
# RECORDS RETENTION AND PROTECTION POLICY

# RHENUS WAREHOUSING SOLUTIONS LUTTERWORTH LTD RECORDS RETENTION AND PROTECTION POLICY

## Introduction

During the course of its standard business operations, Rhenus WS Lutterworth 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.

We also have 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 particular 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 our systems.

## General Principles

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 Rhenus Warehousing Solutions Lutterworth Limited (although this list is not exhaustive) and their general requirements before discussing record protection, destruction and management.

There are a number of 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 at all times
- Where appropriate, records containing personal data must be subject as soon as possible to techniques that prevent the identification of a natural individual

## Record Types and Guidelines

In order to assist with the definition of guidelines for record retention and protection, records held by Rhenus WS Lutterworth 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 of time. 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 and services. Similarly, there may be record types outside of this list which need to be stored and processed in accordance with lawful bases of processing. This document will be revised, where appropriate, to incorporate these record types as they become known.

| Record Category | Description | Retention Period | Reason for Retention Period | Allowable Storage Media |
|---|---|---|---|---|
| Accounting | Invoices, purchase orders, accounts and other historical financial records | 7 years | Legal compliance | Electronic/Paper |
| Customs Data | Commercial invoices, shipping documents, Customs declarations, C79 returns and other official documents | 7 years | Legal compliance | Electronic/Paper |
| Budgeting and Forecasting | Forward-looking financial estimates and plans | 10 years | Legitimate business interest | Electronic/Paper |
| System Transaction Logs | Database journals and other logs used for database recovery | 5 years | Business continuity | Electronic/Paper |
| Audit Logs | Security logs e.g. records of logon/logoff and permission changes | 5 years | Business continuity/investigations | Electronic |
| Customer | Personal data, including customer names, addresses, order history and bank details | 2 years after last purchase unless otherwise stipulated | Data required in the event of a dispute | Electronic/Paper |
| Supplier | Supplier names, addresses, company details | 2 years after end of supply | Data required in the event of a dispute | Electronic/Paper |
| Human Resources | Employee names, addresses, bank details, PAYE data, employment history, date of birth and other personal data | 3 years after end of employment | Data protection requirement; Employment law | Electronic/Paper |
| Other Contractual | Legal contracts, terms and conditions, leases | 2 years after contract end | Data required in the event of a dispute | Electronic/Paper |
| Operational Documents | Pick-sheets, despatch notes, labels and other documents used in operational activities | 6 weeks unless otherwise stipulated | Data required in the event of a dispute | Paper |

## Use of Cryptography

Where appropriate to the classification of information and the storage medium, cryptographic techniques such as tokenisation and encryption must be used to ensure the confidentiality and integrity of records.

Care must be 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 policies.

## Media Selection

The choice of long term storage media must take into account 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.

## Record Retrieval

The choice and maintenance of record storage facilities must ensure that records can be retrieved in a usable format within an acceptable period of time. An appropriate balance should be struck between the cost of storage and the speed of retrieval so that the most likely circumstances are adequately catered for.

## Record Destruction

Once records have reached the end of their life according to the defined policy, they must be securely destroyed. The destruction procedure must allow for the correct recording of the details of disposal which should be retained as evidence.

## Record Review

The retention and storage of records must be 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 must be recorded.