SOLICITORS
Magrath Sheldrick

Data Protection Compliance Policy

1. Introduction

1.1 In the course and ancillary to our business activities we will collect, store and process data, including Personal Data, about our clients, suppliers and other third parties. We recognise the importance of protecting Personal Data and have measures in place to ensure that it is collected, stored and processed properly and in accordance with applicable laws and regulations.

1.2 Data Users are obliged to comply with this policy when processing Personal Data on our behalf. Any breach of this policy may result in disciplinary action.

1.3 The types of Personal Data that we may handle includes information about current, past and prospective clients and suppliers and others that we communicate with in the course of our business. The Personal Data, collected, stored and processed by us may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations.

1.4 This policy sets out the basis upon which we will collect, store and process any Personal Data we collect from Data Subjects, or that is provided to us by Data Subjects or other sources.

1.5 This policy has been approved by the Partners but does not form part of our terms of business or part of any employee's contract of employment and may be amended at any time.

2. Definitions

2.1 In this policy, the following terms have the following meanings:

Data: information which is stored electronically or in certain paper-based filing systems.

Data Subject: a living individual about whom we hold Personal Data.

Personal Data: data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal Data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Data Controllers: people who or organisations which determine the purposes for which, and the manner in which, any Personal Data is processed. Data Controllers are responsible for

establishing practices and policies in line with the Act. We are the data controller of all Personal Data used in our business for our own commercial purposes.

Data Users: those of our employees whose work involves processing Personal Data. Data Users must protect the data they handle in accordance with this Data Protection Policy and any applicable data security procedures at all times.

Data Processors: include any person or organisation that is not a data user that processes Personal Data on our behalf and on our instructions. Employees of Data Controllers are excluded from this definition but it could include suppliers which handle Personal Data on our behalf.

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

Sensitive Personal Data: information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive Personal Data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

3. Data Protection Compliance Officer

3.1 The **Data Protection Compliance Officer** is responsible for ensuring compliance with the Act and with this policy. The Data Protection Compliance Officer's details are set out below. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Officer.

Peter Hunt

Email: peter.hunt@magrath.co.uk

Telephone: 020 7495 3003

4. Data Protection Obligations

4.1 In order to comply with this policy and applicable laws and regulations, applicable Personal Data processed by us will be:

(i) Processed fairly and lawfully;

(ii) Processed for limited purposes and in an appropriate way;

(iii) Adequate, relevant and not excessive for the purpose;

(iv) Accurate;

(v) Not kept longer than necessary for the purpose;

(vi) Processed in line with Data Subjects' rights;

(vii) Secure; and

(viii) Not transferred to people or organisations situated in countries without adequate protection.

4.2 When processing Personal Data as Data Controllers in the course of our business, we will ensure that Personal Data is processed in accordance with one of the legal grounds set out in the Act. These include the consent of a Data Subject to the processing, that the processing is necessary for the performance of a contract with the Data Subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When Sensitive Personal Data is being processed we will comply with the additional conditions required by the Act.

4.3 In the course of our business, we may collect and process Personal Data of clients and their employees, of our employees and our suppliers and third parties. This may include data we receive directly from a Data Subject and data we receive from other sources, including third parties instructed by us to provide information relevant to the Data Subject in the course of our business.

We will only process Personal Data for the specific purposes set out in the Schedule or for any other purposes specifically permitted by the Act. We will notify those purposes to the Data Subject when we first collect the data or as soon as possible thereafter.

4.4 We will only collect Personal Data to the extent that it is required for the specific purpose notified to the Data Subject.

4.5 We will ensure that Personal Data we hold is accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

4.6 We will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

5. Notifying Data Subjects

5.1 When we collect Personal Data directly from Data Subjects, we will inform them:

(i) The purpose or purposes for which we intend to process that Personal Data.

(ii) The types of third parties, if any, with which we will share or to which we will disclose that Personal Data.

(iii) The means, if any, with which Data Subjects can limit our use and disclosure of their Personal Data.

5.2 If we receive Personal Data about a Data Subject from other sources, we will provide the Data Subject with this information as soon as possible thereafter.

5.3 We will also inform Data Subjects whose Personal Data we process that we are the data controller with regard to that data, and who the Data Protection Compliance Officer is.

6. The Rights of Data Subjects

6.1 We will process Personal Data in line with Data Subjects' rights, in particular their right to:

(i) Request access to any data held about them by a data controller;

(ii) Prevent the processing of their data for direct-marketing purposes;

(iii) Ask to have inaccurate data amended; and

(iv) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

7. Data Security

7.1 We will take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

7.2 We will put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data will only be transferred to a data processor if that processor agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

7.3 We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

Confidentiality means that only people who are authorised to use the data can access it.

Integrity means that Personal Data should be accurate and suitable for the purpose for which it is processed.

Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal Data should therefore be stored on the Company's central computer system instead of individual PCs.

7.4 We have security procedures in place to protect Personal Data, including:

(i) Any stranger seen in entry-controlled areas should be reported.

(ii) Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(iii) Paper documents should be shredded. Digital storage devices should be wiped and if appropriate physically destroyed when they are no longer required.

(iv) Data Users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

8. Data Sharing

8.1 We may share Personal Data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

8.2 We may also disclose Personal Data we hold to third parties:

(i) In the course of our business and the provision of services to clients.

(ii) In the event that we sell or buy any business or assets, in which case we may disclose Personal Data we hold to the prospective seller or buyer of such business or assets.

(iii) If we or substantially all of our assets are acquired by a third party, in which case Personal Data we hold will be one of the transferred assets.

8.3 If we are under a duty to disclose or share a Data Subject's Personal Data in order to comply with any legal obligation, or in order to enforce or apply any contract with the Data Subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

8.4 We may also share Personal Data we hold with selected third parties from time to time for the purposes set out in the Schedule.

9. Transferring Data Overseas

9.1 We may transfer any Personal Data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

(i) The country to which the Personal Data are transferred ensures an adequate level of protection for the Data Subjects' rights and freedoms.

(ii) The Data Subject has given his consent.

(iii) The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the Data Subject, or to protect the vital interests of the Data Subject.

(iv) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

(v) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the Data Subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

9.2 Subject to the requirements in 9.1 above, Personal Data we hold may also be processed by staff operating outside the EEA who work for us, for our clients or for one of our suppliers. Those staff maybe engaged in, among other things, fulfilment of contracts with us in respect of the Data Subject or with the Data Subject direct, the processing of payment details and the provision of support services.

10. Access to Data

10.1 Data Subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to Data Protection Compliance Officer immediately.

10.2 When receiving telephone enquiries, we will only disclose Personal Data we hold on our systems if the following conditions are met:

(i) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(ii) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

10.3 Our employees will refer a request for Personal Data to their line manager or the Data Protection Compliance Officer for assistance in complex situations or if they are unsure about their right to disclose information. Employees should not be bullied into disclosing personal information.

11 Miscellaneous

11.1 We reserve the right to change this policy at any time. Where appropriate, we will notify Data Subjects of those changes by mail or email.

11.2 If you have any questions about this policy or our Data Protection practice, or have any comments, observations or concerns about the way Personal Data is being or has been handled, please speak to the Data Protection Compliance Officer.