Data Retention Policy

Gullands LLP

Issue Date	01.11.2022
Approved By	Amanda Finn
Managed By	The Strategic Partner
Next Review Date	01.09.2023
Version Control	Version 1

1. Introduction

This Policy sets out the obligations of **Gullands LLP** ('the Firm') regarding retention of personal data collected, held and processed by the Firm in accordance with the UK General Data Protection Regulation ('UK GDPR'), which sits alongside the Data Protection Act 2018 (DPA 2018).

The UK 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 UK 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 UK 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 UK GDPR to protect that data).

In addition, the UK 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:

- Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
- When the data subject withdraws their consent;
- When the data subject objects to the processing of their personal data and the Firm

has no overriding legitimate interest;

- When the personal data is processed unlawfully (i.e. in breach of the UK GDPR);
- When the personal data has to be erased to comply with a legal obligation; or
- 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 and 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 UK GDPR, please refer to the Firm's **GDPR & Data Protection Policy.**

2. Aims and Objectives

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 subjects' 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 UK GDPR.

In addition to safeguarding the rights of data subjects under the UK 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

This policy applies to all personal data held by the Firm and any third-party data processors processing personal data on the Firm's behalf.

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

- Computers permanently located in the Firm's premises at the Gravesend Office & Maidstone Office
- Laptop computers and other mobile devices provided by the Firm to its employees
- Computers and mobile devices owned by employees, agents and sub-contractors
- Physical records stored with Oasis located at, Oad Street, Borden, Sittingbourne, Kent

ME9 8JP

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

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

Data subjects are kept fully informed of their rights, of what personal data the Firm holds about them, how that personal data is used 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).

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 **GDPR & 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.

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

The following technical measures are in place within the Firm to protect the security of personal data:-

- Personal data may only be transmitted over secure networks;
- All personal data transferred physically should be transferred in a suitable container marked "confidential";
- No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from **Paul Mannering;**
- All hard copies of personal data, along with any electronic copies stored on physical media, should be stored securely;
- 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;
- Personal data must be handled with care at all times and should not be left unattended or on view;
- Computers used to view personal data must always be locked before being left

unattended;

- No personal data should be stored on any mobile device, whether such device belongs to the Firm or otherwise 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;
- All personal data stored electronically should be backed up frequently.
- All electronic copies of personal data should be stored securely using passwords and encryption;
- All passwords used to protect personal data should be changed regularly and must be secure;
- 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 Security Manager does not have access to passwords;
- All software should be kept up-to-date. Security-related updates should be installed;
- No software may be installed on any Firm-owned computer or device without approval; and
- Where personal data held by the Firm is used for marketing purposes, it shall be the responsibility of **Paul Mannering** 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.

The following organisational measures are in place within the Firm to protect the security of personal data:-

- 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 UK GDPR and under the Firm's **GDPR & Data Protection Policy**;
- 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;
- All employees and other parties working on behalf of the Firm handling personal data will be appropriately trained to do so;
- All employees and other parties working on behalf of the Firm handling personal data will be appropriately supervised;
- 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;

- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- The performance of those employees and other parties working on behalf of the Firm handling personal data shall be regularly evaluated and reviewed;
- All employees and other parties working on behalf of the Firm handling personal data will be bound by contract to comply with the UK GDPR and the Firm's **GDPR & Data Protection Policy**;
- 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 UK GDPR and the Firm's **GDPR & Data Protection Policy**;
- Where any agent, contractor or other party working on behalf of the Firm handling personal data fails in their obligations under the UK GDPR and/or the Firm's **GDPR & 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 (subject to the Solicitors Regulation Authority's requirements to store data), personal data shall be deleted, destroyed or otherwise disposed of as follows:-

- Personal data stored electronically (including any and all backups thereof) shall be deleted;
- Personal data stored in hard copy form shall be shredded.

The Firm regards all information held for or on behalf of a client as an information asset and such information will be stored in either paper form or electronic form clearly marked with the client's name and matters reference number ensuring that the information assets can be identified as belonging to that client. On the expiry of the retention period, all information assets will be destroyed as part of the data disposal process.

The use, control, access and retention of all types of data held by the Firm is detailed in the Information Asset Register.

7. **Data Retention**

As the Firm is regulated by the Solicitors Regulation Authority, it is required to store client files in paper form or electronically for a period of 6 years under rule 13.1 of the SRA Accounts Rules (the regulatory period).

It is the Firm's policy to store all records for a minimum period of 7 years, unless an extended period is agreed with the client or dictated by the matter, refer to ***Appendix 1, File and Data Retention Periods by matter type***, to take into account any issues that may arise towards the end of the regulatory period and will allow the Firm to respond to any questions that arise.

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.

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.

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

- The objectives and requirements of the Firm;
- The type of personal data in question;
- The purpose(s) for which the data in question is collected, held, and processed;
- The Firm's legal basis for collecting, holding, and processing that data;
- The category or categories of data subjects to whom the data relates;
- The requirements of the regulator.

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.

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).

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 or the service provided by the firm requires data to be stored to enable the service to be provided.

8. **Data Retention and the AML Regulations**

In accordance with Regulation 19 of the AML Regulations, the Firm is required to retain all records obtained for Client Due Diligence purposes for 5 years. In accordance with section 7, the Firm will retain records for a period exceeding this minimum requirement.

The Regulations do, however, require retention beyond 5 years in the event that the Firm: -

- Is required to retain records by another enactment or rule made by the Solicitors Regulation Authority;
- Is required to retain the data for the purposes of any court proceedings; or
- Has reasonable grounds for believing that the records containing personal data that needs to be retained for the purposes of legal proceedings.

In the event of one of these circumstances, the Firm will be required to retain records for an appropriate timeframe as guided by the Regulator or set by the actual or potential litigation.

9. **Roles and Responsibilities**

The Firm's **Data Protection Officer** is **Paul Mannering**.

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 **GDPR & Data Protection Policy**), and with the UK GDPR and other applicable data protection legislation.

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

10. **Version Control & Updates**

This policy is reviewed annually and updated as necessary.

In the event of any statute or regulation changes, this policy will be brought up to date at that point in time and any policies affected will also be updated.

A printed version of this policy should be considered obsolete.

Appendix 1: File and Data Retention Periods

Matter Type	Period
Conveyancing Purchase, Re-Mortgage, Transfer of Equity	12 Years
Conveyancing Sale	6 Years
Litigation	6 Years
Childcare	Until the Child reaches the age of 21
Matrimonial (provided that where continuing order is in force client is sent a copy of the order & relevant affidavits and court documentation	8 Years
Probate & Administration	12 Years
Wills	Indefinitely
Trusts (unless file given to client)	Indefinitely
Registered Title Deeds	Indefinitely

Type of Data	Retention Period
Recruitment Data (unsuccessful candidates) both paper and electronic	
Application Forms CV and contact details Medical Issues	6 months after notifying candidates of the outcome of the recruitment exercise
Employee Data both Paper and Electronic	
All recruitment data as above Name address Medical Records Bank Details Emergency Contact Details	Seven years after employment ends
Client Data Both paper and electronic	
Client Name address and contact details ID and AML Purposes Bank details Medical Records Personal Information (such as bank statement house valuations tax records) Shared data with organisations such as SearchFlow, Bundledocs, Reliance, Microsoft Teams	As notified to client in retainer letter and closing letter usually no less than 6 years but can be more depending on the nature of the case
Supplier/Expert Data both paper and electronic	
Name address and contact details Expertise Contract terms Bank details for payment	6 years after bill paid or on destruction of file to which it relates
Mobile Phone Data (electronic)	
Numbers Names Call log Email data Txt and whatsapp data Any personal calls/data made by employees	As notified to client in retainer letter and closing letter usually no less than 6 years but can be more depending on the nature of the case Seven years after employment ends.
Notary Public Data both paper and electronic	

All data relating to notarial acts carried out but those within the firm	Forever
Wills & Deeds paper and electronic records of paper	
Wills Deeds Other items stored on behalf of clients	Indefinitely Until required by client or death of client
Website Cookies electronic only	
Cookies acquired from any and all surfing on our website Email newsletters related cookies Forms related cookies Site preferences cookies Third party cookies	Until the user deletes or disables