Ayres Bright Vickers
Data Retention Policy
14 May 2018

1. Introduction

This Policy sets out the obligations of Ayres Bright Vickers, ("the Firm") regarding retention of personal data collected, held, and processed by the Firm in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "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.

The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);

b) When the data subject withdraws their consent;

c) When the data subject objects to the processing of their personal data and the Firm has no overriding legitimate interest;

d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);

e) When the personal data has to be erased to comply with a legal obligation; or

f) Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Firm for acting for clients in accordance with the purposes set out in their respective letters of engagement, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the GDPR, please refer to the Firm's Data Protection Policy.

2. **Aims and Objectives**

2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Firm complies fully with its obligations and the rights of data subjects under the GDPR.

2.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Firm, this Policy also aims to improve the speed and efficiency of managing data.

3. **Scope**

3.1 This Policy applies to all personal data held by the Firm.

3.2 Personal data, as held by the Firm is stored in the following ways and in the following locations:

a) The Firm's servers, located in 36 Crescent Road, Worthing, West Sussex, BN11 1RL;

b) Laptop computers and other mobile devices provided by the Firm to its employees;

c) Computers and mobile devices owned by employees, agents, and sub-contractors used in accordance with the Firm's Bring Your Own Device ("BYOD") Policy;

d) Physical records stored at 36 Crescent Road, Worthing, West Sussex, BN11 1RL;

4. **Data Subject Rights and Data Integrity**

All personal data held by the Firm is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Firm's Data Protection Policy.

4.1 Data subjects are kept fully informed of their rights, of what personal data the Firm holds about them, how that personal data is used as set out in Parts 12 and 13 of the Firm's Data Protection Policy, and how long the Firm will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

4.2 Data subjects are given control over their personal data held by the Firm including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Firm's use of their personal data, and further rights relating to automated decision-making and profiling, as set out in Parts 14 to 17 of the Firm's Data Protection Policy.

5. **Technical and Organisational Data Security Measures**

5.1 The following technical measures are in place within the Firm to protect the security of personal data. Please refer to Parts 19 to 26 of the Firm's Data Protection Policy for further details:

a) All emails containing personal data must be encrypted;

b) All emails containing personal data must be marked “confidential”;

c) Personal data may only be transmitted over secure networks;

d) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

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

f) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;

g) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using Royal Mail or other approved Postal Service;

h) All personal data transferred physically should be transferred in a suitable container marked “confidential”;

i) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from Andrew Dalglish.

j) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;

k) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Firm or not, without authorisation;

l) Personal data must be handled with care at all times and should not be left unattended or on view;

m) Computers used to view personal data must always be locked before being left unattended;

n) No personal data should be stored on any mobile device, whether such device belongs to the Firm or otherwise without the formal written approval of Andrew Dalglish and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

o) 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 agents, contractors, or other parties working on behalf of the Firm where the party in question has agreed to comply fully with the Firm’s Data Protection Policy and the GDPR;

p) All personal data stored electronically should be backed up daily with backups stored offsite. All backups should be encrypted;

q) All electronic copies of personal data should be stored securely using passwords and encryption;

r) All passwords used to protect personal data should be changed regularly and should must be secure;

s) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

t) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;

u) No software may be installed on any Firm-owned computer or device without approval; and

v) Where personal data held by the Firm is used for marketing purposes, it shall be the responsibility of Andrew Dalglish to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

5.2 The following organisational measures are in place within the Firm to protect the security of personal data. Please refer to Part 24 of the Firm's Data Protection Policy for further details:

a) All employees and other parties working on behalf of the Firm shall be made fully aware of both their individual responsibilities and the Firm's responsibilities under the GDPR and under the Firm's Data Protection Policy;

b) Only employees and other parties working on behalf of the Firm that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Firm;

c) All employees and other parties working on behalf of the Firm handling personal data will be appropriately trained to do so;

d) All employees and other parties working on behalf of the Firm handling personal data will be appropriately supervised;

e) All employees and other parties working on behalf of the Firm handling personal data should exercise care and caution when discussing any work relating to personal data at all times;

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

g) The performance of those employees and other parties working on behalf of the Firm handling personal data shall be regularly evaluated and reviewed;

h) All employees and other parties working on behalf of the Firm handling personal data will be bound by contract to comply with the GDPR and the Firm's Data Protection Policy;

i) All agents, contractors, or other parties working on behalf of the Firm handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Firm arising out of the GDPR and the Firm's Data Protection Policy;

j) Where any agent, contractor or other party working on behalf of the Firm handling personal data fails in their obligations under the GDPR and/or the Firm's Data Protection Policy, that party shall indemnify and hold harmless the Firm against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. **Data Disposal**

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

6.1 Personal data stored electronically (including any and all backups thereof) shall be deleted securely using the Gutmann algorithm or by overwriting with a cryptographically secure random number stream;

6.2 Personal data stored in hardcopy form shall be shredded and recycled;

7. **Data Retention**

7.1 As stated above, and as required by law, the Firm shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods **(**and its retention periodically reviewed), as set out below.

7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

a) The objectives and requirements of the Firm;

b) The type of personal data in question;

c) The purpose(s) for which the data in question is collected, held, and processed;

d) The Firm's legal basis for collecting, holding, and processing that data;

e) The category or categories of data subject to whom the data relates;

7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Firm to do so (whether in response to a request by a data subject or otherwise).

Data Ref.	Type of Data	Purpose of Data	Review Period	Retention Period or Criteria	Comments
Accounts and Audit Files	Financial and personal data	To enable compliance with legal obligations of clients in filing accounts with relevant authorities	Annually	Current clients – Indefinite Former clients – 7 years	Accounts and audit files prepared for a variety of purposes
Personal Tax Returns	Financial and personal data	To enable compliance with fiscal and legal obligations of clients and to determine tax position of clients	Annually	Current clients – Indefinite Former clients – 7 years	
Chargeable assets and gifts	Financial and personal data	To ascertain extent of capital gains and/or inheritance tax liabilities contingent on future events	Ad-hoc	Current clients – indefinite Former clients – 8 years, return records and files or destroy	
Files as Trustee	Financial and personal data	To enable us to meet our obligations as trustee for a given client	Ad-hoc	For period of trusteeship and 7 years thereafter	
General client correspondence	Financial and personal data	To maintain a record of communications with client on a variety of relevant topics	Annually	Current clients – indefinite Former clients – 7 years	
Payroll Records	Files and Scanned Files and Payroll Data	To enable clients to meet their payroll, payroll reporting and auto-enrolment pension obligations	Annually	Current clients – indefinite Former clients – 7 years	

VAT and Bookkeeping Records	Financial and personal data	To enable VAT returns to be completed for clients and to enable clients to meet their day to day financial record keeping obligations.	Annually	Records – return to client annually if possible Current clients Files – indefinitely Former clients files – 7 years	
Permanent Audit Files	Financial and personal data	To maintain a record of pertinent long term information on audit clients	Annually	Current clients – indefinitely Former clients – 7 years	As required by our regulatory body in undertaking audit work
Computer based records	Excel Word Central PDF Emails	To enable us to perform the work agreed with clients in our letter of engagement with them	Annually	Current clients – indefinitely Former clients – 7 years	
Ad-hoc Advisory work for one-off clients	Financial and personal data	To enable us to complete ad-hoc and one off assignments as requested by clients	Annually	Retain for 7 years	

8. **Roles and Responsibilities**

8.1 The Firm's Data Protection Officer is Andrew Dalglish FCCA, who can be contacted at Bishopstone, 36 Crescent Road, Worthing, West Sussex, BN11 1RL.

8.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Firm's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

8.3 The Data Protection Officer shall be directly responsible for ensuring compliance with the above data retention periods throughout the Firm.

8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

9. **Implementation of Policy**

This Policy shall be deemed effective as of 25 May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Andrew Dalglish

Position: Partner / Data Protection Officer

Date: 14 May 2018

Due for Review by: 25 May 2019

Signature: