DATA PROTECTION POLICY

1. Overview

1.1 We need to gather and use information or 'data' about individuals as part of the business. We intend to comply with legal obligations under the General Data Protection Regulations (the 'GDPR) in respect of the processing of 'personal data' and 'special categories of personal data'. These rules apply whether data is stored electronically, on paper or on other materials.

1.2 This policy explains how we will hold and process this information. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of Duneane Asset Management Limited.

1.3 This policy applies to all employees, volunteers, consultants, suppliers and anyone else working for or on behalf of the Company. It applies to all data that the Company holds relating to identifiable individuals.

1.4 If you are an employee, this policy does not form part of your contract of employment and it can be amended at any time.

2. Data Protection Principles

2.1 We adhere to the principles relating to Processing of Personal Data set out in the 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 being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

3. How we define personal data

3.1 'Personal data' means any information identifying a living person or information relating to a living person that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive 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.

4. How we define special categories of personal data

4.1 'Special categories of personal data' is a type of personal data consisting of information as to:

- The racial or ethnic origin of the person;
- His or her political opinions;
- His or her religious or other beliefs;
- Whether he or she is a member of a trade union;
- His or her physical or mental health or condition;
- His or her sexual life;
- The commission or alleged commission by him or her of any offence;

Criminal proceedings for any such offence or allegation, the disposal of the proceedings or any court sentence are a separate category but is similar to special categories of personal data.

5. How we define processing

5.1 'Processing' means obtaining, recording or holding the information or data or carrying out any operation(s) on that information or data, including:

- Organisation, adaptation or alteration of it;
- Retrieval, consultation or use of it;
- Disclosure of it by transmission, dissemination or otherwise making available; or
- Alignment, combination, blocking, erasure or destruction of it.

6. How will we process personal data?

6.1 We will process personal data (including sensitive personal data) in accordance with our obligations under the GDPR and the Data Protection Principles in paragraph 2.

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

6.3 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

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

(a) the Data Subject has given his or her Consent;

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

(c) to meet our legal compliance obligations.;

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

(e) to pursue our legitimate interests 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 we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices;

6.5 You must identify and document the legal ground being relied on for each Processing activity.

6.6 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

6.7 Data Subjects 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 you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.8 Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

6.9 You will need to evidence Consent captured and keep records of all Consents so that we can demonstrate compliance with Consent requirements.

7. Transparency

7.1 The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices 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 we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and data protection manager, how and why we will use, Process, disclose, protect and retain that Personal Data through a Fair Processing 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 publically available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data (where appropriate – note it will not always be appropriate in the nature of our business) (where not disproportionate – it will not always be proportionate to notify each person personally). You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed use of same.

8. How should you process personal data and special categories of personal data?

8.1 Everyone who works for, or on behalf of Duneane Asset Management Limited, has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy. The Data Protection Manager (who will be Donall McCann until otherwise notified) is responsible for reviewing this policy and

updating partners on Duneane Asset Management Limited's data protection responsibilities and any risks in relation to the processing of data.

8.2 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.

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

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

8.5 You should only collect and access data covered by this policy if you need it for the work you do for, or on behalf of Duneane Asset Management Limited and are authorised to do so.

8.6 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

8.7 You should not share personal data informally.

8.8 You should keep personal data secure and not share it with unauthorised people.

8.9 You should regularly review and update personal data which you have to deal with for work.

8.10 You should not make unnecessary copies of personal data and should keep and dispose of those copies securely.

8.11 You should use strong passwords.

8.12 You should lock your computer screens when not at your desk.

8.13 Personal data should be encrypted before being transferred electronically to authorised external contacts. Speak to IT for more information on how to do this.

8.14 Do not save personal data to your own personal computers or other devices.

8.15 Personal data should never be transferred outside the European Economic Area without the consent of the data subject or the authorisation of the Data Protection Manager.

8.16 Don't leave paper with personal data lying about.

8.17 Personal data should be shredded and disposed of securely when you have finished with it.

8.18 You should ask for help from your manager or our Data Protection Manager if you are unsure about data protection or if you notice any areas of data protection we can improve upon.

8.19 There are additional conditions on processing of special categories of personal data which must be met under the GDPR. This includes the express consent of the data subject in certain circumstances. You should refer to the Data Protection Manager for advice.

9. Data Subject Rights and Requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

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

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us 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) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(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.

You must immediately forward any Data Subject request you receive to the Data Protection Manager.

10. Storage Limitation

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

10.2 You 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 we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

10.3 We will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

10.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with our applicable records, retention schedules and policies. This includes requiring third parties to delete such data where applicable.

10.5 You will inform Data Subjects of the period for which data is stored and how that period is determined by providing them with the appropriate Privacy Notice or Fair Processing Notice.

11. Security, Integrity and Confidentiality

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

11.2 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You 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. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

11.3 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You 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.

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

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

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

11.5 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

12. Report a Personal Data Breach

12.1 The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

12.2 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Data Protection Manager. You should preserve all evidence relating to the potential Personal Data Breach

13. Record Keeping

13.1 The GDPR requires us to keep full and accurate records of all our data Processing activities.

13.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

13.3 These records should include, at a minimum, the name and contact details of the Data Controller, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

14. Training and audit

14.1 We are required to ensure all Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

14.2 You must undergo all mandatory data privacy related training and ensure your department undergo similar mandatory training.

14.3 You must regularly review all the systems and processes under your 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.

15. Privacy by Design and Data Protection Impact Assessments (DPIA)

15.1 We are 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.

15.2 You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

15.3 Data controllers must also conduct DPIAs in respect to high risk Processing.

15.4 You should conduct a DPIA (and discuss your findings with the Data Protection Manager) when implementing major system or business change programs involving the Processing of Personal Data including:

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

(b) Automated Processing including profiling and ADM;

(c) large scale Processing of Sensitive Data; and

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

15.5 A DPIA must include:

(a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(c) an assessment of the risk to individuals; and

(d) the risk mitigation measures in place and demonstration of compliance.

16. Sharing Personal Data

16.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

16.2 You may only share the Personal Data we hold with another employee, agent or representative of Duneane Asset Management Limited if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

16.3 You may only share the Personal Data we hold with third parties, such as our 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 GDPR approved third party clauses has been obtained.