SQFT Knowledge Services

RECORD RETENTION AND ERASURE POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/RREP/POL/043	03-Jan-2023	Initial version created	K.Gokhul	S.Nandhini
1.0	SQFT/RREP/POL/043	01-Mar-2023	Reviewed and No Changes are done	K.Gokhul	S.Nandhini
1.0	SQFT/RREP/POL/043	29-Feb-2024	Reviewed and No Changes are done	S.Nandhini	K.Gokhul

TABLE OF CONTENTS

1. PURPOSE, SCOPE, AND OBJECTIVES

This Policy has been established to set the required retention periods for specified categories of personal data, as well as to guide the destruction of records within SQFT Knowledge services.

With this policy, it is therefore established a data and records management system complaint with General Data Protection Regulation ("GDPR") which allows for an efficient handling of personal data-related records (i.e. all documents regardless of format) that may be created, received or maintained.

This policy applies to all the business units, processes, systems and staff (permanent, fixed term and temporary staff) in all countries in which the company carries out business and has dealings or other business relationships with third parties.

Furthermore, this policy applies to all records used at company, including but not limited to:

- Emails
- Word Documents
- Spread Sheets
- PDF Files
- Web Files
- Video and Audio files

Given the aforementioned information, the company's objectives surrounding the establishment of this policy are concerning the management of the following processes:

- The conception and storage of records
- Compliance with legal, regulatory and contractual requirements
- The protection of record confidentiality, integrity, and validity
- Access to and disposal of records
- Usage of the records and information contained therein

2. POLICY STATEMENT

SQFT Knowledge Services acknowledges that the efficient management of personal data is crucial and must be looked for in order to attain a more proficient document and records organization that better supports the company's core business functions.

This policy has been developed to meet the best practices of records and personal data management, with the goal of achieving compliance to legal and regulatory obligations concerning personal data protection, necessary to:

- Certify that the company act in a structured, efficient and accountable way
- Provide a better backup and disaster recovery in terms of personal data, fundamental for ensuring business continuity
- Protect the interests of the company and right of data subjects
- Avoid inaccurate or misinforming data, as well as minimize risks to personal data
- Satisfy document retention requirements in line with legislative and regulatory impositions

Information held for longer than it is strictly necessary conveys an additional risk ad cost can lead to the breach of data protection rules and principles, therefore, the company shall only retain records for the time necessary in accordance to their legitimate purposes.

3. RESPONSIBILITIES

The SQFT has the responsibility of maintaining its records and documents control systems according to the legislative and regulatory impositions. The Data Privacy Officer has overall responsibility over this policy

The Data Protection Officer is responsible for the overall management of records in the SQFT, shall give relevant guidance for good records management practices and shall endorse compliance with this policy at all times, so that information will be retrieved in an easy, appropriate, and timely manner. Moreover, any suspicion of a breach to this policy must be promptly communicated to the Data Protection Officer.

The Information Asset Owners (IAO) are designated to all systems and records designated and are allocated based on their role, business area and level of access to the data required.

Data Owners are responsible for taking reasonable measures to produce and uphold the data retention schedule for their area, ensure data and records are managed in line with their data retention schedule, guarantee data and records are disposed of and that disposal is appropriate for the type of data. Certify that logs are maintained for Special Categories of Personal Data within their area.

All employees are responsible for working in accordance with this policy and schedule, but also in consonance with any relevant and applicable procedure and guidelines.

4. RETENTION GUIDELINES AND PROCEDURE

- **General Data Protection Regulation (GDPR) – Retention General Principles**
  The **GDPR's Article 5** establishes the principle of "Storage limitation", under which organizations must ensures that personal data be kept in a form that permits:
  - Identification of data subjects for no longer than necessary in relation to the purposes for which the personal data are processed
  - Personal data may be stored for longer periods, inasmuch as the personal data will only be processed for archiving purposes in the public interest, Scientific or historical research purposes or statistical purposes as per Article 89(1) Subject to implementation of the appropriate technical and organizational measure required by the regulations in order to safeguard the right and freedom of the data subject
- **Retention Periods Protocols**
  The (person responsible) defines the time period for which the records should be retained through the Data Retention Schedule, present in Annex I.

  All records held during their specified time periods are traceable and retrievable. Any file movement, use or access is trailed and logged, including inter-departmental alterations. For all data collected, used and stored within the Company, we:
  - Establish and perform periodical reviews of the data retained, verifying purposes, validity, accuracy and necessity to retain;

- Determine and attest retention periods, with special ponderation to:

  - ✓ Requirements of the Company
  - ✓ Category of personal data
  - ✓ Purpose of processing
  - ✓ Lawful basis for processing
  - ✓ Categories of data subjects
  - ✓ Specific retention periods set by the Supervisory Authority or Law.

- Where it is not possible to define a legal retention period pursuant to the GDPR requirement, the SQFT shall ascertain the criteria try' which the period can be determined. If requested by the data subjects, these criteria shall also be provided to them;
- Shall ensure the records pending audit, litigation or investigation are not destroyed or modified
- Transfer paper-based records to an alternative media format in cases of long retention periods.

- **Safeguarding during the Data Retention period**

The SQFT shall ascertain that documents and data are stored in a way that meets the "Privacy by Design" principle and appropriate safeguards are applied regardless of storage type or location.

If electronic Storage media are selected, any procedures and systems ensuring that the documents can be accessed during the retention time period shall also be stored in order to safeguard the documents against loss due to potential technological changes. The Company shall also store as few copies of the same documents and data as possible.

The documents shall also be retained in a secure Location, with authorized personnel being the only ones to have access to them. Once the retention period ends, the documents are either reviewed, archived or securely destroyed, determined by their purpose and action type.

The responsibility for the storage falls to the (person responsible e.g. DPO) and the location of data and documentation storage will comply with the GDPR.

Typically, the storage whereabouts will be on-site, and several steps will be taken to secure electronic records, such as:

- Not using computer hard drives to store sensitive data and choosing to keep that data stored in record-keeping systems or, alternatively, in secured network drives.
- Guarantee that all computer systems with these records are configured with security systems, anti-virus software, password protection and rigid access control features.
- Regularly audit computers and network locations and assess their security and integrity.

5. RECORD DISPOSAL

- **Routine Disposal Schedule**
  All data of confidential or sensitive nature, on paper or electronic media, must be securely destroyed when no longer needed. This ensures compliance with the Data Protection laws and the onus of confidentiality to our staff, customers, and stakeholders.

  The Company is devoted to the secure and safe disposal of any information assets in consonance with our contractual and legal duties and we do so in an ethical and compliant manner.

  Our approach and procedures are in conformity with the laws and provisions made in the GDPR and all staff are trained and advised accordingly on the procedures and controls in place.

- **Destruction Method**
  For the destruction of document and data, the Company uses the classification assigned to them to prescribe the adequate means of disposal:

  - **Level I** record include Sensitive personal data. For the disposal of these types of documents, when on paper, they shall be securely disposed of as confidential waste and can either be shredded or burned on-site or by professional disposal services. When these records are in electronic format, the storage hardware may be physically destroyed through Incineration, if needed, &addition to being completely wiped. A record of documents disposal must be maintained.
  - **Level Il** records are those that comprise information that is the second highest security and confidentiality level, which include personal data. These documents, if on paper, shall be disposed of as confidential Waste and shredded whether on-site or by professional shredding/disposal service; the records are in electronic format, they shall be subject to secure electronic deletion. A record of documents disposal shall be retained.

6. ERASURE

Under the GDPR, the Data Subjects have the right to request their personal data to be eliminated and, hence, for them to "be forgotten", in some instances. The SQFT recognizes that this is not an absolute right and the request to do so can only be met if one of the following is true:

- Personal data is no longer needed for the purposes for which it was originally collected or processed
- The data subject withdraws their consent to the processing
- The data subject objects to the processing and there is no overriding legitimate interest for continuing it
- Personal data was unlawfully processed
- Personal data must be erased to comply with a legal obligation
- Personal data is processed in relation to the offer of information society services to a child.

Where one such request that meets the conditions described above is received, the Company shall first confirm that no legal obligations or legitimate Interest applies. After ensuring this and confirming the data subject has the right to have their data erased, the process is then carried out by the (person responsible e.g., DPO) in association with any department manager and IT team needed in order to guarantee that all data related to that data subject is securely erased.

7. ACCOUNTABILITY, COMPLIANCE AND MONITORING

The SQFT committed to safeguard the continued compliance with this policy and any associated legislation and carry out regular audits and monitoring of the records, but also their management, storage, archiving and retention.

Observance of the Policy is mandatory, and non-compliance could lead to internal disciplinary.

8. VALIDITY AND DOCUMENT MANAGEMENT

This document is valid as of (date of validity e.g. 25M of May of 2018) and is saved in (folder where the document is). The owner of this document is the (person responsible e.g., Data Protection Officer) who must review and, if necessary, update the document at least (frequency of update e g. once a year)

9. APPENDIX – RETENTION SCHEDULE

Record ID	Record Type	Retention Period and Notes	Actions at the end of record's life	Information Asset Owner
1234	Working Time Records	Date of record + 2 years	Secure Disposal: Shredded	Head of HR
5678	Board Policies	Permanent	---	CFO