1.1

HENCHLEYS SOLICITORS

www.henchleys.co.uk

Data Retention Policy
April 2018

2. Introduction

This Policy sets out the obligations of Henchleys, Solicitors of 39a High Street, Littlehampton, West Sussex BN17 5EG ("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, 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.

3. Aims and Objectives

3.1 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.

3.2 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.

4. Scope

4.1 This Policy applies to all personal data held by the Firm**;**

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

a) The Firm's servers, located at the Firm's Littlehampton and Worthing offices

b) Third-party servers, operated by Gmail and AOL

c) Computers permanently located in the Firm's premises at 39a High Street, Littlehampton, West Sussex BN17 5EG and 196/198 Findon Road, Worthing, West Sussex BN14 0EJ

d) Laptop computers provided by the Firm to its employees;

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

f) Physical records stored in the Firm's Littlehampton Office, Worthing Office and two secure garages

5. 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.

5.1 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).

5.2 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.

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

6.1 The following technical measures are in place within the Firm to protect the security of personal data. Please refer to Parts 22 to 26 of the Firm's Data Protection Policy for further details:

a) All emails containing personal data must be marked "confidential";

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

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

d) 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;

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

f) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using first class post;

g) All personal data transferred physically should be transferred in a suitable container marked "confidential";

h) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from KFH or LH

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

j) 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;

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

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

m) 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 KFH or LH 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;

n) No personal data should be transferred to any device personally belonging to an employee without consent 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;

o) All personal data stored electronically should be backed up daily with backups stored onsite and offsite. All backups should be password protected;

p) All electronic copies of personal data should be stored securely using passwords;

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

r) 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;

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

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

6.2 The following organisational measures are in place within the Firm to protect the security of personal data. Please refer to Part 27 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.

7. **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:

7.1 Personal data stored electronically (including any and all backups thereof) shall be deleted;

7.2 Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely;

7.3 Personal data stored in hardcopy form shall be shredded and recycled or disposed of via a contractor engaged by the firm providing a certificate in respect of disposal/destruction in compliance with the GDPR

7.4 Special category personal data stored in hardcopy form shall be shredded and recycled or disposed of via a contractor engaged by the firm providing a certificate in respect of disposal/destruction in compliance with the GDPR

8. **Data Retention**

8.1 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.

8.2 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.

8.3 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;

8.4 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.

8.5 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).

8.6 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

8.7 There are differing data retention periods applicable for different purposes. For example, legal time limitation concerning contractual disputes is 6 years. The authorities require solicitors to keep documentation relevant to anti-money laundering procedures for 5 years. Mortgagees generally require data retention for 6 years. HMRC usually operates on a 6 year period as well. The firm, over the years, has adopted a policy of retaining files/data for 7 years so as to cover the above. There are clear benefits for clients which may be summarised as follows and discussed further

- The documentation/data may be of assistance in relation to subsequent

later instructions received by the firm. For example, information and data received in relation to a property purchase would be highly relevant, a few years later, in the event of a sale of the same property

- The data subject (client) may over time lose important documents and data and, as a firm of solicitors, we often receive requests from clients concerning past matters, enquiring whether we are able to provide certain documents or data e.g. a financial completion statement requested by the client's accountant

We shall be pleased to discuss data retention and the Firm's policy further and we reiterate here the Firm's Data Protection Policy which notes the data protection principles at paragraph 2 and the rights of data subjects (clients) at clause 3 thereof.

Data Ref.	Type of Data	Purpose of Data	Review Period	Retention Period or Criteria	Comments
Data received upon enquiry as to firm's services or instructions for such services	Personal data of potential client or clients and matter to be the subject of legal services. As referred to in the Firm's Data Protection Policy and Policy Notice.	Providing details of the Firm's legal services and compliance with legal obligations such as anti-money laundering/terrorist financing regulations	During the continuation of instructions pursuant to the Firm's retainer	7 years from conclusion of legal services or termination of instructions	The firm will retain personal data for 7 years upon termination of the firm's retainer pursuant to data subject's consent or earlier upon exercise of any rights pursuant to Clause 3 of the Firm's Data Protection policy or in compliance with legal obligations such as anti-money laundering/terrorist financing regulations. See in particular paragraph 7.7
Data received upon performing legal services as per instructions/retainer	As above	As above but for the additional purpose of undertaking work pursuant to instructions for the provision of legal services.	As above	As above	As above
Data received up to conclusion of matter the subject of request for legal services/retainer or upon earlier termination of such retainer	As above	As above	As above	As above	As above

Data received upon employing member of staff	Personal data of employee pursuant to the Firm's Employee Data Protection Policy and Privacy Notice	To enable the firm to employ the individual concerned and to enable the firm to discharge obligations and responsibility relevant contract of employment including paying salary, PAYE, NIC, pension contributions and compliance with legal obligations as referred to in line 1 above.	During the continuation of employment and pursuant to contract of employment	7 years from termination of employment	The firm will retain personal data for 7 years upon termination of employment pursuant to data subject's consent or earlier upon exercise of any rights pursuant to Clause 3 of the Firm's Data Protection policy or in compliance with legal obligations such as anti-money laundering/terrorist financing regulations. See in particular paragraph 7.7
Data received during the course of employment of member of staff	As above	As above	As above	As above	As above
Special category personal data received e.g. for PI claims	As specifically referred to in Privacy Notice at paragraph 5.	Providing legal services pursuant to contract/retainer	During the continuation of instructions pursuant to the Firm's retainer	7 years from conclusion of legal services or termination of instructions	The firm will retain personal data for 7 years upon termination of the firm's retainer pursuant to data subject's consent or earlier upon exercise of any rights pursuant to Clause 3 of the Firm's Data Protection policy or in compliance with legal obligations such as anti-money laundering/terrorist financing regulations. See in particular paragraph 7.7.

Data received during the course of compliance with legal obligations such as compliance with AMLR	Personal data to establish identity verification' provenance/source of funds, business activities	Compliance with applicable regulations	During the continuation of the solicitor/client relationship the subject of the regulations in question	5 years pursuant to AMLR but see comments	The Firm will generally retain data for 7 years as noted in comments above subject to the exercise of any rights by the data subject as also referred to above.
Document entrusted to the firm for safe custody	Deeds, Wills, LPAs and other legal documents	Safe custody at the request of the data subject	As per Data Retention Policy and the instructions of the data subject	For property deeds and documents – until further instructions upon dealing with land/property in question. In relation to Wills – pending amendment to Will or death or other instructions. In relation to other documents, pending further instructions from the data subject. The control of data retention is in the hands of the data subject	In this instance, documents are specifically retained at the request of the data subject who is in control of continuing data retention.

9. **Roles and Responsibilities**

9.1 The Firm's Data Protection Officer is KFH

9.2 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.

9.3 KFH and LH shall be directly responsible for ensuring compliance with the above data retention periods throughout the Firm

9.4 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.

10. **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: Kevin François Henchley.

Position: Principal.