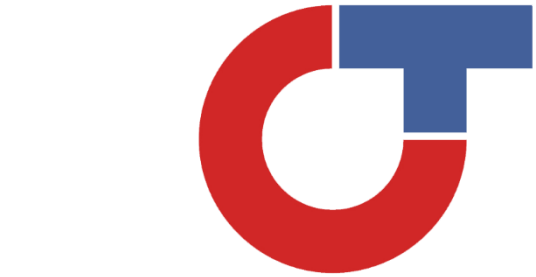

COMPLY TODAY

Records Retention and Protection Policy

Issued 2019

GUIDELINES
Purpose of this document This document sets out how organisational records should be protected and their retention rules.
Areas of the GDPR addressed The following articles of the GDPR are addressed by this document: Chapter II – Principles
Review Frequency It will be reviewed at least on annual basis and upon significant change to the organization and relevant legislation.

Contents

List of Tables

1 Introduction

In its everyday business operations **COMPLY TODAY** collects and stores records of many types and in a variety of different formats. The relative importance and sensitivity of these records also varies and is subject to the organisation's security classification scheme.

It is important that these records are protected from loss, destruction, falsification, unauthorised access and unauthorised release and a range of controls are used to ensure this, including backups, access control and encryption.

COMPLY TODAY also has a responsibility to ensure that it complies with all relevant legal, regulatory and contractual requirements in the collection, storage, retrieval and destruction of records. Of relevance is the European Union General Data Protection Regulation (GDPR) and its requirements concerning the storage and processing of personal data.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to **COMPLY TODAY** systems and records.

2 Records Retention and Protection Policy

This policy begins by establishing the main principles that must be adopted when considering record retention and protection. It then sets out the types of records held by **COMPLY TODAY** and their general requirements before discussing record protection, destruction and management.

2.1 General Principles

There are several key general principles that must be adopted when considering record retention and protection policy. These are:

- Records must be held in compliance with all applicable legal, regulatory and contractual requirements
- Records must not be held for any longer than required
- The protection of records in terms of their confidentiality, integrity and availability must be in accordance with their security classification
- Records must remain retrievable in line with business requirements always
- Where appropriate, records containing personal data must be subject as soon as possible to techniques that prevent the identification of a living individual

2.2 Record Types and Guidelines

In order to assist with the definition of guidelines for record retention and protection, records held by **COMPLY TODAY** are grouped into the categories listed in the table on the following page. For each of these categories, the required or recommended retention period and allowable storage media are also given, together with a reason for the recommendation or requirement.

Note that these are guidelines only and there may be specific circumstances where records need to be kept for a longer or shorter period. This should be decided on a case by case basis as part of the design of the information security elements of new or significantly changed processes, services and legislation.

Record Category	Description	Retention Period	Reason for Retention Period	Allowable Storage Media
Internal Accounting	Invoices, purchase orders, accounts and other historical financial records	According to the local legislation	Governmental compliance requirement	Electronic and hard copy – paper records must be scanned
Budgeting and Forecasting	Forward-looking financial estimates and plans	1 year	Local and EU directives	Electronic/Paper
System Transaction Logs	Database journals and other logs used for database recovery	5 years	Based on backup and recovery strategy	Electronic/tape media
Audit Logs	Security logs - records of logon/logoff and permission changes	5 years	Maximum period of delay before forensic investigation	Electronic
Operational Procedures	Records associated with the completion of operational procedures	5 years	Maximum period of time elapsed regarding dispute	Electronic/Paper
Customer	Personal data, including customer names, addresses, order history, credit card and bank details	2 years after last business transaction	Data protection requirement	Electronic
Supplier	Supplier names, addresses, company details	2 years after end of cooperation	Maximum period within which dispute might occur	Electronic/Paper
Human resources	Employee names, addresses, bank details, tax codes, employment history	Wage information 3y Working hours & related information 3y Collective redundancy information 3y Parental leave records 8 Carer's leave 3 Employment permit records 5 years or period equal to duration of employment (whichever is longer) Accident records 10	Data protection requirement; Employment law	Electronic/Paper
Contractual	Legal contracts, terms and conditions, leases	2 years after contract ends	Maximum period within which dispute might occur	Electronic/Paper
Customers' cooperatives	Data and records as revealed within invoices, agreements, bank details, addresses			

Table 1 - Record types and retention periods

2.3 Use of Cryptography

Where appropriate and deemed necessary to the classification of information and the storage medium, cryptographic techniques will be used to ensure the confidentiality and integrity of records.

Care is being taken to ensure that encryption keys used to encrypt records are securely stored for the life of the relevant records and comply with the organisation's policy on cryptography.

2.4 Media Selection

The choice of long term storage media must consider the physical characteristics of the medium and the length of time it will be in use.

Where records are legally (or practically) required to be stored on paper, adequate precautions must be taken to ensure that environmental conditions remain suitable for the type of paper used. Where possible, backup copies of such records should be taken by methods such as scanning. Regular checks must be made to assess the rate of deterioration of the paper and action taken to preserve the records if required.

For records stored on electronic media, similar precautions must be taken to ensure the longevity of the materials, including correct storage and copying onto more robust media if necessary. The ability to read the contents of the media must be maintained by the keeping of a device capable of processing it. If this is impractical an external third party may be employed to convert the media onto an alternative format.

2.5 Record Retrieval

There is little point in retaining records if they are not able to be accessed in line with business or legal requirements. The choice and maintenance of record storage facilities must ensure that records can be retrieved in a usable format within an acceptable period. **COMPLY TODAY** maintains an appropriate balance considering the cost of storage and the speed of retrieval so that the most likely circumstances are adequately catered for.

2.6 Record Destruction

Once records have reached the end of their life according to the defined policy, they must be securely destroyed in a manner that ensures that they can no longer be used. The destruction procedure allows for the correct recording of the details of disposal which should be retained as evidence.

2.7 Record Review

The retention and storage of records is subject to a regular review process carried out under the guidance of management to ensure that:

- The policy on records retention and protection remains valid
- Records are being retained according to the policy
- Records are being securely disposed of when no longer required
- Legal, regulatory and contractual requirements are being fulfilled
- Processes for record retrieval are meeting business requirements

The results of these reviews are properly recorded.