Data Protection Policy

New policy August 2017

1. Purpose

While carrying out its business, the firm collects, stores and uses a large amount of information relating to individuals. The types of personal data that we may process include information about current, past and prospective clients, employees, contract staff, suppliers and other organisations with whom we have dealings. Personal data may consist of data kept on paper, computer or other electronic media; all of which is protected under the Data Protection Act 1998.

The collection and use of this information is regulated by the UK Data Protection Act 1998 and by various other data privacy laws and regulations. Any codes of practice or advisory notes issued by the Information Commissioner should also be noted. These impose many restrictions and controls on the processing of personal data. They also grant several rights to the individuals whose information is processed by the Firm.

This policy aims to serve as a guide for the directors, employees and contractors with brief details about the Data Protection Act and its implications for the firm. It is also intended to provide employees with basic information on the impact of the Act on their daily business and to minimise any risk to the firm by setting out clear guidelines relating to the processing, storage and disposal of data.

If the Firm fails to comply with the Data Protection Act 1998 ("the Act") then this could have serious consequences for its reputation or business. In extreme cases, it could be found to have committed a criminal offence.

This policy is not contractual but indicates how the Firm intends to meet its legal responsibilities for data protection.

2. Scope

This policy applies to all employees and workers (e.g. self-employed staff) who handle personal data, whether this relates to their colleagues, clients/customers or anyone else. It also extends to consultants and subcontractors. A copy will also be given to any third parties to whom we outsource any data processing.

3. Definitions

3.1. Data Controller

3.1.1. The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and to renew their notification on an annual basis. Failure to do so is a criminal offence.

The Firm is registered in the Information Commissioner's public register of data controllers.

The compliance officer also acts as our Data Controller and is responsible for ensuring compliance with the Data Protection Act, for notifying and updating the Information Commissioner of our processing of personal data, and for the monitoring and implementation of this policy on behalf of the Firm. Any changes made to the information stored and processed must be brought to the attention of the Data Controller immediately.

3.2. Data Processors

Data Processors include those employees and workers who have access to personal data, and who have responsibility for ensuring its accuracy and that it is kept secure.

3.2.1. The Act places obligations on Data Processors. This will be the case whether the Firm collects the personal data directly from the data subjects itself, or whether it collects the personal data from another source.

3.3. Data Subjects

3.3.1. A data subject is anyone whose personal data is held by us. This is typically data relating to clients, but also employee data, suppliers, shareholders, job applicants and former employees, as well as consultants and any other workers or contractors.

4. Principles

We endorse and adhere to the eight principles of the Data Protection Act which are summarised as follows:

Data must:

1. be processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. be adequate, relevant and not excessive for those purposes.
4. be accurate and, where necessary, kept up to date.
5. only be kept for as long as is necessary for the purpose for which it was obtained.
6. be processed in accordance with the data subject's rights.
7. be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measure.
8. not be transferred to a country or territory outside the European Economic Area, 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.

These principles apply to obtaining, handling, processing, transportation and storage of personal data. Employees and agents of the Firm who obtain, handle, process, transport and store personal data for us must always adhere to these principles.

5. Handling of personal/sensitive information

The Firm will, through appropriate management and the use of strict criteria and controls:

- observe fully the conditions concerning the fair collection and use of personal information
- specify the purpose for which information is used
- collect and process information only to the extent that it is needed to fulfil operational needs or legal requirements
- endeavour always to ensure the quality of information used
- not keep information for longer than required (operationally or legally)
- always endeavour to safeguard personal information by physical and technical means (i.e. keeping paper files and other records or documents containing personal/sensitive data in a secure environment; protecting personal data held on computers and computer systems using

secure passwords which, where possible, are changed periodically; and ensuring that individual passwords are not easily compromised)
- ensure that personal information is not transferred abroad without suitable safeguards
- ensure that the lawful rights of people about whom the information is held can be fully exercised.

In addition, the Firm will ensure that:

- all those who manage and handle personal information understand that they are responsible for following good data protection practice
- all those who manage and handle personal information are trained to do so and appropriately supervised
- a clear procedure is in place to deal with any data access requests (internal or external) that ensures that such enquiries are dealt with promptly and courteously
- methods of handling personal information are regularly assessed and evaluated
- any data sharing is carried out under a written agreement, setting out the scope and limits of the sharing
- any disclosure of personal data will comply with approved procedures.

The Firm also has a legal obligation to provide employee liability information to any organisation that our employees are transferring to, in line with the Transfer of Undertakings (Protection of Employment) Regulations (TUPE).

6. Procedure

6.1. The definition of processing in the Act is very wide and, generally, will cover all conceivable activities in relation to personal data. Processing therefore includes:

- obtaining, recording, consulting or holding personal data; and
- carrying out any operation or set of operations on personal data including:
  - organisation, adaptation or alteration;
  - retrieval, consultation or use;
  - disclosure (by transmission, dissemination or otherwise making available); or
  - alignment, combination, blocking, erasure or destruction.

However, this list is not exhaustive and therefore other forms of processing are possible.

6.2. <u>Personal Data</u>

6.2.1. The Act only applies to “personal data”, and not to every piece of information held by the Firm. The DPA lays down conditions for the processing of any personal data, and makes a distinction between 'personal data' and 'sensitive personal data'.

'Personal data' is defined as data relating to a living individual who can be identified from that data; or from that data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

6.2.2. Personal data does not need to be factual or numerical and will include any expression of opinion about an individual and any indication of intention about an individual (whether by the Firm or a third party).

6.2.3. Certain types of personal data are classed as 'sensitive personal data. This includes information relating to a person's racial or ethnic origin; political opinions; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life or criminal proceedings or convictions. All the general compliance requirements in the Act apply to sensitive personal data in the same way as they apply to non-sensitive personal data. However, the conditions which must be satisfied before sensitive personal data can be processed are stricter.

6.2.4. Information on deceased persons or companies will not be protected under the DPA but should still be treated with sensitivity. Information about individual contacts at companies will be personal data.

6.3. Manual Records

6.3.1. The Act applies to data held on paper-based files or any other manual system which is structured in such a way that specific information relating to an individual is readily accessible, as well as to data that is electronically stored. In summary therefore, it is sensible to assume that all computerised and paper-based data is covered by the Act, unless the data is so unstructured that information relating to an individual is difficult to retrieve (e.g. a disorganised pile of papers).

6.4. Employee responsibilities

6.4.1. All employees must ensure that, in carrying out their duties, the Firm is able to comply with its obligations under the DPA. In addition, each employee is responsible for:

- checking that any personal data that he/she collects is accurate and up to date
- ensuring that if, as part of their responsibilities, they collect information about clients or about other employees, they comply with this policy. This includes ensuring that information is processed in accordance with the DPA, is only processed for the purposes for which it is held, is kept secure, and is not kept any longer than is necessary.

6.4.2. Employees are reminded that the DPA does not just apply to records relating to our clients, but also to the records of employees. The information stored should be reviewed regularly to ensure it is accurate and up to date. All documents, whether hand written or saved electronically (for example in emails, current or deleted) are potentially disclosable in the event of a Data Subject Request

6.5. Client Data

6.5.1. Clients should be made aware of the identity of the Data Controller, any uses to which personal data will be put and any proposed disclosure of data to third parties. This must be done at the time the customer first provides the personal data. Processing may only be carried out where one of the following conditions has been satisfied:

- the individual has given his/her consent to the processing (this will always be a requirement of the firm when sensitive personal data, such as details of the individual's physical condition, is provided);
- the processing is required under a legal obligation;
- the processing is necessary to protect the vital interests of the individual; or to carry out public functions;
- the processing is necessary to pursue the legitimate interests of the Data Controller or certain third parties (unless prejudicial to the interests of the individual).

6.6. Employee records

6.6.1. We hold personal information about all employees as part of our general employee records. This includes address and contact details, age, date of birth, marital status or civil partnership, educational background, employment application, employment history with the Firm, areas of expertise, details of salary and benefits, bank details, performance appraisals and salary reviews, records relating to holiday, sickness and other leave, working time records and other management records. We may receive and/or retain this information in various forms (whether in writing, electronically, verbally or otherwise).

6.6.2. This information is used for a variety of administration and management purposes, including payroll and benefits administration, facilitating the management of work and employees, performance and salary reviews, complying with record keeping and other legal obligations.

6.6.3. We also process information relating to employees' health, some of which may fall under the definition of 'sensitive personal data'. This typically includes pre-employment health questionnaires; records of sickness absence and medical certificates (including self-certification of absence forms) night worker assessments; VDU assessments; noise assessments and any other medical reports. This information is used to administer contractual and Statutory Sick Pay, monitor and manage sickness absence and comply with our obligations under health and safety legislation and the Working Time Regulations.

6.6.4. From time to time we may ask employees to review and update the personal information we hold about them and will at least annually ask them to update their basic personal data. However, we ask that employees do not wait until asked to update this information, but inform us immediately of any significant change(s).

6.7. The rights of Data Subjects

6.7.1. Data Subjects are granted various rights under the Act. All individuals who are the subject of personal data held by us are entitled to:

- ask what information we hold about them and why
- ask how to gain access to it
- be informed of how to keep it up to date
- have inaccurate personal data corrected or removed
- prevent us from processing information or request that it is stopped if the processing of such data is likely to cause substantial, unwarranted damage or distress to the individual or anyone else
- be informed what we are doing to comply with our obligations under the Data Protection Act.

Those which are relevant to the business include:

- a right of access to personal data by written request;
- a right to prevent processing likely to cause damage or distress; and
- a right to prevent processing for purposes of direct marketing.

6.7.2. This right is subject to certain exemptions which are set out in the Act. More detail on some of these rights is set out below. Generally, if you receive a notification from any person that they wish to exercise any right under the Act, you should contact the Data Controller in the first instance.

6.8. Dealing with Subject Access Requests

6.8.1. Individuals are entitled to request detailed information regarding the personal data held about them by the Firm, together with copies of that data.

6.8.2. We reserve the right to charge the maximum fee payable for each subject access request. If personal details are inaccurate, they will be amended upon request. If by providing this information we would have to disclose information relating to or identifying a third party, we will only do so provided the third party gives consent, otherwise we may edit the data to remove the identity of the third party.

6.8.3. To comply with this obligation in a systematic manner, the Data Controller will be responsible for responding to all subject access requests.

6.8.4. Unless we are under a legal obligation to release data, or the individual has given us permission, personal information will only be released to the individual to whom it relates. The disclosure of such information to anyone else without their consent may be a criminal offence. Any employee who is in doubt regarding a subject access request should check with the Data Controller. Information must under no circumstances be sent outside of the UK without the prior permission of the Data Controller.

6.8.5. Any employee or worker who receives any request from an individual) to have access to or copies of their data should:

- not respond directly to the individual concerned, other than to thank them for their request and to confirm that their request is being dealt with.

- immediately forward the request (together with all information in the recipient's possession as to the nature and circumstances of the request e.g. the date it was made) to the Data Controller.

- We aim to comply with requests for access to personal information as quickly as possible, but will ensure that this is provided within 40 days of receipt of a written request unless there is good reason for delay. In such cases, the reason for the delay will be explained in writing to the individual making the request.

6.8.6. Any employee or worker who receives any requests for copies of personal data in his/her possession or control relating to an individual (whether a subject access request was received directly from that individual) should respond promptly to the Data Controller with a description of:

- any personal data which is held by him/her relating to the individual concerned;
- the purposes for which that data is processed; and
- the recipients to whom that data may be disclosed.

The Data Controller should also be provided with:

- copies of the personal data held in relation to the individual concerned;
- any information as to the source of the data.

6.8.7. The definition of personal data is very wide and is deemed to cover all personal data relating to the relevant individual in our possession or control. It should include emails and data in electronic databases as well as paper based files.

6.9. Security of Information

6.9.1. The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted Access to personal information is strictly controlled and limited to those who are entitled to see it as part of their duties. The Firm regards security of information as an extremely important issue and employees should note the following:

- All hard copy client files are kept in a locked cabinet and are not to be removed from the office except for client visits. Other information that is stored electronically has appropriate levels of authorisation which prevent unauthorised access.
- The Directors have access to the personnel records of all employees but store them in private folders (in separate filing cabinets or separate server partition.)
- Data retained on laptops, smartphones and any other electronic equipment that is removed from our office must be password protected.
- All employees and workers are responsible for ensuring that any personal data that they hold is stored securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.
- References that disclose personal information will not be provided to any third party without the data subject's prior authority (unless this is required or permitted by law such as by the FCA, NCA, HMRC, or similar body).
- It is a criminal offence and will be a disciplinary matter if an employee obtains, passes on or discloses personal data unlawfully to a third party.
- The Firm's computer systems security procedures should be followed.
- Computer discs, memory sticks and paper records should be always secured properly.
- Data on computers and in paper records should be maintained as accurately and securely as possible.
- Any rules, procedures or instructions which the Firm may issue from time to time to ensure the security of information should be observed.
- The Firm should conduct a data security review on a regular basis to monitor compliance with the above security features

Third party processors (such as insurance companies or pension providers) will be required to provide sufficient guarantees for their data security measures and compliance with them. A written contract will be in place with suppliers which requires them to dispose of data securely and to provide suitable evidence of this.

Any employee who discovers personal or sensitive data in an inappropriate place (for example unknowingly sent to the wrong printer) should immediately pass this to the Data Controller, ensuring that its contents are not revealed to anyone else.

6.10. Subject consent

6.10.1. Our client agreements and terms of business require the consent of clients to the processing of personal data for the purposes of administration and processing.

6.10.2. Information about an individual will only be kept for the purpose for which it was originally provided. Employees and managers must not collect data that is simply "nice to have" nor use data for any purpose other than what it was provided for originally.

6.11. Publication of information

6.11.1. Information that is already in the public domain is exempt from the Data Protection Act. This would include, for example, information contained within externally circulated publications such as brochures and other sales and marketing literature, or included on our website.

6.12. Retention and disposal of data

6.12.1. Information will be kept in line with the FCA document retention guidelines. All employees are responsible for ensuring that information is not kept for longer than necessary.

6.12.2. Documents containing any personal information will be disposed of securely, and paper copies will be shredded (not disposed of directly into a normal bin or recycling bin). Information stored on obsolete electronic equipment (desktops, laptops and other devices) will be erased prior to the equipment being sold, disposed of or reallocated to other employees.

6.13. Ensuring compliance

6.13.1. To ensure that the Firm is not in breach of its obligations under the Act, all employees and contractors of the Firm should observe the guidelines set out below.

6.13.2. Consider each of the separate tasks and activities which comprise your job. Identify which of these involve the processing of personal data and sensitive personal data.

6.13.3. Notify the Data Controller if you intend, or have started, to process personal data in a different way, or for different purposes to that carried on previously. This will enable the Data Controller to make the necessary changes to the Firm's data protection registration.

6.13.4. Ensure that personal data is being held and used in accordance with the data protection principles. The following steps should be followed:

6.13.4.1. You should ensure that personal data is processed fairly and lawfully. Personal data should only be used in connection with, and to the extent necessary, for the purposes of your role.

6.13.4.2. You should obtain consent from the individual which the personal data relates to before the personal data is collected or used. This can be done by verbal agreement asking the client to proceed and reinforced through explanation of the data protection policy in the client agreement.

6.13.4.3. Where employees have been requested to disclose personal data to a third party and such disclosure is not a routine part of your business, you should forward this request to your line manager before making such disclosure as in some cases it will be necessary to obtain the consent of the individual concerned.

6.13.5. The Firm may collect sensitive personal data where this is necessary for the purposes of life insurance (e.g. health, etc.)

6.13.6. Employees should only collect personal data for a definite purpose and should not use the data for any other purpose, unless the individuals concerned are notified of this.

6.13.7. Employees should ensure that any personal data is kept accurate and up to date.

6.13.8. If a data subject notifies the Firm that their data needs to be amended then

6.13.8.1. if it is agreed that the data is inaccurate then it should be changed.
6.13.8.2. If it is not agreed that the data is inaccurate then it should be left un-amended but a note of the data subject's views should be included with the data.

6.13.9. You should observe any relevant data retention policies and procedures in place in your area of work to ensure that personal data is deleted after a reasonable time. If there are no such policies and procedures in place then you should delete personal data once it is no longer required for the purpose for which it was originally collected.

6.13.10. The Firm provides appropriate organisational, physical and technical security arrangements in relation to all personal data.

6.13.11. The level of security used should be appropriate to the nature of the data and the harm that could result if it is used in an unauthorised manner. For example, employees should ensure that:

- Paper files are stored in locked cabinets.
- Computer printouts are not put in a waste paper bin but are correctly disposed of by shredding.
- Computer passwords are not disclosed to anybody other than the relevant authorised user.
- Computer discs and USB sticks are not used or secured properly.
- All security procedures set out in the Firm's IT and computer use policies and in any other relevant policies or guidelines, are followed.

6.13.12. Employees should not transfer personal data to any country outside the European Economic Area unless this has been authorised by the Data Controller, who will check that appropriate security precautions for the transfer of data are in place.

6.13.13. The Data Controller should be notified immediately of any query, request or complaint from any individual in relation to the processing of their data.

6.13.14. Whenever you record or use personal data, you should be aware that the material contained within these databases might have to be disclosed to the individuals which they relate to if a subject access request is made. You should therefore ensure that the information is recorded in a business-like manner and does not include comments that could be considered offensive or inappropriate.

6.14. Non Compliance

6.14.1. Where individuals are deemed to have not complied with the principles of the Data Protection Act, and the guidance outlined above they may be subject to action under our Disciplinary Procedure. Any breach will be taken seriously. Any employee who considers that the policy has been breached in any way should raise the matter with the Data Controller.

7. Related Policies

- Computer Usage Policy
- Email Policy
- Internet Policy

- Data Security Policy
- Whistleblowing policy

The above list is not exhaustive and other Firm policies may be applicable.

8. Where to find further information

If you require further information on this policy or the interpretation or operation of this policy, please speak with your Manager in the first instance.

9. Declaration and sign off

In signing this document, you confirm that you have read it and will abide by these data protection regulations and our own internal procedures.

Signed by the directors

Stephen Sutherland
Stephen Sutherland (Aug 15, 2017)

Paul Sutherland
Paul Sutherland (Aug 15, 2017)

Signed by employees and workers

Karen Harrop
Karen Harrop (Aug 15, 2017)