Data Retention Policy

Contents

Distribution List

☐	CEO	☐	COO
☐	CFO	☐	Country Managers
☐	Internal Only	☐	Internal and External
☐	All Staff	☐	Board Members

1. Introduction

1.1 Information is one of *CompanyX's* key corporate assets; in the course of carrying out its various functions, *CompanyX* accumulates information from both individuals and external organisations. *CompanyX* also generates a wide range of data, which is recorded in documents and records. How we manage them is key from both a commercial and a legislative/ compliance perspective.

1.2 These documents and records are in several different formats, examples of which include, (but are not limited to) data such as names, emails, IP addresses; financial information; payroll for the purpose of processing employee contractual rights; legal documents such as contracts.

1.3 For the purposes of this Policy, the terms 'document' and 'records' include information in both hard copy and electronic form and refers to personal identifiable data within.

1.4 In certain circumstances it will be necessary to retain specific documents in order to fulfil statutory or regulatory requirements and also to meet operational needs. Document retention may also be useful to evidence events or agreements in the case of disputes, and also to preserve information which has historic value.

1.5 Premature destruction of documents could result in inability to defend litigious claims, operational difficulties and failure to comply with the GDPR.

1.6 Lengthy or indefinite retention of personal information could result in *CompanyX* breaching the GDPR.

1.7 It is important for the above reasons that *CompanyX* has in place systems for the timely and secure disposal of documents and records that are no longer required for business purposes and in accordance with the GDPR are kept up-to-date and relevant.

2. Aims and Objectives

2.1 The key objective of this Policy is to provide *CompanyX* with a simple framework which will govern decisions on whether a particular document should be retained or disposed of. In the case of documents which are to be retained by *CompanyX*, the Policy includes guidance on the format in which they should be retained and agreed retention periods.

2.2 Implementation of the Policy should ensure transparency when retrieving information, for the purposes of a subject access and reduce the amount of information that may be held unnecessarily.

2.3 The Policy clarifies the different roles of employees in relation to document retention and disposal in order that they understand their responsibilities, and who to refer to if they are unsure about any document and require clarification.

3. Scope

3.1 This Document Retention Policy applies to all information held by *CompanyX* and its external service providers where they are processing information on *CompanyX* behalf.

4. Policy Statement

4.1 *CompanyX* will ensure that information is not kept longer than is necessary and will retain the minimum amount of information that it requires to carry out its' statutory functions and the provision of services.

5. Retention and Disposal Policy

5.1 Decisions relating to the retention and disposal of documentation should be taken in accordance with this Policy, in particular:

Document Retention Schedules – Guidance on the recommended and statutory minimum retention periods for specific types of documents and records.

5.2 In circumstances where a retention period of a specific document has expired, a review should always be carried out prior to a decision being made to dispose of it. This review should not be particularly time consuming and should be straightforward. If the decision to dispose of a document is taken, then consideration should be given to the method of disposal to be used.

6. Roles and Responsibilities

6.1 Directors will be responsible for determining (in accordance with this Policy) whether to retain or dispose of specific documents within the remit of their service area.

6.2 Directors may delegate the operational aspect of this function within the organisation.

6.3 Directors should seek advice from the CEO if they are uncertain as to whether minimum retention periods are prescribed by law, or whether the retention of a document is necessary to protect *CompanyX* position where a potential claim has been identified, or for operational purposes.

7. Safeguarding of Data during Retention Period

The possibility that data media used for archiving will wear out shall be considered. If electronic storage media are chosen, any procedures and systems ensuring that the information can be accessed during the retention period (both with respect to the information carrier and the readability of formats) shall also be stored in order to safeguard the information against loss as a result of future technological changes. The responsibility for the storage falls to the Data Protection Officer.

8. Destruction of Data

CompanyX, its employees and external consultants should, on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant. See the Appendix for the retention schedule. Overall responsibility for the destruction of data falls to the Data Protection Officer.

Once the decision is made to dispose according to the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some expired or superseded contracts may only warrant in-house shredding. The Document Disposal Schedule section below defines the mode of disposal.

In this context, the employee shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the Data Protection Officer subcontracts for this purpose. Any applicable general provisions under relevant data protection laws and the Company's Personal Data Protection Policy shall be complied with.

Appropriate controls shall be in place that prevents the permanent loss of essential information of the company as a result of malicious or unintentional destruction of information – these controls are described in the company's IT Security Policy.

The Data Protection Officer shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

9. Disposal

9.1 Confidential waste which is located around the *CompanyX* offices should be disposed of using the shredder.

9.2 Disposal of documents other than those containing confidential or personal data may be disposed of by binning, recycling, and deletion (in the case of electronic documents).

9.3 Records of disposal should be maintained by each department and should detail the batch of documents disposed of, the date, and the Director who authorised the document's disposal.

Appendix A: Disposal and Retention Considerations

Each of the following questions and guidance underneath them should be considered prior to the disposal of any document.

1. Has the document been appraised?

    Check that the nature and contents of the document is suitable for disposal.

2. Is retention required to fulfil statutory obligations or other regulatory obligations?

    Specific legislation setting out mandatory retention periods for documentation held by CompanyX is very limited, but includes the following:

        Tax legislation – minimum retention periods for certain financial information are stipulated by the VAT Act 1994 and the Taxes Management Act 1970.

        HMRC legislation – minimum retention periods for employee processing payroll

3. Is retention required for evidence?

    Keep any documents which may be required for legal proceedings until the threat of proceedings has passed.

4. Is retention required to meet the operational needs of the service?

    Consider whether the document in question may be useful for future reference, as a precedent or for performance

Appendix B: Document Retention Schedules

1. Introduction
The following schedules provide guidance on the retention periods applicable to a wide range of CompanyX documents.

Human Resources

Data Type	Retention Period	Notes or Comments
Personnel Files	7 Years after staff member final date of employment	
Files related to any staff disciplinaries	7 Years after staff member final date of employment	
Recruitment	7 Years After Last Recruitment Activity	
Holiday and Sickness Records	7 Years after staff member final date of employment	
Passports, Visa's, Right to Work	7 Years after staff member final date of employment	
Photographs	7 Years after staff member final date of employment	
Bank Details	Until final day of departure/ final salary payment	

Finance

Data Type	Retention Period	Notes or Comments
Internal Audit	7 Years	
Payroll	7 Years	
Management Accounts	7 Years	
Employee Expenses	7 Years	
Company Bank Details	7 Years	
Tax	7 Years	

Business Records

Data Type	Retention Period	Notes or Comments
Articles of Incorporation	Permanently	
Board Policies	Permanently	
Board Meeting Minutes	Permanently	
Tax and Employee Identification Designations	Permanently	
Annual Corporate Filings	Permanently	

Customer Data

Data Type	**Retention Period**	**Notes or Comments**
Platform data – inclusive of Video data, comments, attachments, profile picture, email address, first and second name	Retained whilst organisation remains a customer or deleted by user. Once an organisation requests all records to be deleted, data will be removed from the back-ups within 9 months	
Live chat history	Until no longer needed or requested to be deleted	
Screen recordings from support session	Deleted after 90 days	
CRM data – inclusive of Name, Email address, mobile number, address, emails and phone call summaries	Until no longer needed or requested to be deleted	
Metrics Data	Retained whilst organisation remains a customer or deleted by user. Once an organisation requests all records to be deleted, data will be anonymised	

Non-Customer Data

Data Type	**Retention Period**	**Notes or Comments**
Name, Mmail address	Kept until person unsubscribes / requests to be removed from system	
Call recordings	Deleted after 6 months	