Polyco Healthline Data Retention Policy

Published Date: 15th March 2018

Review due: 15th March 2019

Introduction

The need to retain data varies widely with the type of data. Some data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists.

Since this can be somewhat subjective, a retention policy is important to ensure that the company's guidelines on retention are consistently applied throughout the organisation.

Scope

The scope of this policy covers all company data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location.

Note that the need to retain certain information can be mandated by local, industry regulations and will comply with EU General Data Protection Regulation GDPR and the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

Policy Elements

Reasons for Data Retention

We do not wish to simply adopt a "save everything" approach. That is not practical or cost effective and would place an excessive burden on company and IT Staff to manage the constantly-growing amount of data.

Some data, however, must be retained to protect our interests, preserve evidence, and generally conform to good business practices. Some reasons for data retention include:

- Litigation
- Accident investigation
- Security incident investigation
- Regulatory requirements
- Intellectual property preservation

Data Duplication

As data storage increases in size and decreases in cost, companies often err on the side of storing data in several places on the network. A common example of this is where a single file

may be stored on a local user's machine, on a central file server, and again on a backup system. When identifying and classifying the company's data, it is important to also understand where that data may be stored, particularly for duplicate copies, so that this policy may be applied to all duplicates of the information. For this reason, you should only duplicate data when there is an absolute valid business reason.

Retention Requirements

The following guidelines should be used to determine the storage period for different types of data:

- Personal customer data: Personal data will be held for as long as the individual is a customer of the company plus 6 years.
- Personal employee data: General employee data will be held for the duration of employment and then for 6 years after the last day of contractual employment. Employee contracts will be held for 6 years after last day of contractual employment.
- Tax payments will be held for six years.
- Records of leave will be held for three years.
- Recruitment details: Interview notes of unsuccessful applicants will be held for 1 year after interview. This personal data will then be destroyed.
- Planning data: 7 years.
- Health and Safety: 7 years for records of major accidents and dangerous occurrences.
- Public data: Public data will be retained for 3 years
- Operational data: Operational data will be retained for 5 years.
- Critical data including Tax and VAT: Critical data must be retained for 6 years
- Confidential data: Confidential data must be retained for 7 years.
- Customer data: Customer data will be retained for 5 years.

Retention of Encrypted Data

If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

Data Destruction

Data destruction is a critical component of a data retention policy. Data destruction ensures that we will use data efficiently, thereby making data management and data retrieval more efficient and cost effective. The method of destruction will vary, according to the media, but the following methods may be employed:

- Electronic files – full deletion (note – the Recycle Bin is not classed as deletion. You should also empty the Recycle Bin)
- Paper – secure shredding or burning
- USB storage – secure physical destruction
- Hard drive storage – secure physical destruction

When the retention timeframe expires, the responsible person must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her line manager so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of the company's senior management team.

We explicitly direct that you must not destroy data in violation of this policy. Destroying data that a user may feel is harmful to himself or herself is particularly forbidden or destroying data in an attempt to cover up a violation of law or company policy.

Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data retention guidelines will invoke disciplinary and possibly legal action.