HENDERSON ROWE

Data Protection Policy

Date: January 2017

www.hendersonrowe.com
25 Grosvenor Street London W1K 4QN
0207 907 2200

Henderson Rowe Limited is authorised and regulated by the Financial Conduct Authority
Henderson Rowe Limited is registered in England and Wales, company number 4379340

1 PURPOSE

1.1. The Data Protection Act 1998 ("the Act") has two primary purposes:
  1.1.1. To regulate the use of personal information within the firm; and
  1.1.2. To provide rights to those individuals whose information is held.

1.2. At the core of the Act are eight key principles, which are designed to:
  1.2.1. Provide guidance on how Data Controllers create, acquire, hold, process, query, amend, edit, disclose, transfer and destroy data comprising in whole or in part personal information;
  1.2.2. Prescribe the purpose for which data may be gathered from sources and held by Data Controllers; and
  1.2.3. Enshrine the rights of data subjects.

1.3. So that Henderson Rowe ("the Firm") can comply with this, guidance has been sought from the data protection regulator, known as the Information Commissioner's Office ("the ICO").

1.4. The Act applies to the Firm, which is the Data Controller for the purposes of the Act, and to any member of staff who holds or has access to personal information in such a way that retrieval is possible.

1.5. The Firm takes the view that all staff have access to personal information, whether that be in relation to clients, staff, service providers or suppliers; accordingly, this policy applies to all staff.

1.6. The purpose of this policy is to help staff familiarise themselves with their duties and the Firm's responsibilities established under the Act and to set out the standards by which the Firm wishes to conduct its day-to-day business in relation to the use and safeguarding of personal data, which staff are expected to comply with and uphold.

1.7. For the purposes of this policy, the Head of Compliance acts as the Firm's Data Protection Officer. In her absence, the Operations Manager will act as a temporary replacement and will be responsible for advising the Head of Compliance on any issues that have arisen in her absence.

2 DEFINITIONS

2.1. The Act regulates the use of 'personal data'. This covers data which relates to a living individual who can be identified from that data alone or from that data alongside other information which is or is likely to come into the possession of the data controller.

2.2. The Act is further designed to protect the use of 'sensitive personal data', which is any personal data, as defined in paragraph 2.1, that consists of information or data regarding:

- race;
- ethnicity;
- political opinion;
- religious belief (or similar);
- membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- physical or mental health;
- sex life, including sexual orientation;
- the commission or alleged commission of criminal or regulatory offences; or
- the proceedings (whether past, present or future) for any offence committed or alleged to have been committed, including the disposal of proceedings or any sentence passed by a court in any such proceedings.

2.3. For the purposes of data protection, 'use' includes (but is not limited to):

- processing, obtaining, recording or holding data or information in that data;
- carrying out any operation on data or information contained in that data;
- organising, adapting or altering data or information contained in that data;
- retrieving, consulting or using data or information contained in that data;
- disclosing data or information in that data by way of transmission, dissemination, or otherwise making available; or
- aligning, combined, blocking, erasing or destroying data or information contained in that data.

3 COVERAGE

3.1. This policy covers all individuals working at all levels and grades throughout the Firm, including Directors, Officers, investment managers, analysts, traders, assistants, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual employees and any agency staff (collectively referred to as 'staff' throughout this policy).

4 SCOPE

4.1. Staff are required to comply with the spirit of this policy at all times, and to ensure that the personal information of clients and confidential business documents are protected from disclosure to, use by or manipulation by outside sources.

5 DATA PROTECTION PRINCIPLES

The Firm, as required by the Act and based on guidance published by the ICO, works on the basis that there are eight key principles at the core of data protection. The principles apply to all personal data held by the Firm, whether that information relates to clients, staff, suppliers or any other person.

5.1 PRINCIPLE 1: PERSONAL DATA SHALL BE PROCESSED FAIRLY AND LAWFULLY

5.1.1. The Firm is required to have legitimate grounds for collecting and using personal data. This is not likely to be contentious where the Firm is required to request the information in order to ascertain the client's suitability for the Firm's services or for anti-money laundering purposes, but any extraneous information should not be sought.

5.1.2. Information that is acquired and processed by the Firm should only be obtained with the express permission of the data subject; if that data falls under the definition of 'sensitive personal data', consent is a mandatory requirement established by law.

5.1.3. The Firm must be transparent in how it seeks to use personal data; this is best achieved by Investment Managers when initiating a client or conducting ongoing reviews on their behalf. However, it can additionally be achieved by communications by the Head of Compliance if she is required to request further information for a legitimate purpose.

5.1.4. The Firm must only handle data in ways that clients know or could reasonably expect. For example, any information obtained for conducting anti-money laundering checks should only be used for conducting that check and later stored so that the Firm may ensure compliance with anti-money laundering regulations.

5.1.5. The Firm must not use personal data unlawfully; this extends to all staff who have access to such information.

5.2 PRINCIPLE 2: PERSONAL DATA SHALL ONLY BE OBTAINED FOR SPECIFIED AND LAWFUL PURPOSES AND SHALL NOT BE PROCESSED IN ANY MANNER INCOMPATIBLE WITH THOSE PURPOSES

5.2.1. The Firm is required to be clear about how it uses personal data so that it can be sure that any personal data held is processed in a way that is compatible with the Act.

5.2.2. To comply with the Act's requirement for fair processing, the Firm is under a duty to provide privacy notices to any individual when collecting personal data. The Firm should not presume that clients will check its ICO registration to ascertain the exact purpose for which it seeks information. A privacy notice is included in the Firm's Terms and Conditions of Business.

5.2.3. Where a purpose is stated and information provided to cover that purpose, that information should only be used for that purpose or any other purpose that is not

incompatible with that original purpose. For example, it is theoretically legitimate for the Firm to contact its personal account holders to promote its ISA range; it is not legitimate for the Firm to contact its high net worth account holders to advertise a secured or unsecured lending facility.

5.3 PRINCIPLE 3: PERSONAL DATA SHALL BE ADEQUATE, RELEVANT AND NOT EXCESSIVE IN RELATION TO THE PURPOSE(S) FOR WHICH THEY ARE PROCESSED

5.3.1. So that the Firm can comply with this principle, the Firm must ensure that any personal data held is sufficient for the purpose that the Firm is holding it for. Further, any personal information held should be the sufficient amount for the stated purpose; maintaining too much information should be avoided. The Firm takes the view that sufficient quantity should be assessed on a case-by-case basis and that any general rules regarding quantity on any given issue will be established by the Data Protection Officer.

5.3.2. Information should not be retained because it is thought that it might be useful in the future. However, the Firm reserves the right to seek personal information from staff in order to prepare for events that the Board of Directors consider to be foreseeable.

5.3.3. This purpose works equally the other way: if the information that the Firm uses is insufficient, it must no longer be processed. This can be remedied by approaching the data subject and seeking supplementary information so that the entire cache of information is adequate for the intended purpose.

5.4 PRINCIPLE 4: PERSONAL DATA SHALL BE ACCURATE AND KEPT UP TO DATE

5.4.1. To comply with this principle, the Firm and its staff must take all reasonable steps to ensure the accuracy of personal data obtained, ensure that that information is clear and where necessary consider whether it is necessary to update that information.

5.4.2. The Act does not define what is meant by accuracy, therefore, the Firm takes the simple English understanding of 'accuracy', alongside the examples of 'inaccuracy' provided by legislative guidelines. According to that guidance, data is inaccurate if it is incorrect or misleading as to any matter of fact: for example, if a client contacts the Firm to say that he is moving from London to Leeds and the Firm's records continue to say he is living in London, that data is inaccurate; if, however, the Firm's records state that he once lived in London, that data is accurate.

5.4.3. Where an error occurs in relation to the data subject, it is important that that error is corrected as soon as is practicable. It is legitimate to retain a note stating that an error occurred and was rectified.

5.4.4. It is necessary for the Firm to ensure that data is kept up to date where possible.

5.4.5. An exception to this policy applies where personal data has been supplied by the data subject directly. In this situation, the Firm must ensure that the information provided by the individual is recorded accurately as they have provided and that the Firm has taken all reasonable steps to ensure the data is accurate. For example, if a client provides their address and confirms this by providing a utility bill with the same address, it is reasonable to say that whilst this cannot be guaranteed to be accurate (as the individual could have moved property after the bill was issued), the Firm has taken all reasonable steps to record and ensure the data is accurate.

5.5 PRINCIPLE 5: PERSONAL DATA SHALL NOT BE KEPT FOR LONGER THAN IS NECESSARY FOR THE RELEVANT PURPOSE(S)

5.5.1. This principle has close links with principles 3 and 4, in that retaining data for only as long as is necessary helps to ensure that any data held is accurate and adequate for the purposes it was sought for.

5.5.2. The Act itself does not stipulate a minimum period by which the personal data of clients shall be retained, but under the Firm's Terms and Conditions of Business we agree with clients to retain all information for a minimum period of six years after termination of our relationship with them. This is so the Firm can comply with the regulatory requirements over record-keeping in COBS 9.1.2 (which itself requires the Firm to retain records for a minimum of five years).

5.5.3. With regards to the personal data of staff, the Firm retains all staff records for a minimum period of six years after the termination of an employment or service contract. If an employee has his or her employment or service contract terminated and subsequently enters into a new employment or service contract with the Firm at a later date, all personal data obtained in the former period shall be maintained and, if necessary, updated upon commencement of the latter period.

5.5.4. Upon the expiry of either period indicated above, the Firm will be responsible for securely destroying all data held for any purpose. This may be conducted in-house or be outsourced at the discretion of the Operations Manager. Unless otherwise stated, all confidential waste should be disposed of through the confidential paper bin by the Head of Compliance's desk.

5.5.5. The Firm takes the view that whilst it is important to regularly assess and update information, none of the existing information can be destroyed due to regulatory requirements imposed by the FCA.

5.6 PRINCIPLE 6: PERSONAL DATA SHALL BE PROCESSED IN ACCORDANCE WITH THE RIGHTS OF DATA SUBJECTS

Under the Act, data subjects have six rights in relation to their personal data:

5.6.1. **A right to access a copy of information held about them**

This is covered in paragraph 6, below.

5.6.2. **A right to object to the use of information if it is or is likely to cause damage or distress**

The Firm takes the view that no customer will ever be subject to unwarranted and substantial damage or distress through their relationship with the Firm and any suggestion of this must be reported immediately to the Data Protection Officer for further guidance.

5.6.3. **A right to prevent use of personal data for direct marketing**

Individuals have the right to prevent their personal data being processed for direct marketing. Any individual can, at any time, give the Firm written notice to stop (or not begin) using their personal data for direct marketing. Further, any individual (regardless of the relationship with the Firm) can exercise this right, and the Firm is under a duty to comply within a reasonable period if it receives such a notice. Guidance provided by the ICO states that a reasonable period is 28 days for electronic communications and two months for postal communications. There are no rules regarding telesales calls, except those phone numbers registered with the Telephone Preference Service ("TPS"); any number listed on the TPS Register must not be contacted for the purpose of unsolicited telesales.

5.6.4. **A right to object to automated decision taking**

An individual has the right to provide the Firm with written notice requiring the personal data not be used for the purpose of automated decision taking. This does not apply to the Firm as the Firm does not undertake any automated decision taking.

5.6.5. **A right to have inaccurate personal data rectified, blocked, erased or destroyed**

This relates to principle 4; if an individual is aware that personal data held by the Firm is inaccurate, they have a right to require that that data be rectified. Due to regulatory requirements, the Firm cannot block, erase or destroy any information. If an error is found in the client's personal data, a note recording that an error has been discovered and rectified should be stored.

5.6.6. **A right to claim for compensation for damage caused by breach of the Act**

If an individual suffers damage as a result of the Firm breaching the Act, they are entitled to make a claim for damages through the court system. In the event of this taking place, the Firm may be able to defend the claim if it can show that all reasonable care was taken to avoid the breach. A definable damage must be shown; distress is insufficient, unlike in paragraph 5.6.2.

5.7 PRINCIPLE 7: MEASURES SHALL BE TAKEN AGAINST UNAUTHORISED OR UNLAWFUL USE OR ACCIDENTAL LOSS, DAMAGE OR DESTRUCTION OF PERSONAL DATA

5.7.1. The Firm recognises the need to have in place appropriate security measures designed to prevent data under the Firm's control from being accidentally or deliberately compromised.

5.7.2. The Firm's security infrastructure is designed and organised to securely hold and manage the use of any and all personal data held by the Firm and prevent the risk of harm that may result from a security breach.

5.7.3. The Firm has put in place appropriate physical and technical security mechanisms and systems, backed up by robust policies and procedures in addition to reliable and well-trained staff.

5.7.4. In the event of a breach in the Firm's technical security measures, the Firm is prepared and ready to respond swiftly and effectively.

5.7.5. The Chief Operating Officer will be responsible for implementing, administering and maintaining the Firm's information security systems, policies and procedures.

5.8 PRINCIPLE 8: PERSONAL DATA SHALL NOT BE TRANSFERRED OUT OF THE EUROPEAN ECONOMIC AREA UNLESS THAT COUNTRY ENSURES AN ADEQUATE LEVEL OF PROTECTION FOR THE RIGHTS OF DATA SUBJECTS.

5.8.1. It is useful for staff to be aware of this principle, however, under the Firm's Terms and Conditions of Business that clients agree to before an account is opened, the Firm is exempt from this principle by way of consent.

6 SUBJECT ACCESS REQUESTS

6.1. Any person who has personal data held by the Firm, regardless of their relationship with the Firm, has the right to request access to all personal data.

6.2. The Firm is required, upon receipt of a valid 'Subject Access Request' made in writing and upon payment of a fee:

- to provide a description of the information held;
- state the purposes for which that information is, has been or will be processed; and
- the recipients to whom that information may be disclosed.

6.3. The Firm takes the view that it is reasonable to charge the maximum fee permissible by law; this fee is currently (as at the time of writing) £10.

6.4. Any valid Subject Access Request must be fulfilled within 40 calendar days of receipt of the request and payment of the fee. If a response is not provided within this period, the individual making the request has the right to complain to the ICO or to apply for a court order requiring disclosure of the information.

6.5. Where the Firm has previously complied with a subject access request under section 7 of the Act by an individual, the data controller is not obliged to comply with a subsequent identical or similar request by that individual unless a reasonable period has elapsed between the previous request and the current request. Whether a period of time is reasonable will be determined at the discretion of the Data Protection Officer, who will have regard to the nature of the data, the purpose for which that data was processed and the frequency with which that data was altered.

7 PERSONAL EQUIPMENT

7.1. Where a member of staff conducts company business on personal equipment, such as (but not limited to) an iPhone or iPad, the Firm retains the right to require that security requirements imposed by the Operations Manager be complied with. Such security requirements will be determined at the Operations Manager's discretion and staff will be notified in the event that such policies change.

7.2. In the event that personal equipment is lost or stolen, the Firm retains the right to remotely remove or retrieve any and all data from that equipment without the explicit consent of the staff concerned.

7.3. In the event that a member of staff leave's the Firm's employment, the Firm retains the right to remotely remove or retrieve any and all data from their personal equipment, if used for company purposes, without the explicit consent of the person concerned.

8 BREACH

8.1. Staff who are aware of or suspect a breach of this policy should report this, in confidence, to the Head of Compliance (or, in her absence, the CEO), in line with the Firm's Public Interest Disclosure Policy.

8.2. Unlawfully obtaining or disclosing personal data or any other breach of section 55 of the Act will be treated seriously be the Firm and may lead to disciplinary action.

8.3. Breach of this policy will be sufficient cause to terminate any contract of employment for gross misconduct.

9 POLICY REVIEW

9.1. The Head of Compliance will be responsible for reviewing this policy annually (or at the request of the CEO or another member of the Board) to ensure that it continues to meet legal requirements and that it reflects best business practice.