Records and protection policy

Document Ref	GDPR-DOC-04-1
Version	1
Dated	25 May 2018]
Document author	J.Herrington
Document owner	J.Herrington

Revision history

Version	Date	Revision author	Summary of changes

Distribution

Name	Title

Approval

Name	Position	Signature	Date

Mighton Products | Hinxton | Cambridgeshire | CB10 1RG | UK
+44 (0)1223 497097 | wwwmightonproducts.com | sales@mighton.co.uk

Contents

1 Introduction 4

2 Records retention and protection policy 5

2.1 General principles 5

2.2 Record types and guidelines 5

2.3 Use of cryptography 7

2.4 Media selection 7

2.5 Record retrieval 7

2.6 Record destruction 7

2.7 Record review 8

List of tables

Table 1 - Record types and retention periods 6

Mighton Products | Hinxton | Cambridgeshire | CB10 1RG | UK
+44 (0)1223 497097 | wwwmightonproducts.com | sales@mighton.co.uk

1 Introduction

In its everyday business operations Mighton Products Ltd 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.

Mighton Products 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 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 the Mighton systems.

The following documents are relevant to this policy:

- Data protection policy
- Data protection impact assessment process
- Privacy notice procedure
- Personal data analysis procedure

Mighton Products | Hinxton | Cambridgeshire | CB10 1RG | UK
+44 (0)1223 497097 | wwwmightonproducts.com | sales@mighton.co.uk

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 Mighton Products and their general requirements before discussing record protection, destruction and management.

2.1 General principles

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 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 Mighton Products 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.

Further information about records held by the organisation, including their security classifications and owners can be found in the Organisation-wide personal data inventory.

Mighton Products | Hinxton | Cambridgeshire | CB10 1RG | UK
+44 (0)1223 497097 | wwwmightonproducts.com | sales@mighton.co.uk

Record category	Description	Retention period	Reason for retention period	Allowable storage media
Accounting	Invoices, purchase orders, accounts and other historical financial records	six years	SOX compliance requirement	Electronic only – paper records must be scanned
Budgeting and forecasting	Forward-looking financial estimates and plans	one year	SOX compliance requirement	Electronic/Paper
System transaction logs	Database journals and other logs used for database recovery	six weeks	Based on backup and recovery strategy	Electronic/tape media
Audit logs	Security logs eg records of logon/logoff and permission changes	six months	Maximum period of delay before forensic investigation	Electronic
Operational procedures	Records associated with the completion of operational procedures	six years	Maximum period of time elapsed regarding dispute	Electronic/Paper
Customer	Personal data, including customer names, addresses, order history, credit card and bank details	six years after last purchase	Data protection requirement	Electronic/Paper
Supplier	Supplier names, addresses, company details	six years after end of supply	Maximum period within which dispute might occur	Electronic/Paper/Microfiche
Human resources	Employee names, addresses, bank details, tax codes, employment history	six years after end of employment	Data protection requirement; Employment law	Electronic/Paper
Contractual	Legal contracts, terms and conditions, leases	six years after contract end	Maximum period within which dispute might occur	Electronic/Paper
Further categories				

Table 1 | Record types and retention periods

Mighton Products | Hinxton | Cambridgeshire | CB10 1RG | UK
+44 (0)1223 497097 | wwwmightonproducts.com | sales@mighton.co.uk

2.3 Use of Cryptography

Where appropriate to the classification of information and the storage medium, cryptographic techniques 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 policy on cryptography.

2.4 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 or microfiching. 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 such as tape, 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 particular tape (or other similar media) format 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 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.

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 must allow for the correct recording of the details of disposal which should be retained as evidence.

Mighton Products | Hinxton | Cambridgeshire | CB10 1RG | UK
+44 (0)1223 497097 | wwwmightonproducts.com | sales@mighton.co.uk

2.7 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.

Mighton Products | Hinxton | Cambridgeshire | CB10 1RG | UK
+44 (0)1223 497097 | wwwmightonproducts.com | sales@mighton.co.uk