



Data Retention Policy

Data Security



		DATA SECURITY		
POLICY	Data Retention Policy			
Approved by:	Jonathan Cartwright, Director of Strategy (& DPO)	Reviewed (No changes made)	Yes	Date: 1 st July 2023
Approved by:	Jonathan Cartwright, Director of Strategy (& DPO)	Revised (Changes made)	Yes	Date: 31 st Jan 2024
Department:	All	Prior Policy: N/A		
Applies to:	All			
Data Classification: Sensitive		Electronic Approvals are maintained in the Policy Repository		
Additional Information:				



1. Introduction

This Policy sets out the obligations of Silver Agency LTD a company registered in England & Wales under number 05489754, whose registered office is at 6 Manor Park Business Centre, Mackenzie Way, Cheltenham, Glos, GL51 9TX (“the Company”) regarding retention of personal data collected, held, and processed by the Company in accordance with the Data Protection Legislation. “Data Protection Legislation” means all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the “UK GDPR”), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation.

The Data Protection Legislation 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 Data Protection Legislation 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 Data Protection Legislation, 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 Data Protection Legislation to protect that data).

In addition, the Data Protection Legislation 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 Company has no overriding legitimate interest;
- d) When the personal data is processed unlawfully (i.e. in breach of the Data Protection Legislation);
- 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 Company for processing



client-owned marketing data, managing employee and recruitment data and processing the company's own marketing data, 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 Data Protection Legislation, please refer to the Company'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 Company complies fully with its obligations and the rights of data subjects under the Data Protection Legislation.
- 2.2 In addition to safeguarding the rights of data subjects under the Data Protection Legislation, by ensuring that excessive amounts of data are not retained by the Company, 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 Company.
- 3.2 Personal data, as held by the Company is stored in the following ways and in the following locations:
 - a) Third-party servers operated and hosted by Microsoft365/Azure server platforms and located Sharepoint 365 Data Storage.
 - b) Laptop computers and other mobile devices provided by the Company to its employees;
 - c) Computers and mobile devices owned by employees, agents, and sub-contractors used in accordance with the Company's Bring Your Own Device ("BYOD") Policy.
 - d) Third-party servers, operated by 'Breathe'

4. Data Subject Rights and Data Integrity

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

- 4.1 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used as set out in the Company's Data Protection Policy, and how long the Company 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 Company 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 Company's use of their personal data, and further rights relating to



automated decision-making and profiling , as set out in the Company's Data Protection Policy.

5. Technical and Organisational Data Security Measures

- 5.1 The following technical measures are in place within the Company to protect the security of personal data. Please refer to the Company's Data Protection Policy for further details:
- a) M365 uses the highest encryption available called TLS (Transport Layer Service) to encrypt the connection/Sessions between two email servers.
 - b) All emails containing personal data must be marked "confidential";
 - c) Personal data may only be transmitted over secure networks;
 - d) All personal data transferred physically should be transferred in a suitable container marked "confidential";
 - e) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from HR Director
 - f) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation;
 - g) Personal data must be handled with care at all times and should not be left unattended or on view;
 - h) Computers used to view personal data must always be locked before being left unattended;
 - i) No personal data should be stored on any mobile device, whether such device belongs to the Company or otherwise
 - j) 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 Company where the party in question has agreed to comply fully with the Company's Data Protection Policy and the Data Protection Legislation;
 - k) All personal data stored electronically should be backed up using **SkyKick** and stored **offsite** using 256-bit encryption at rest and 128-bit encryption in-transit. Data never leaves the Azure environment which ensures all the inherent security and compliance capabilities that Azure offers.
 - l) Password complexity with MFA is enabled for M365 accounts
 - m) Passwords are encrypted in M365 and accounts will be locked after 10 failed logon attempts
 - n) 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;
 - o) All software should be kept up to date. Security related updates will be installed 9 days follow its release and installed via the Automate agent.
 - p) No software may be installed on any Company-owned computer or device without approval;
 - q) Where personal data held by the Company is used for marketing purposes, it



shall be the responsibility of Director of Strategy 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 Company to protect the security of personal data. Please refer to the Company's Data Protection Policy for further details:
- a) All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Data Protection Legislation and under the Company's Data Protection Policy;
 - b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;
 - c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
 - d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;
 - e) All employees and other parties working on behalf of the Company 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 Company handling personal data shall be regularly evaluated and reviewed;
 - h) All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the Data Protection Legislation and the Company's Data Protection Policy;
 - i) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the Data Protection Legislation and the Company's Data Protection Policy;
 - j) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the Data Protection Legislation and/or the Company's Data Protection Policy, that party shall indemnify and hold harmless the Company 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 following the Microsoft default retention policy of 30 days.



- 6.2 Special category personal data stored electronically (including any and all backups thereof) shall be deleted following the Microsoft default retention policy of 30 days.

7. Data Retention

- 7.1 As stated above, and as required by law, the Company 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 Company;
 - 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 Company'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 Company 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
Client-owned marketing data	PII contact data (lead data)	Acting as a processor of this data to facilitate marketing activity on behalf of our clients	Every 3 years	1 year
The Company's own marketing data	PII contact data (lead data)	Acting as a processor of this data to facilitate marketing activity	Every 3 years	Deleted once the data is no longer required or relevant
Employee data	PII & special category data	To ensure the efficient and effective management of the business and its employees	Every 3 years	During employment and 7 years post
Recruitment data	PII contact data	To support the management of candidates and potential candidates	Every 3 years	30 days following to conclusion of any recruitment activity



8. Roles and Responsibilities

- 8.1 The Company's Data Protection Officer is Jonathan Cartwright, Director of Strategy, jonny@silver.agency
- 8.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the Data Protection Legislation.
- 8.3 The Data Protection Officer AND department heads shall be directly responsible for ensuring compliance with the above data retention periods throughout the Company.
- 8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of Data Protection Legislation compliance should be referred to the Data Protection Officer.