DATA PROTECTION POLICY

Reference:	PDMS-DOC-01.01
Version:	1.00
Effective Date:	1 May 2018
Document Owner:	David Benge
Approved by:	Gleeds Main Board
Security Classification:	**Public**

Change History Record

Date	Version	Created by	Description of change

Table of Contents

1. Policy

The Main Board of Directors and management of Gleeds are committed to compliance with all relevant European (EU) and Member State laws in respect of personal data, and to protecting the "rights and freedoms" of individuals whose data Gleeds collects in accordance with the General Data Protection "Regulation" (GDPR) 2016 ("the "Regulation"). To that end, the Main Board has developed, implemented, maintains and continuously improves a documented Personal Data Management System ('PDMS') for Gleeds.

2. Scope

This Policy sets out the obligations of Gleeds regarding data protection and the rights of employees; individuals working for outsourced suppliers, service providers and consultants; and individuals working for client organisations and other business contacts ("Data Subjects") in respect of their personal data under the "Regulation".

This Policy forms part of Gleeds "Personal Data Management System", and is applicable to all Gleeds Companies, Business Units and Departments, employees and any third parties working with or for Gleeds.

3. Objectives of the Personal Data Management System

3.1 Gleeds objectives for the Personal Data Management System (PDMS) are that it should enable Gleeds to meet its own requirements for the management of personal data; that it should support organisational objectives and obligations; that it should impose controls in line with Gleeds' acceptable level of risk; that it should ensure that Gleeds meets applicable statutory, regulatory, contractual and/or professional duties; and that it should protect the interests of individuals.

3.2 Gleeds is committed to complying with data protection legislation and good practice including:

(1) Processing personal data only where this is strictly necessary for legitimate organisational purposes;

(2) Collecting only the minimum personal data required for these purposes and not processing excessive personal data;

(3) Providing clear information to individuals about how their personal data will be used and by whom;

(4) Only processing relevant and adequate personal data;

(5) Processing personal data fairly and lawfully;

(6) Maintaining an inventory of the categories of personal data processed by Gleeds;

(7) Keeping personal data accurate and, where necessary, up to date;

(8) Retaining personal data only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes;

(9) Respecting individuals' rights in relation to their personal data, including their right of subject access;

(10) Keeping all personal data secure;

(11) Only transferring personal data outside the EU in circumstances where it can be adequately protected;

(12) Applying various exemptions allowable by data protection legislation;

(13) Developing and implementing a PDMS to enable the Policy to be implemented;

(14) Where appropriate, identifying internal and external stakeholders and the degree to which these stakeholders are involved in the governance of Gleeds' PDMS; and

(15) Identifying employees with specific responsibility and accountability for the PDMS.

Notification

3.3 Gleeds has notified the Information Commissioner that it is a Data Controller and that it processes certain information about Data Subjects. Gleeds has identified all the personal data that it processes and this is contained in the Data Inventory (PDMS-DOC-04.06).

3.4 A copy of the Information Commissioner's (ICO's) notification details is retained by the Data Protection Officer (DPO) on Gnet (go to: UK Business Managements System/ Personal Data Management System / ICO Notification Details) and the ICO Notification Handbook is used as the authoritative guidance for notification.

3.5 The ICO notification is renewed annually on 9 June.

3.6 The DPO is responsible, each year, for reviewing the details of notification, in the light of any changes to Gleeds' activities (as determined by changes to the Data Inventory and the management review) and to any additional requirements identified by means of Privacy Impact Assessments (PIAs).

3.7 Any breach of the "Regulation" or this PDMS by an employee of Gleeds will be dealt with under Gleeds' Disciplinary Policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities. The nature of the breach will determine the sanction given under Gleeds' Disciplinary Policy, which could result in formal action being taken against the employee up to and including dismissal.

3.8 All third parties working with or for Gleeds, and who have or may have access to personal data, will be expected to have read, understood and to comply with this Policy. No third party may access personal data held by Gleeds without having first entered into a "Data Confidentiality Agreement", which imposes on the third party obligations no less onerous than those to which Gleeds is committed, and which gives Gleeds the right to audit compliance with the agreement.

4. Background to the General Data Protection "Regulation" ('GDPR')

The General Data Protection "Regulation" 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

5. Definitions

Definitions for the following terms used in this Policy, and in other documents forming Gleeds' Personal Data Management System (PDMS), have been drawn from the "Regulation":

- **Child** – the "Regulation" defines a child as anyone under the age of 16 years old. The processing of personal data of a child under 13 years of age is only lawful if parental or custodian consent has been obtained.
- **Data Controller** – means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by European Union (EU) or Member State law, the Data Controller or the specific criteria for its nomination may be provided for by EU or Member State law.

  The Data Controller is Gleeds.
- **Data Subject** – means any living individual who is the subject of personal data held by an organisation.
- **Data Subject consent** – means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.
- **Establishment** – means the main establishment of the Data Controller in the EU will be the place in which the Data Controller makes the main decisions as to the purpose of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a Data Controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the Data Controller operates, to act on behalf of the Data Controller and deal with supervisory authorities.

  The main establishment of the Data Controller for Gleeds is the UK.
- **Filing system** – means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
- **Personal data** – means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Processing** – means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation,

use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **Profiling** – means any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the Data Subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.
- **Personal data breach** – means a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the Data Controller to report personal data breaches to the Supervisory Authority and where the breach is likely to adversely affect the personal data or privacy of the Data Subject.
- **Special categories of personal data** – means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- **Territorial scope** – the "Regulation" will apply to all Data Controllers that are established in the EU who process the personal data of Data Subjects, in the context of that establishment. It will also apply to Data Controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour to Data Subjects who are resident in the EU.
- **Third party** – means a natural or legal person, public authority, agency or body other than the Data Subject, Data Controller, Data Processor and persons who, under the direct authority of the Data Controller or Data Processor, are authorised to process personal data. Third parties include natural or legal persons within outsourced suppliers, service providers, consultants, contractors and clients working with or for Gleeds.

6. Responsibilities under the General Data Protection "Regulation"

6.1 Gleeds is both a Data Controller and a Data Processor under the "Regulation".

6.2 The Main Board and all those in managerial or supervisory roles throughout Gleeds are responsible for developing and encouraging good data handling practices within Gleeds; responsibilities are set out in individual job descriptions.

6.3 The Data Protection Officer (DPO) is accountable to the Main Board for the management of personal data within Gleeds and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

(1) Development and implementation of the PDMS as required by this Policy; and

(2) Security and risk management in relation to compliance with this Policy.

6.4 The DPO and the Data Protection Co-ordinator who the Main Board consider to be suitably qualified and experienced, have been appointed to take responsibility for Gleeds' compliance with this Policy on a day-to-day basis and, in particular, have direct responsibility for ensuring that

Gleeds complies with the "Regulation", as do managers in respect of data processing that takes place within their area of responsibility.

6.5 The DPO and the Data Protection Co-ordinator have specific responsibilities in respect of procedures such as the Subject Access Request Procedure (PDMS-DOC-02.02) and are the first point of call for employees seeking clarification on any aspect of data protection compliance.

6.6 Compliance with data protection legislation is the responsibility of all employees of Gleeds who process personal data.

6.7 Gleeds' Data Protection Training Policy (PDMS-DOC-01.01) sets out specific training and awareness requirements in relation to specific roles and to employees of Gleeds generally.

6.8 Employees are responsible for ensuring that any personal data supplied by them, and that is about them, to Gleeds is accurate and up-to-date.

7. Risk Assessment

7.1 Risk assessments are undertaken by the DPO, in conjunction with the Data Protection Co-ordinators, to ensure that Gleeds is aware of any risks associated with the processing of particular types of personal data.

7.2 Gleeds has a process for assessing the level of risk to individuals associated with the processing of their personal data. Assessments will also be carried out in relation to processing undertaken by third parties on behalf of Gleeds. Gleeds shall manage any risks which are identified by the risk assessment in order to reduce the likelihood of a non-conformance with this Policy.

7.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the "rights and freedoms" of natural persons, Gleeds shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

7.4 A single assessment may address a set of similar processing operations that present similar high risks.

7.5 Where, as a result of a Privacy Impact Assessment (PIA), it is clear that Gleeds is about to commence processing of personal data that could cause damage and/or distress to the Data Subjects, the decision as to whether or not Gleeds may proceed must be escalated for review to the Data Protection Officer (DPO). The DPO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the Supervisory Authority (i.e. the "Information Commissioners Office (ICO)).

7.6 Appropriate controls will be selected from ISO 27001 Annex A and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to Gleeds' risk acceptance criteria and the requirements of the "Regulation".

8. Data Protection Principles

8.1 All processing of personal data must be done in accordance with the following data protection principles of the "Regulation", and Gleeds' policies and procedures are designed to ensure compliance with them:

(1) Processed lawfully, fairly, and in a transparent manner in relation to the Data Subject;

(2) Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(3) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

(4) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

(5) Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the "Regulation" in order to safeguard the rights and freedoms of the Data Subject;

(6) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

8.2 **Lawful, Fair and Transparent Data Processing** ('lawfulness, fairness and transparency')**:**

Gleeds Fair Processing Procedure is set out in PDMS-DOC-02.01.

(1) The "Regulation" seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the Data Subject. The "Regulation" states that processing of personal data shall be lawful if at least one of the following applies:

(a) The Data Subject has given 'explicit' consent to the processing of his or her personal data for one or more specific purposes;

(b) Processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract (e.g. a contract of employment);

(c) Processing is necessary for compliance with a legal obligation to which the Data Controller is subject (e.g. obtaining evidence of the right to work in the country);

(d) Processing is necessary to protect the vital interests of the Data Subject or of another natural person (e.g. the disclosure of medical records essential for someone's life – i.e. in matters of life and death);

(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;

(f) Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a child (i.e. an individual under the age of 16 (unless the Member State has made provision for a lower age limit – which may be no lower than 13)).

(2) The "Regulation" introduces the requirement for transparency whereby the Data Controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information must be communicated to the Data Subject in an intelligible form using clear and plain language.

(3) The specific information that must be provided to the Data Subject must as a minimum include:

(a) The identity and the contact details of the Data Controller and, if any, of the Data Controller's representative;

(b) The contact details of the Data Protection Officer (DPO) and the Data Protection Co-ordinators;

(c) The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) The period for which the personal data will be stored;

(e) The existence of the rights to request access, rectification, erasure or to object to the processing;

(f) The categories of personal data concerned;

(g) The recipients or categories of recipients of the personal data, where applicable;

(h) Where applicable, that the Data Controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;

(i) Any further information necessary to guarantee fair processing.

8.3 **Collected for Specified, Explicit and Legitimate Purposes** ('purpose limitation')**:**

Gleeds only collects personal data for the specific purposes (or for other purposes expressly permitted by the "Regulation"). The purposes for which Gleeds process personal data will be informed to Data Subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of Gleeds' GDPR registration.

PDMS-DOC-02.01: Fair Processing Procedure sets out the relevant procedures.

8.4 **Adequate, Relevant and Limited Data Processing** ('data minimisation')**:**

Gleeds will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to Data Subjects via a Fair Processing Notice.

(1) The Data Protection Officer (DPO) and the Data Protection Co-ordinators are responsible for ensuring that data, which is not strictly necessary for the purpose for which it is obtained, is not collected.

(2) All data collection forms (electronic or manual), including data collection requirements in new information management systems, must be approved by the DPO.

(3) The DPO will ensure that, on an annual basis, all data collection methods are reviewed by internal audit to ensure that collected data continues to be adequate, relevant and not excessive.

(4) If data is given or obtained that is excessive or not specifically required by Gleeds' documented procedures, the Data Protection Co-ordinator are responsible for ensuring that it is securely deleted or destroyed in line with ISMS-DOC-02.11.02.07 (Secure Disposal of Storage Media).

8.5 **Accurate and Kept up to Date** ('accuracy')**:**

Gleeds shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at yearly intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

(1) Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

(2) The Data Protection Co-ordinator are responsible for ensuring that all employees are trained in the importance of collecting accurate data and maintaining it.

(3) Individuals are to ensure that their personal data held by Gleeds is accurate and up-to-date. Completion of an appropriate registration or application form, etc. will be taken as an indication that the data contained therein is accurate at the date of submission.

(4) Employees should notify Gleeds of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records are contained in MyGleeds (Open HR). It is the responsibility of Gleeds to ensure that any notification regarding change of circumstances is noted and acted upon.

(5) The Data Protection Officer (DPO) is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

(6) On at least an annual basis, the DPO and the Data Protection Co-ordinator will jointly review all the personal data maintained by Gleeds, by reference to the Data Inventory,

and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely erased or otherwise disposed of in line with ISMS-DOC-02.11.02.07: Secure Disposal of Storage Media.

(7) The Data Protection Co-ordinator are responsible for making appropriate arrangements that, where third parties may have been passed inaccurate or out-of-date personal data, for informing them that the data is inaccurate and/or out-of-date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

8.6 **Timely Processing** ('storage limitation')**:**

Gleeds shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

(1) Where personal data is retained beyond the processing date, it will be automatically encrypted by Gleeds' ICT systems in order to protect the identity of the Data Subject in the event of a data breach.

(2) Personal data will be retained in line with PDMS-DOC-02.03: Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

(3) The Data Protection Officer must specifically approve any data retention period that exceeds the retention periods defined in PDMS-DOC-02.03 (Retention of Records Procedure), and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be in writing.

8.7 **Secure Processing** ('integrity and confidentiality')**:**

Gleeds shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

8.8 **Data Protection Measures**

Gleeds shall ensure that all its employees and third parties working on behalf Gleeds comply with the following when working with personal data:

(1) All e-mails containing personal data must be automatically encrypted by Gleeds' ICT systems;

(2) Personal data is to be erased or otherwise disposed of in line with Gleeds' Secure Disposal of Storage Media Procedure (ISMS-DOC-02.11.02.07);

(3) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

(4) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

(5) Personal data contained in the body of an e-mail, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;

(6) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

(7) Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Registered / Signed For post;

(8) No personal data may be shared informally and if an employee or third party working on behalf of Gleeds requires access to any personal data that they do not already have access to, such access should be formally requested from the applicable Data Protection Co-ordinator.

(9) All manual copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked drawer, cabinet or similar;

(10) No personal data may be transferred to any employees or third party, whether such parties are working on behalf of Gleeds or not, without the authorisation of the applicable Data Protection Co-ordinator;

(11) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees or third parties at any time;

(12) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

(13) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to Gleeds or otherwise without the formal written approval of the Data Protection Officer (DPO) and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

(14) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to third party parties working on behalf of Gleeds where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the “Regulation” (which may include demonstrating to Gleeds that all suitable technical and organisational measures have been taken);

(15) All personal data stored electronically should be backed up daily with backups stored on onsite and offsite servers. All backups should be automatically encrypted by Gleeds’ ICT systems;

(16) All electronic copies of personal data should be stored securely using passwords data encryption;

(17) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All

passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.

(18) Under no circumstances should any passwords be written down or shared between any employees or third parties working on behalf of Gleeds, irrespective of seniority or Business Unit / Department. If a password is forgotten, it must be reset using the applicable method. Gleeds Technology Limited (GTL) employees do not have access to passwords;

(19) Where personal data held by Gleeds is used for marketing purposes, it shall be the responsibility of the applicable Data Protection Co-ordinator to ensure that the Data Subjects explicit consent has been obtained.

8.10 **Technical and Organisational Measures**

(1) **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**

(a) Controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

(b) Gleeds compliance with this principle is contained in its Information Security Management System (ISMS), which has been developed in line with ISO/IEC 27001: 2013 and Gleeds' Information Security Policy (ISMS-DOC-01.01).

(c) Security controls will be subject to audit and review.

(2) Gleeds shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

(a) All employees and third parties working on behalf of Gleeds shall be made fully aware of both their individual responsibilities and Gleeds' responsibilities under the "Regulation" and under this Policy, and shall be provided with a copy of this Policy;

(b) Only employees and third parties working on behalf of Gleeds that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by Gleeds;

(c) All employees and third parties working on behalf of Gleeds handling personal data will be appropriately:

(i) Trained to do so; and

(ii) Supervised;

(d) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

(e) The performance of employees and third parties working on behalf of Gleeds handling personal data shall be regularly evaluated and reviewed;

(f) All employees and third parties working on behalf of Gleeds handling personal data will be bound to do so in accordance with the principles of the "Regulation" and this Policy by contract or agreement;

(g) All employees and third parties working on behalf of Gleeds handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of Gleeds arising out of this Policy and the "Regulation";

(h) Where any third party working on behalf of Gleeds handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless Gleeds against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

8.10 **Transferring Personal Data to a Country or Territory outside the European Union**

(1) **Personal data shall not be transferred to a country or territory outside the European Union (EU) 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.**

(2) The transfer of personal data outside of the EU is prohibited unless one or more of the specified safeguards or exceptions apply.

(a) **Safeguards**:

An assessment of the adequacy by the Data Controller taking into account the following factors:

(i) The nature of the data being transferred;

(ii) The country or territory of the origin, and final destination, of the data;

(iii) How the data will be used and for how long;

(iv) The laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and

(v) The security measures that are to be taken as regards the data in the overseas location.

(b) **Binding Corporate Rules**:

Gleeds may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant Supervisory Authority for approval of the rules that Gleeds is seeking to rely upon.

(c) **Model Contract Clauses**:

Gleeds may adopt approved model contract clauses for the transfer of data outside of the EU. If Gleeds adopts the model contract clauses approved by the relevant Supervisory Authority there is an automatic recognition of adequacy.

(d) **Exceptions**:

In the absence of an adequacy decision, including binding corporate rules, a transfer of personal data to a third country, or an international organisation, shall take place only on one of the following conditions:

(i) The Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards;

(ii) The transfer is necessary for the performance of a contract (e.g. a contract of employment) between the Data Subject and the Data Controller or the implementation of pre-contractual measures taken at the Data Subject's request;

(iii) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and another natural or legal person;

(iv) The transfer is necessary for important reasons of public interest;

(v) The transfer is necessary for the establishment, exercise or defence of legal claims;

(vi) The transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent;

(vii) The transfer is made from a register which according to EU or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in EU or Member State law for consultation are fulfilled in the particular case.

A list of countries that satisfy the adequacy requirements of the EU Commission are published in the *Official Journal of the European Union*.

8.11 **Accountability**:

(1) The Gleeds' **Data Protection Officer (DPO)** is:

- David Benge, Director – Head of Quality, Compliance and Performance

(2) **Data Protection Co-ordinators – United Kingdom:**

Area of Responsibility	Business Unit / Department	Data Protection Co-ordinator
• Recruitment • Employment	Human Resources (HR)	Louise Ellis (People Director)

Area of Responsibility	Business Unit / Department	Data Protection Co-ordinator
• Payroll • Transactions • Reporting Team • Credit Control	Finance	Greg Hughes (Finance Director)
• Training Records	Training & Development	Stuart Earl (T&D Director)
• Pensions	Trustees	Stuart Senior
• Marketing • Contacts Database • Website	Corporate Communications	Rebecca Ayrton (Corporate Communications Director)
• Projects Database	Research & Development	Sarah Davidson (R&D Director)
• Approved Supplier Database	Risk Directorate	David Benge (Director - Head of Quality, Compliance and Performance)
• Customer Relationship Databases	Business Unit / Office	Individual appointed by Area Chair to collect, hold, input, protect and keep up-to-date personal data

(3) **Data Protection Co-ordinators – European Offices:**

Country	Data Protection Co-ordinator
• Czech Republic	Michaela Rottova
• France	Eleanor Braund
• Germany	Florian Huebel
• Hungary	Julia Ribiczey
• Poland	Michal Lewczuk
• Portugal	Salome Iglesias Manzanero
• Romania	Corina Tanasie
• Slovakia	Viktoria Petkova

Country	Data Protection Co-ordinator
• Spain	Salome Iglesias Manzanero

(4) Gleeds shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

(a) The name and details of Gleeds, its DPO, and any applicable third party Data Controllers;

(b) The purposes for which Gleeds processes personal data;

(c) Details of the categories of personal data collected, held, and processed by Gleeds; and the categories of Data Subject to which that personal data relates;

(d) Details (and categories) of any third parties that will receive personal data from Gleeds;

(e) Details of any transfers of personal data to non-European Union (EU) countries including all mechanisms and security safeguards;

(f) Details of how long personal data will be retained by Gleeds; and

(g) Detailed descriptions of all technical and organisational measures taken by Gleeds to ensure the security of personal data.

8.12 **Privacy Impact Assessments:**

Gleeds shall carry out Privacy Impact Assessments (PIAs) when and as required under the "Regulation". DPIAs shall be overseen by Gleeds' Data Protection Officer and undertaken in accordance with PDMS-DOC-02.04: Data Processing Impact Assessment Procedure.

Note:

The term 'Data Protection Impact Assessment (DPIA)' is used by the European Commission, whereas the Information Commissioner's Office (ICO) in the UK use the term Privacy Impact Assessment (PIA) to mean the same.

9. The Rights of Data Subjects

9.1 The "Regulation" sets out the following rights applicable to Data Subjects:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure (also known as the 'right to be forgotten');
- The right to restrict processing;
- The right to data portability;
- The right to object; and

- Rights with respect to automated decision-making and profiling.

9.2 Data Subjects have the following rights regarding data processing, and the data that is recorded about them:

(1) To make subject access requests regarding the nature of information held and to whom it has been disclosed.

(2) To prevent processing likely to cause damage or distress.

(3) To prevent processing for purposes of direct marketing.

(4) To be informed about the mechanics of automated decision-taking process that will significantly affect them.

(5) Not to have significant decisions that will affect them taken solely by automated process.

(6) To sue for compensation if they suffer damage by any contravention of the "Regulation".

(7) To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.

(8) To request the Information Commissioner's Office (ICO) to assess whether any provision of the "Regulation" has been contravened.

(9) The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

(10) The right to object to any automated profiling without consent.

9.3 Data Subjects may make data access requests as described in PDMS-DOC-02.02 (Subject Access Procedure); this procedure also describes how Gleeds will ensure that its response to the data access request complies with the requirements of the "Regulation".

9.4 **Complaints**:

(1) Data Subjects who wish to complain to Gleeds about how their personal information has been processed may lodge their complaint directly with the Data Protection Officer (DPO) by means of e-mail (data-protection@gleeds.co.uk).

(2) Data Subjects may also complain directly to the Supervisory Authority and the DPO, and Gleeds provides appropriate contact details.

(3) Where Data Subjects wish to complain about how their complaint has been handled, or appeal against any decision made following a complaint, they may lodge a further complaint to the DPO. The right to do this is to be included in the "Regulation" section of Gleeds complaints procedure

10. Consent

10.1 Gleeds understands **'consent'** to mean that it has been **explicitly and freely given**, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she by

statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the Data Subject can be withdrawn at any time. Gleeds keeps records of all consents given.

10.2 Gleeds understands 'consent' to mean that the Data Subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties which demonstrate active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent (PDMS-DOC-04.09: Data Subject Consent Form) of Data Subjects must be obtained unless an alternative legitimate basis for processing exists.

10.3 In most instances consent to process personal and sensitive data is obtained by Gleeds using standard consent documents (PDMS-DOC-04.09: Data Subject Consent Form); e.g. when a new employee signs a contract of employment, or during induction for participants on programmes.

10.4 Gleeds does not currently provide online services to children. Should Gleeds begin to provide online services to children, parental, or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit – which may be no lower than 13).

11. Security of Data

11.1 All employees are responsible for ensuring that any personal data which Gleeds holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Gleeds to receive that information and has entered into a 'Data Confidentiality Agreement'.

11.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with ISMS-DOC-01.09: Access Control Policy. The Data Protection Officer (DPO) will form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

- In a lockable room with controlled access; and/or
- In a locked drawer or filing cabinet; and/or
- If computerised, password protected in line with Gleeds requirements specified in ISMS-DOC-01.09: Access Control Policy; and/or
- Stored on (removable) computer media which are encrypted in line with ISMS-DOC-01.09: Access Control Policy.

11.3 Care must be taken to ensure that personal computer (PC) screens and terminals are not visible except to Gleeds employees authorised to view the personal data. All employees are required to enter into an Individual Use Agreement (ISMS-DOC-04.09.01) before they are given access to personal data of any sort.

11.4 Manual records must not be left where they can be accessed by unauthorised personnel and must not be removed from Gleeds' premises without explicit authorisation, in writing, from the

applicable Data Protection Co-ordinator. As soon as manual records are no longer required for day-to-day use, they must be placed in secure archiving.

11.5 Personal data may only be disposed of in line with PDMS-DOC-02.03: Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by ISMS-DOC-02.11.02.07: Secure Disposal of Storage Media) before disposal.

11.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Employees must be specifically authorised to process data off-site.

12. Rights of Access to Data

12.1 Data Subjects have the right to access any personal data about them which is held by Gleeds in electronic format and/or in manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by Gleeds, and data obtained from third-parties about that person.

12.2 Subject access requests are dealt with in accordance with PDMS-DOC-02.02: Subject Access Request Procedure.

13. Disclosure of Data

13.1 Gleeds must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All employees should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Gleeds business.

13.2 The "Regulation" permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- To safeguard national security;
- Prevention or detection of crime including the apprehension or prosecution of offenders;
- Assessment or collection of tax duty;
- Discharge of regulatory functions (includes health, safety and welfare of persons at work);
- To prevent serious harm to a third party; or
- To protect the vital interests of the individual, this refers to life and death situations.

13.3 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

14. Retention and Disposal of Data

Personal data may not be retained for longer than it is required. Once an employee has left Gleeds, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. PDMS-DOC-02.03: Retention of Records Procedure will apply in all cases.

15. Disposal of Data

Personal data must be disposed of in a way that protects the "rights and freedoms" of Data Subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion / erasure) and in line with procedure ISMS-DOC-02.11.02.07: Secure Disposal of Storage Media.

16. Personal Data Breach Notification

All personal data breaches must be reported immediately to the Gleeds Data Protection Officer (DPO) in line with procedure PDMS-DOC-02.05: Personal Data Breach Notification Procedure).

This Policy is itself reviewed at least annually for continuing suitability. It is available upon request by any interested party.

Richard Steer
Chairman

12 April 2018