipients of personal data;

(D) the categories of transfers of personal data to countries outside the EEA;

(E) the envisaged time limits for erasure of the personal data (where possible); and

(F) a general description of the technical and organisational security measures adopted by the Company.

17.2 The Company will keep a central record of its processing activities, which will be maintained by the Head of Compliance and reviewed periodically by the Directors, and will be updated to reflect new processing activities or material changes to existing processing activities.

17.3 Records of processing activities and transfer impact assessments are maintained and kept up to date.

18. Roles and Responsibilities

18.1 The Directors are ultimately responsible for ensuring that the Company meets its legal obligations. The Company may delegate certain data protection responsibilities to its service providers and delegates, provided that the Company retains overall responsibility for compliance with applicable data protection laws.

18.2 The Directors are responsible for ensuring that the Company:

(A) reviews all data protection procedures and related policies;

(B) deals with all requests from individuals to see the data the Company holds about them (Subject Access Requests);

(C) reviews and approves any contracts or agreements with data processors;

(D) ensures all systems, services and equipment used for storing personal data meet acceptable security standards; and

(E) evaluates any third-party services the Company is considering using to store or process personal data.

19. **Changes to this Policy**

19.1 The Company reserves the right to change this policy at any time. Where appropriate, the Company will notify data subjects of those changes by mail, email or by publishing an updated version of this policy on its website.

20. **Annual Review**

20.1 The policy will be reviewed on an annual basis.