

Data Retention Policy (ISP-40)

1. About this policy	2
2. Policy Scope	2
3. Purpose of Data Retention	2
4. Types of Personal Data	3
5. Location of Personal Data	3
6. Business Retention and Erasure of Personal Data	3
7. Retention Criteria	4
8. Data Retention Periods	5
8.1 Retention of Client, Supplier and third Party Personal Data Schedule	6
8.2 Retention of Employee, Worker, Consultant, Partner etc. Personal Data Schedule	8
Version Control	10

1. About this policy

This Retention Policy outlines how the Business ("we", "our", "us", the "Business") meets its data privacy obligations under the UK General Data Protection Regulation (UKGDPR). Personal data is defined as any information identifying a living person or relating to a living person who can be identified, directly or indirectly, from that data alone or in combination with other identifiers we possess or can reasonably access.

Personal data may include information such as a person's name, address, email address, identification number, online identifiers, or other identity verification elements.

This policy applies to all internal employees, workers, consultants, partners, and to all clients, prospective clients, and third parties involved with the Business.

This Policy supplements our **Data Protection Policy** and incorporates its definitions. In case of any conflict between this policy and retention/destruction procedures for Client or third-party materials, the latter policies take precedence, as long as they are compatible with UKGDPR.

2. Policy Scope

This policy applies to all employees, workers, consultants, partners, clients, prospective clients, suppliers, vendors, and third parties associated with the Business. It is not a contractual document and is not included in employment or engagement terms. The Business reserves the right to modify or amend this policy at any time.

3. Purpose of Data Retention

This policy ensures compliance with UKGDPR by processing personal data lawfully, fairly, and transparently. Specifically, it ensures:

- **Legitimate Data Collection:** Personal data is collected only for specified, explicit, and legitimate purposes, and is not processed in ways

incompatible with those purposes.

- **Data Minimisation:** Personal data must be adequate, relevant, and limited to what is necessary.
- **Data Accuracy:** Personal data is kept accurate and up to date. Inaccurate data must be corrected or deleted without delay.
- **Retention Limitations:** Personal data must not be kept longer than necessary for its intended purpose.
- **Data Protection:** Adequate technical and organisational measures are in place to protect personal data from unauthorised processing, loss, or damage.

Our Data Protection Officer (DPO) is responsible for ensuring compliance with this policy and all UKGDPR requirements. Any questions about this policy should be directed to the DPO at **dpo@myserene.io**

4. Types of Personal Data

The Business gathers and processes personal data regarding its employees (including job applicants), contractors, consultants, partners, clients, prospects and other third parties, such as suppliers and vendors of products and services.

5. Location of Personal Data

Personal data related to clients, prospects, suppliers, and other third parties is stored by various departments within the Business, including sales, marketing, and finance. All data is stored within the UK.

6. Business Retention and Erasure of Personal Data

The Business ensures that it adheres to the data protection principles delineated in this policy and in line with the requirements of UKGDPR, with a particular emphasis on:

- Documents are routinely reviewed to guarantee that they are sufficient, pertinent, and restricted to the extent necessary to support the Business's operational and/or employment requirements (where applicable) and/or

compliance with legal or regulatory requirements.

- Secure storage and protection from unauthorised or unlawful processing, as well as incidental loss, destruction, or damage, are implemented for documents. The Business will employ data obfuscation techniques in accordance with the sensitivity and criticality of the data processed, and wherever feasible, anonymisation will be implemented to prevent the identification of individuals.
- The Business will ensure that documents and records, regardless of whether they are stored in digital format or as paper records, are permanently and securely expunged following their destruction.
- The Business will determine whether the data requires anonymisation when a document is archived, and it is necessary to consider whether the document should be destroyed, subject to a further period of retention, or perpetual retention as an archive.

7. Retention Criteria

We keep personal information we acquire from you if we have a valid business need to do so (for example, to provide you with a requested service or to comply with applicable legal, tax, or accounting obligations).

When we no longer have a legitimate business reason to process your personal information, we will either delete or anonymise it. If this is not possible (for example, because your personal information is stored in backup archives), we will securely store your personal information and isolate it from further processing until deletion is possible.

The Business considers the purpose for which personal data was collected when determining the appropriate retention period. Retention periods are set out in the schedules below and may also be determined by applicable contractual, legal or regulatory requirements.

The following criteria will be considered by the Business in determining our data retention periods:

- Any directives or regulations from our regulatory body;
- What our insurance providers demand and what our insurance terms state;
- The reason we retain the Personal Data;

- The potential risk of harm from unauthorised use or disclosure of the Personal Data;
- Whether we need the Personal Data to defend any proceedings in line with the Statute of Limitations. This includes but is not limited to any orders for the preservation of evidence, including Personal Data that may arise within the civil or criminal courts.
- Any legal or regulatory requirements;
- Any specific requests from a Data Subject to retain such Personal Data;
- Any legal, accounting, or reporting requirements. This includes any matters in relation to HR and people management and requirements from bodies such as the HMRC;
- Whether we must retain such Personal Data to help us carry out our services or fulfil a contract; and/or
- Any investigations required by the regulator or law enforcement agencies within the UK or elsewhere

8. Data Retention Periods

The schedule below provides an overview of the categories of personal information we maintain and the length of time we believe is suitable for its keeping.

The schedule is meant to serve as a guide only, and the Business may deviate from the retention periods listed if there is a valid and legal basis to do so.

In certain situations, the Business will make sure that any further retention of personal data beyond what is suggested in the schedule below takes into account the principles of protecting personal data and that the Business otherwise complies with the Data Protection Policy. Additionally, the business will regularly evaluate its records to determine if the personal data contained therein needs to be kept on file or if it may be anonymised or deleted.

Please note the recommended retention periods set out in the below tables are subject to further review and may be changed from time to time.

8.1 Retention of Client, Supplier and third Party Personal Data Schedule

Type of record containing personal data	Retention period	Reasons for retention period including where applicable any legal requirements
Client documents This may include: - Signed contracts between the parties - Data Processing Agreements - Communications - Documents and drafts of documents, including SOWs / SLAs - Records of telephone calls - Master Agreements - Final reports or deliverables provided to clients, where these do not contain client-provided personal data	7 years following termination of the client relationship, unless otherwise specified or there is a specific legal or contractual reason for longer retention.	Limitation Act 1980; establishment, exercise or defence of legal claims; contractual and business record-keeping requirements.
Client-provided data processed in delivery of Serene services This may include: - Pseudonymised transactional data provided by clients - Unique customer identifiers	Retained in pseudonymised form for the period specified in the applicable client contract, Statement of Work and/or Data Processing Agreement. At the end of that period, data will be securely deleted, returned or anonymised in accordance with the applicable contractual requirements upon client request. Where permitted, irreversibly anonymised data may be retained for up to 10 years.	Processing of personal data is undertaken on behalf of the client in accordance with the client's documented instructions and applicable contractual and data protection requirements. Anonymised data retained following the applicable personal data retention period is not personal data and may be retained for the stated business purposes.
Supplier contracts This may include: - SOWs - Signed contracts	Life of contract plus 7 years	Limitation Act 1980

• Communications • Notices given or received • SLAs		
CRM database This may include contact details and preferences of clients, prospects, suppliers and other third parties	The Business's CRM database will be reviewed on an annual basis and obsolete personal data removed or anonymised	
Third party enquiries This may include enquiries which did not convert into a contract / agreement with the Business to provide a product or service.	1 year	
Data Subject Access Requests Any request from a data subject to exercise their rights under the UKGDPR (or other laws / regulations relating to data protection)	7 years from the conclusion of the request	Limitation Act 1980; UKGDPR
Records of Business actions This may include: • Claims brought by the Business • Complaints against the Business which do not result in a professional indemnity notification	In relation to legal claims, 7 years from the conclusion, settlement or withdrawal of the claim; in relation to complaints 7 years from the conclusion of our complaints procedure.	Limitation Act 1980
Financial management and accounting records This may include: • Annual plans and budgets • Accounts payable and receivable ledgers • Annual audit reports • Financial statements • Bank statements, cancelled cheques, deposit slips	The current financial year and 7 years prior to it.	Value Added Tax Act 1994; Limitation Act 1980

• Business expense records • Electronic fund transfer documents • Invoices • Tax records		
Insurance records other than documents relating to claims under our professional indemnity insurance This may include: • Insurance claims • Insurance applications • Insurance contracts and policies • Settlement or withdrawal of claims	In relation to insurance claims, 7 years from the conclusion, settlement or withdrawal of the claim. In relation to other insurance related documentation 7 years from the conclusion of the insurance policy to which it relates	Limitation Act 1980

8.2 Retention of Employee, Worker, Consultant, Partner etc. Personal Data Schedule

Type of employment record	Retention period and reasons (where appropriate)
Recruitment records These may include: • Completed online application forms or CVs. • Equal opportunities monitoring forms. • Assessment exercises or tests. • Notes from interviews and short-listing exercises. • Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may be transferred to a successful candidate's employment file.) • Criminal records checks. (These may be transferred to a successful candidate's employment file if they are relevant to the ongoing relationship.)	Six months after notifying rejected candidates of the recruitment results. The rationale for this is to account for the time constraints for any rejected candidate to file a claim for discrimination or unfair treatment resulting from the recruitment process (S.123 Equality Act 2010). For successful candidates who are hired by the Business, certain of these records (where relevant to the ongoing employment relationship) may be kept while the individual is still working. In general, application forms, CVs, assessment exercises and tests, and interview notes will be kept for no more than two years after employment begins.
Right to Work checks	Three years after the termination of employment.

Contracts These may include: • Written particulars of employment. • Contracts of employment or other contracts. • Documented changes to terms and conditions.	While employment continues and for seven years after the contract ends. This is to take into account the limitation periods for bringing claims against the Business – Limitation Act 1980.
Payroll and wage records These may include: • Payroll and wage records • Details on overtime. • Bonuses. • Expenses. • Benefits in kind.	These must be retained for at least three years following the end of the tax year to which they pertain. However, due to their possible importance in wage disputes, they will be kept for seven years after employment ends. See Gov.uk: PAYE and payroll for employers; https://www.gov.uk/payee-for-employers/keeping-records ; as well as Section 5 of the Limitation Act 1980 and the National Minimum Wage Regulations 1998 (as modified).
Current bank details	Bank details will be deleted as soon after the end of employment as possible once final payments have been made
PAYE records	These must be retained for at least three years following the end of the tax year to which they pertain. However, due to their possible importance in wage disputes, they will be kept for seven years after employment ends.
Payroll and wage records for LLPs	These must be retained for six years after the fiscal year end in which payments were made. However, due to their possible importance in wage disputes, they will be kept for seven years after employment ends.
Records in relation to hours worked and payments made to workers	These must be preserved for three years, beginning on the day the pay reference period immediately following the one to which they relate ends. However, due to their possible importance in pay disputes, they will be kept for seven years after the employment relationship ends (Employment Time Regulations 1998 and Limitation Act 1980).
Travel and subsistence	While employment continues and for seven years after employment ends (Limitation Act 1980).
Record of advances for season tickets and loans to employees	While employment continues and for seven years after employment ends.
Personnel records These include: • Qualifications/references. • Consents for the processing of special categories of personal data. • Annual leave records. • Annual assessment reports. • Disciplinary procedures.	While employment continues and for seven years after employment ends (Limitation Act 1980).

- Grievance procedures. - Death benefit nomination and revocation forms. - Resignation, termination and retirement	
Records in connection with working time Working time opt-out	Three years from the date on which they were entered into (Working Time Regulations 1998)
Records to show compliance, including: - Time sheets for opted-out workers. - Health assessment records for night workers.	Three years after the relevant period (Working Time Regulations 1998)
Maternity records These include: - Maternity payments. - Dates of maternity leave. - Period without maternity payment. - Maternity certificates showing the expected week of confinement.	Four years following the end of the tax year in which the maternity pay period expires (Regulation 26, The Statutory Maternity Pay (General) Regulations 1986, as modified).
Accident records These are created regarding any reportable accident, death or injury in connection with work.	For at least four years from the date the report was made (to take into account limitation period under Limitation Act 1980 and time for issuing and serving proceedings).

Version Control

Title	Data Retention Policy ISP-40			
Description	Policy Document			
Created By	Information Security Office			
Date Created	2025			
Maintained By	Information Security Office			
Approved By	Board of Directors			
Version Number	Modified By	Modifications Made	Date Modified	Status
1.0	ISO	Initial creation	2024	Superseded
1.1	ISO	Reviewed for 2025 Audit purposes - no material update	04/2025	Superseded
1.2	ISO	Reviewed for 2026 Audit purposes - changes made to reflect current operating model	04/2026	Live