(Version April 2020)

Prescient

DATA PROTECTION POLICY

1. INTRODUCTION

1.1 Prescient Holdings (Pty) Ltd and its subsidiaries and related parties ("**Prescient**") collects and processes personal information for various reasons, including to provide clients with access to our services and products. The type of information that is collected will depend on the purpose for which it is collected and processed. Prescient will only collect information that is required for a specific purpose. This information may include customer or client information, supplier and service provider information, business contacts, employee data and data relating to third parties and their clients.

1.2 This policy describes how this personal data must be collected, processed and stored to meet Prescient's data protection standards. It should be read in conjunction with all other relevant policies, including in particular the IT Security Policy.

1.3 **Policy objectives**

This data protection policy ensures that Prescient:

- Complies with data protection laws and follows good data protection practices;
- Protects the rights of staff, customers/clients and partners;
- Is transparent about how it stores and processes personal data;
- Protects itself from the risks of a data breach.

1.4 **Policy Scope**

The data protection policy applies to:

- Prescient Investment Management (Pty) Ltd;
- Prescient Fund Services (Pty) Ltd;
- Prescient Analytics (Pty) Ltd;
- Prescient Management Company (RF) (Pty) Ltd;
- Prescient Securities (Pty) Ltd;
- Prescient Khawuleza (Pty) Ltd;
- Prescient Nominees (Pty) Ltd;
- Prescient Investment Management Retail (Pty) Ltd;
- Prescient Staff Share Scheme (Pty) Ltd;
- Prescient Profile (Pty) Ltd;
- Prescient Global Limited;
- Prescient Investment Management China Limited;
- Prescient Fund Services (Ireland) Limited;
- Prescient Global Funds ICAV;
- Prescient Global Qualifying Investor Fund plc;
- Prescient ICAV;

each being an "**In-Scope Entity**".

This policy is subject to the approval of the board of directors of Prescient Holdings (Pty) Ltd in accordance with the following process:

(i) The policy is presented for consideration and if acceptable, approval, at the Prescient Group monthly CEO meeting, at which each of the In-Scope Entities are represented. In accordance with Prescient procedures, the draft policy or indeed any proposed updates to the policy must be circulated in advance of the monthly CEO meeting to provide sufficient time to each In-Scope Entity to review and consider;

(ii) Upon approval by the CEOs, the policy will be presented to the Prescient Group Audit and Risk Committee for final approval (on behalf the board of directors of Prescient Holdings (Pty) Ltd). As such, the board of directors of Prescient Holdings (Pty) Ltd delegates the approval of the policy to the Prescient Group Audit and Risk Committee;

1.5 **Policy Application**

This policy applies to all data that Prescient holds relating to identifiable individuals ("**Data Subjects**") including:

- Name and surname of an individual;
- Identity or passport numbers;
- Physical and or Postal Addresses;
- Email Addresses;
- Telephone Numbers;
- IP addresses (specifically relates to the General Data Protection Regulation, "**GDPR**");
- Any other information that can be linked to an individual.

The above is not an exhaustive list and other data fields should be considered on their merits. Certain categories of personal data is considered to be particularly sensitive ("**Sensitive Data**") and is subject to stricter processing rules as detailed in Section 3 below. Sensitive Data includes information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

1.6 **Policy ownership**

Where necessary, an In-Scope Entity may decide to appoint a Data Protection Officer ("**DPO**"). In such circumstances the DPO will own this Policy and will have a direct reporting line to the Board for data protection related matters.

In circumstances where an In-Scope Entity is not required to appoint a DPO, this Policy will be owned by the Board collectively, with a designated Data Privacy Manager being appointed to monitor and oversee compliance with this policy. The Data Privacy Manager will have a direct reporting line to the Board for data protection related matters.

1.7 **Protection**

This policy aims to protect Prescient from various data security risks, including:

- Breaches of confidentiality through data breaches or hacking risks;
- Associated liability in relation to client, third party data acquired from clients and employee data.

The rules and standards set out in this policy apply, regardless of:

- Whether personal data relates to a client or an employee of Prescient, and/or
- Is stored electronically, in hard copy, or through other methods.

1.8 **Prescient status as Data Controller and Data Processor**

Depending on the circumstances, Prescient may act as either a Data Controller or a Data Processor in respect of the personal data it collects and processes. When acting as a Data Controller, Prescient will determine the purposes and means of the processing of personal data. When acting as a Data Processor, Prescient will process personal data under the instruction of the Data Controller of such data. Regardless of the context in which it is processing personal data, Prescient will respect the key principles as set out in Section 2 below.

1.9 Prescient will record details of its key data processing activities in an internal register (the **"Data Register**") and its Data Controller / Data Processor status in relation to same. The Data Register consists of the following elements:

- categories of Data Subjects;
- categories of personal data;
- processing activity;
- the grounds for processing the personal information;
- in which jurisdiction the processing is conducted;
- whether the data is transferred to a third party;
- where applicable, whether the data is transferred outside the European Economic Area;
- the retention period.

1.10 **Data Processors appointed by Prescient**

To the extent that a service provider conducts data processing on behalf of Prescient, Prescient will ensure that its contractual relationship with the service provider provides for sufficient protections in relation to the processed data. Each service provider acting as a Data Processor on behalf of Prescient is required to provide Prescient with a copy of its data protection policy (and any updates thereto). Prescient's appointed Data Processors will also be required on an annual basis to make a presentation to the (Board / DPO / Data Privacy Manager) or otherwise provide written information on its data protection procedures which may impact Prescient.

Under its agreement with the relevant Data Processor, Prescient shall have a contractual right to obtain all relevant information from that Data Processor which is necessary in order for the Data Processor to demonstrate its compliance with the data protection obligations set down in the contract. Furthermore Prescient shall have the contractual right to carry out an audit or inspection of the relevant Data Processor for such purposes.

2. KEY PRINCIPLES RELATING TO PERSONAL DATA

2.1 Personal data shall at all times be:

- Processed fairly and lawfully and in a transparent manner. An individual's personal data must not be processed unless there are lawful grounds for doing so and the individual must be informed as to how and why their personal data is being processed either upon or before collecting it through the provision of a privacy notice.
- Collected and processed only for specific, lawful purposes. Personal data must not be processed in any manner which is incompatible with the specified and lawful purpose.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up to date. Any personal data which is incorrect must be rectified as soon as possible.
- Held for no longer than is necessary for the purpose for which it was obtained.
- Processed in accordance with the rights of data subjects.
- Protected appropriately and according to suitable methods, both organisationally and technologically.
- Not be disclosed, transferred or exported illegally, or in breach of any agreement with a client.

2.2 Prescient must ensure that it is in a position to demonstrate compliance with this policy by maintaining appropriate records of all material activities regarding its processing of personal data.

2.3 **Responsible Parties**

All employees shall continually be responsible for ensuring the safeguarding, protection and avoidance of any unauthorised disclosure or breach of personal data in the execution of employment duties and

services to Prescient, or otherwise in the course of rendering services or being associated with Prescient.

2.4 **General Data Protection Rules**

All personal data shall be deemed confidential and should be handled as such. Access to data will be granted on a 'need to know basis', based on the needs of the employee to fulfil their responsibilities. Data or personal information may not be shared outside of the scope of required work duties.

Employees will receive induction and on-the-job training in relation to all security standards applicable to such employee's service delivery and work outputs involving personal information of data subjects. Employees shall keep all data secure by taking sensible practical precautions and complying with all rules, practices and protocols, such as:

- Ensuring that strong passwords are employed at all times;
- Passwords may not be shared under any normal circumstances;

Note: In exceptional circumstances, it may be necessary to share a password. This may only take place after explicit, verifiable authorisation has been obtained from the business unit CEO, and only for the stated purpose. All necessary steps shall be taken after a password has been shared in such exceptional circumstances, to reset it to a strong, unique password to avoid future data compromise or breach.

3. PROCESSING OF PERSONAL DATA

3.1 Processing personal data includes any operation that is carried out in respect of personal data, including, but not limited to, collecting, storing, using, recording, disclosing, transferring or deleting personal data.

3.2 Personal data collected by Prescient is generally processed in order to:

(a) provide products and services to clients;

(b) comply with legal, tax or regulatory obligations imposed on it under applicable law;

(c) efficiently manage its relationship with service providers;

(d) carry out statistical analysis and market research;

(e) share personal data with necessary third parties such as auditors, regulatory or tax authorities and technology providers in the context of its day to day operations.

3.3 **Grounds for Processing Personal Data**

Personal data must only be processed if there is a permissible legal basis for doing so. The below details the lawful bases for processing which are most likely to be relevant to Prescient's processing activities:

(a) **Non-Sensitive Personal Data**

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

(i) where the processing is in Prescient's legitimate interests or the legitimate interests of a third party and the proposed processing does not cause unwarranted prejudice to the Data Subject;

(ii) 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 with a view to entering into a contract at the request of the Data Subject;

(iii) where the processing is required by law or other regulation to which Prescient is subject to;

(iv) where the Data Subject has provided his/her consent to the processing for the specific purpose.

(b) **Sensitive Personal Data**

In order to lawfully process Sensitive Personal Data, Prescient must identify both a lawful basis for the processing under Section 3.3(a) above and one of the following conditions must be present:

(i) the Data Subject has given explicit consent to the processing;

(ii) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of Prescient as Data Controller or of the Data Subject in the field of employment and social security and social protection law;

(iii) processing relates to personal data which are manifestly made public by the Data Subject;

(iv) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(v) processing is necessary for reasons of substantial public interest, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

(c) **Consent**

In order for consent to be valid, it must satisfy the following criteria:

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

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

(iii) the consent must be freely given which means that the Data Subject must have a genuine free choice as to whether they give the consent;

(iv) the performance of a contract 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;

(v) the consent must be given by way of an unambiguous statement of some other clear active communication by the Data Subject, such as signing a form. Consent cannot be inferred from silence or inactivity such as the use of pre-selected boxes; and

(vi) 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 cannot be buried within the terms of a broader contract that the Data Subject is asked to sign.

It is important to note that a Data Subject has the right to withdraw their consent at any time and it must be as easy for a Data Subject to withdraw consent as it was for them to provide it in the first place. Prescient shall put in place appropriate processes in place to promptly action any withdrawal of consent. Where a Data Subject wishes to exercise this right, they may contact the person designated for this purpose via the contact details provided in the Privacy Notice. A record of consents will retained by Prescient.

(d) **Legitimate Interests**

Prescient will conduct a "legitimate interests assessment" ("**LIA**") when relying on legitimate interests as a lawful basis for processing. This LIA will:

(i) identify the legitimate interest for which Prescient intends processing the personal data;

(ii) consider whether the processing is necessary for the pursuit of its objectives; and

(iii) involve the completion of a balancing test which assesses whether or not the Data Subject's interests override the legitimate interests of Prescient. Factors taken into account by Prescient in conducting the balancing test include:

(A) the nature of the legitimate interests and the Data Subject's reasonable expectations about what will happen to their data;

(B) the impact of processing on the Data Subject; and

(C) any safeguards which are or could be put in place in order to limit undue impact on the Data Subject.

In the event that a Data Subject objects to the processing of personal data on legitimate interests grounds, Prescient shall stop the processing of such personal data unless, having re-conducted the balancing test, Prescient is satisfied that the Data Subject's interests should not prevail over those of Prescient. Furthermore, Prescient will carry out a new LIA if the purpose of the processing changes or if it becomes aware of a change in the factors relating to the outcome of the LIA previously conducted.

3.4 **High Risk Processing Activities**

Wherever the processing of personal data is likely to result in a "high risk" to the Data Subject, Prescient as a Data Controller will need to, before carrying out the processing activity, perform an assessment of the potential impact of the intended processing on the rights and freedoms of the Data Subject (a "**Data Protection Impact Assessment**"). Prescient will maintain a record of all completed Data Protection Impact Assessments.

3.5 **Fair Processing Information**

Any process which involves the gathering of data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. 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 their personal data by Prescient. This information must be provided either before or upon collection of the personal data. If the personal data is obtained from a third party, then the information must be provided within a reasonable time period from obtaining the personal data or at the time of the first communication with the Data Subject, whichever is earlier.

The 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 and, where necessary, shall meet the requirements of the GDPR.

If any of the information required to be provided to the Data Subjects changes after it has been provided to the Data Subject, the Data Subject must be provided with an updated copy of the information.

4. DATA STORAGE

4.1 Prescient must implement appropriate technical and organisational measures which seek to ensure that personal data is appropriately protected against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access. 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 or on behalf of Prescient shall be subject to a retention period which can be justified by reference to those lawful grounds. Retention periods shall 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.

4.2 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. This includes shredding, disposal of confidential waste and secure electronic deletion.

4.3 **Paper**

Where data is stored on paper, it must be kept in a secure place, when not in use, such that an unauthorised person cannot access the information. e.g. on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated. This also applies to data stored electronically which has been printed to hard copy. Employees should ensure that paper and print outs are not left in places where unauthorised persons could gain access, e.g. on a printer or an employees desk. All unwanted paper must be shredded.

A Clean Desk/clear screen policy reduces the risks of unauthorized access, loss of and damage to information during and outside normal working hours. Safes or other forms of secure storage facilities might also protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

All employees shall be required to clear their desks or all personal information when leaving desks for any length of time and at the end of the day.

4.4 **Electronic data**

Where data is stored electronically, it must be protected from unauthorised access, accidental deletion or risk of exposure to malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees;
- Where data is stored on removable media such as a DVD, USB or removeable media these must at all times be locked away securely when not in immediate use;
- All data may only be stored on designated servers and may only be uploaded to approved cloud computing services;
- All Prescient servers containing personal data will be located within the Prescient data centres;
- Data will be backed up frequently in accordance with backup protocols. Such backups will be tested regularly in line with the company's standard backup procedures and protocols under the direction of the IT Manager. The Head of Governance will be responsible to schedule a minimum of two random tests each year;
- Personal data may not be saved directly to laptops or other mobile or removable devices, such as tablets or smart phones or removable USB drives;
- In exceptional circumstances, where personal data must be saved to a laptop hard drive to work offline, this may only be done where the laptop has been protected with hard drive encryption;
- All servers and computers containing data will be protected by approved security software, and one or more firewalls under the direction of the IT Manager.

5. DATA USE

5.1 It is acknowledged that personal data is at the greatest risk of loss, breach of confidentiality, corruption, hacking or theft while it is being accessed or used. Therefore, employees should lock their computer screens when left unattended. Screens should be manually locked, rather than relying on the automatic screen lock setting.

5.2 Personal data may not be shared informally, and in particular may not be sent by email without appropriate protection e.g. in a password protected file.

5.3 Data shall be encrypted before being transferred electronically. The IT Manager together with the Head of Governance will develop and maintain protocols for data transfer to ensure it is sent in protected form to authorised external contacts only, and to avoid it being sent to any unauthorised external or internal parties.

5.4 Personal data may never be transferred or sent to any entity that is not authorised to receive it. Employees are prohibited from saving copies of personal data to their own computers. Employees may, at all times, access and update only the central, official copy of any data or work output document.

6. DATA ACCURACY

6.1 Employees shall take reasonable steps to comply with Prescient's rules and work practices to ensure data is kept accurate and up-to-date. The more important the accuracy of any component of personal data is, the greater the effort and measures will be to ensure its accuracy.

6.2 Data should always be held in as few places as necessary to ensure efficient service delivery and risk avoidance. Employees are not permitted to create any unnecessary additional data sets.

6.3 Employees must make all reasonable efforts to ensure that a data component is accurate and up to date, e.g. by confirming details when handling a client call.

6.4 Employees shall at all times remain knowledgeable and informed about all data updating practices and work protocols used by Prescient, such as updating via official, acknowledged websites and platforms used by clients.

7. DATA SUBJECT ACCESS REQUESTS

7.1 Where an employee or individual requests his/her personal information, this is referred to as a "subject access request". Employees and individuals who are the subject of personal data held by Prescient are entitled to:

(a) the right to be informed at the time the personal data is obtained as to how their data will be processed;

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

(c) the right to receive a copy of any personal data which Prescient processes about them, including the right to receive personal data in a structured, commonly used electronic format and/or request that this data is transmitted to a third party where this is technically feasible;

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

(e) the right to withdraw consent to processing at any time;

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

(i) it is no longer necessary for Prescient to retain their personal data for the purposes for which we collected it; or

(ii) Prescient is only entitled to process the Data Subject's personal data with their consent and the Data Subject withdraws their consent; or

(iii) where Prescient is processing a Data Subject's personal data on legitimate interest grounds and the Data Subject objects to such processing.

(g) the right to lodge a complaint with a supervisory authority, if the Data Subject thinks that any of their rights have been infringed by Prescient.

7.2 Whilst data protection legislation affords Data Subjects these rights, in some instances it may not be appropriate to fulfil any requests. For example, where a request to erase personal data may not be

able to be completed due to an overriding legal or regulatory reason why the information must be retained.

7.3 Furthermore, while a service provider may process personal data on behalf of Prescient, it may also act as a data controller of such personal data where it uses the data for its own purposes. In such circumstances, all Data Subject rights shall be exercisable by the Data Subject against the service provider alone.

7.4 Prescient expects that any Data Subject requests will be made directly to the DPO / Data Privacy Manager, being the nominated contact point for data protection issues provided in Prescient's data privacy notice. Any Data Subject received should be forwarded to the DPO / Data Privacy Manager for action. Service providers acting as Data Processor on behalf of Prescient are obliged under contract to assist Prescient in complying with its obligations with respect to such requests. On receipt of any such request, the DPO / Data Privacy Manager will engage with the relevant service provider in order to ensure that, where applicable, the request is dealt with as soon as possible.

7.5 Prescient will respond to the Data Subject within one month of receiving such a request. If the request is complex then the response period may be extended by a further two months provided the Data Subject is kept informed as to the delay and provided a reasonable time period as to when the data will be provided. If Prescient does not take action on receipt of a Data Subject request, it shall inform the Data Subject without delay (and at the latest within one month of receipt of the request). The Manager shall ensure that the reasons for which it cannot comply with the request are advised to the Data Subject and that the Data Subject is reminded of the possibility of (i) lodging a complaint with a supervisory body and (ii) seeking a judicial remedy.

7.6 Prescient cannot generally charge a fee for dealing with any Data Subject requests. However, where requests from a Data Subject are manifestly unfounded or excessive, in particular because of their repetitive character, Prescient may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

In such circumstances, Prescient shall maintain all necessary records to demonstrate the manifestly unfounded or excessive character of the Data Subject request.

8. TO WHOM WE DISCLOSE INFORMATION

8.1 Prescient must ensure that personal data is not disclosed to unauthorised third parties. We may disclose personal information to any company in the Prescient Group and to our service providers who are involved in the delivery of products or services to the client. We have agreements in place to ensure that all service providers comply with these privacy terms. We may also disclose information where we have a legal obligation or duty to disclose this information or where it is necessary to protect our legal rights.

8.2 In certain circumstances, legislation will allow that personal data be disclosed to law enforcement or other agencies without the consent of the data subject. In such circumstances, Prescient may be obliged to disclose the requested data, but will first ensure that the request is legitimate and will seek assistance beforehand from its legal advisers or other experts. Only the Head of Governance or the Head of Legal will be authorised to furnish the requested data to the enquiring party.

8.3 All personnel acting on behalf of Prescient must exercise caution when asked to disclose any personal data to a third party and prior to completing any such transfer, Prescient must be satisfied that there is a lawful basis for such disclosure of personal data to third parties.

9. DATA TRANSFER BY EU-BASED PRESCIENT ENTITIES

9.1 Specific legal requirements apply to the transfer of personal data out of the European Economic Area ("**EEA**") by EU-based companies. The transfer of data includes sending data to another country or allowing that data to be accessed remotely in another country. 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 as determined by the European Commission[1] or alternatively one of the following safeguards have been put in place by the transferring entity:

(a) the entry into a data transfer agreement between the transferring entity (or a service provider acting as its agent) and the non-EEA recipient of the personal data which contains standard contractual clauses that have been approved by the European Commission;

(b) the existence of binding corporate rules;

(c) the recipient of the personal data is a an active member of the EU-US Privacy Shield (applies to US recipients only).

10. ISSUES AND BREACH MANAGEMENT

10.1 The response to any personal data breach can have a serious impact on Prescient's reputation. The consequential impact can be immeasurable. Not all personal data protection incidents result in data breaches, and not all data breaches require notification. Therefore, exceptional care must be taken when responding to data breach incidents.

10.2 A personal data breach is a loss of control, compromise, unauthorised disclosure, unauthorised acquisition, unauthorised access, or any similar term referring to situations where persons other than authorised users, for an authorised purpose, have access or potential access to personal data in usable form, whether manual or automated. This could mean:

(a) loss of a laptop, memory stick or mobile device that contains personal data;

(b) lack of a secure password on computers and applications;

(c) emailing personal data to someone in error;

(d) giving a system login to an unauthorised person; or

(e) failure of a door lock or some other weakness in physical security which compromises personal data.

10.3 Actual, suspected, or potential breaches should be reported immediately to the DPO / Data Privacy Manager. All data breaches will be recorded by the DPO / Data Privacy Manager in an incident log. The log will maintain a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of Personal Data. The record will include a brief description of the nature of the incident and (if applicable) an explanation of why the relevant regulatory authority was not informed.

10.4 **Requirement to Notify**

The GDPR imposes strict requirements to notify the relevant data protection authority in the event of a data breach where the breach presents a risk to the rights of affected individuals. If a notifiable data breach occurs, Prescient shall notify the relevant data protection authority without delay and not later than within 72 hours of becoming aware of the data breach. If a report is not made within 72 hours then an explanation as to the delay needs to accompany the report. Prescient will also notify the affected individuals, unless any of the following applies:

(a) Prescient has implemented security measures to ensure the personal data is unintelligible to anyone not authorised to access it (e.g. the personal data is encrypted);

(b) Prescient has taken measures to ensure the high risk to individuals is no longer likely to materialise; or

[1] The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection.

(c) notifying the individuals concerned would involve disproportionate effort. In this instance a public communication or similar would be provided for the individuals concerned to ensure that they are informed in an equally effective manner.

10.5 The DPO / Data Privacy Manager will notify the Board of reported personal data breaches and shall, if considered necessary, convene a board meeting in order to consider the matter further.

10.6 **Incident Response Objectives**

In the event of a data breach incident Prescient's primary objectives are to:

(a) stop the incident and limit the damage caused;

(b) prevent the spread/loss of data;

(c) recover data and/or systems that have been lost/stolen/damaged or otherwise compromised;

(d) minimise the impact of the incident on the business and get 'up and running' again as soon as possible;

(e) identify risks arising from the incident;

(f) notify appropriate parties or authorities of the incident;

(g) learn from the incident; and

(h) take steps to prevent future incidents.

10.7 The DPO / Data Privacy Manager maintains a central log for all data protection breaches and issues This is set out in Appendix 2.

11. DATA PRIVACY BY DESIGN AND BY DEFAULT

11.1 Prescient will adopt a "data privacy by design and by default" approach by:

(a) considering data protection issues as part of the design and implementation of systems, services, products and business practices;

(b) making data protection an essential component of the core functionality of our processing systems and services;

(c) anticipating risks and privacy-invasive events before they occur, and taking steps to prevent harm to individuals;

(d) only processing the personal data that we need for our purposes(s), and only using the data for those purposes;

(e) ensuring that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy;

(f) providing the identity and contact information of those responsible for data protection both within our organisation and to individuals;

(g) adopting a ‘plain language’ policy for any public documents so that individuals easily understand what we are doing with their personal data;

(h) offering strong privacy defaults, user-friendly options and controls, and respect user preferences;

(i) only using data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.

12. DISCIPLINARY CODE AND INCORPORATION OF THIS POLICY INTO THE EMPLOYEE'S EMPLOYMENT CONTRACT

12.1 This data protection policy governs every employee of Prescient, both during the course of his/her services to it, and to the extent applicable, after termination of services. This policy shall form part of Prescient staff's employment contracts and Human Resources Manual and is hereby also incorporated into it.

12.2 A breach of any rule in relation to the protection of personal data set out in this policy shall, in the event of breach thereof, form the basis of disciplinary action. In appropriate circumstances a breach hereof proven in a disciplinary enquiry may lead to dismissal.

12.3 The imposition of any disciplinary sanction or dismissal shall not preclude Prescient from instituting civil proceedings against an employee who acted in breach of this policy where such breach has resulted in liability, loss, reputational damage and/or other damages to the company in the course of pursuing its commercial operations. It shall be incumbent upon every employee to familiarise him/herself with the content of this policy, and to remain up to date as to any changes to it issued in written form as part hereof by Prescient.

Appendix 1: Version Control

Note: Changes older than two years are removed for manageability of this document and stored centrally.

Date	Version	Comments	Signed-off

Appendix 2: Personal Data Security Breach Log

Personal data security breach log **Effective Date [x], 2019**

Details of breach								Measure taken / to be taken		
No.	Date of breach	No of people affected	Nature of breach	Description of breach	How breach was identified	Description of data	Consequence of breach	All individuals informed?	Remedial action	Data Protection Authority Informed