DATA RETENTION AND ERASURE POLICY

# Data retention and erasure policy guidance

## How should I use my data retention and erasure policy?

Your company’s data retention and erasure policy is designed to provide your company with a defined data retention schedule. You should fill in the template using your company’s particulars and store this document with your other GDPR documents, for safekeeping.

## Will I need to update my data retention and erasure policy?

Yes. It is a crucial aspect of your company’s GDPR compliance to ensure that you have a clearly defined policy in place, dictating data retention and erasure. You should review this policy at least every 6 months and amend as necessary to ensure your company remains GDPR compliant.

# Data retention and erasure policy introduction

## Our approach towards data retention

This policy is designed to ensure [COMPANY NAME] does everything within its power to adequately protect, maintain and store data. This policy has also been developed to ensure that any data, documents or records that have no further use or value to [COMPANY NAME] are disposed of in line with our regulatory obligations and relevant company policy.

Employees should consult our data retention and erasure policy, to develop an understanding of our company’s obligations relating to the ways in which we retain data or electronic documents. These documents may include, but are not limited to:

* Emails
* Word Documents
* Spreadsheets
* PDF documents
* Web files
* Sound files
* Videos

Personal data must never be kept for longer than it is needed. Consequently, employees should utilise our company’s data retention schedule as a guide to understanding [COMPANY NAME]’s general retention period time for various data categories that have been assigned based upon the purpose of the data. In line with our regulatory obligations, all data that is no longer necessary should be deleted and all copies must be destroyed in line with our data erasure schedule.

## Data retention schedule administration

This data retention schedule documents the maintenance, retention and disposal guidelines relating to any and all records our company holds. It must be reviewed and accordingly amended on a regular basis to ensure data storage and erasure processes are adhering to [COMPANY NAME]’s wider data retention policy approach.

There will be times when data may need to be retained longer than the pre-defined amount of time permitted. Circumstances in which our policy will need to be suspended may include, but are not limited to:

* Legal proceedings
* Regulatory investigations
* If criminal activity is suspected or alleged
* If relevant data concerns a company or organisation in receivership or liquidation
* If the relevant data is of historical importance to the owner or controller

In the event of legal proceedings, criminal activity or investigations, [COMPANY NAME] and its employees must retain data that relates to the situation and could serve to aid the company’s case or position, liability or amount involved. If such a situation may occur during the lifetime of this policy, [COMPANY NAME] will inform all staff of the policy’s suspension as it relates to said situation.

# Data retention schedule

[COMPANY NAME] has developed its data retention policy in line with the following data retention schedule:

|  |  |
| --- | --- |
| **Department** | **Function** |
| 1 | Accounting and finance data |
| 2 | Contract data |
| 3 | Corporate records |
| 4 | Correspondence and internal memoranda |
| 5 | Personal data |
| 6 | Electronic data |
| 7 | Insurance data |
| 8 | Legal data |
| 9 | Miscellaneous data |
| 10 | Personnel records and data |
| 11 | Tax records and data |

# 1. Accounting and finance data

|  |  |
| --- | --- |
| **Record** | **Retention period** |
| Company financial statements and annual audit reports | Permanent |
| Annual audit records (including relevant documents) | 7 years after audit completion |
| Company bank statements | 7 years |
| Cancelled cheques | 7 years |
| Employee expense reports | 7 years |
| Interim company financial statements | 7 years |
| Credit card records | 2 years |
| Annual plans and company budgets | 2 years |

Any and all items that display customer bank details or credit card information must be kept under secure conditions when not in immediate use. This includes keeping printed records in a locked desk drawer or filing cabinet.

If [COMPANY NAME] determines it is necessary to keep a document that displays customer financial details beyond a retention period of 2 years, all identifying details or financial information as it relates to any customer must be redacted or removed from the document in question.

# 2. Contract data

|  |  |
| --- | --- |
| **Record** | **Retention period** |
| All company contracts | 7 years after expiration or termination |
| All correspondence relating to contracts | 7 years after expiration or termination |

# 3. Corporate records

|  |  |
| --- | --- |
| **Record** | **Retention period** |
| Corporate records | Permanent |
| Licenses and permits | Permanent |

For the purpose of this schedule and corresponding policy, ‘corporate records’ should be defined to include anything relating to:

* Meeting minutes
* Signed minutes of the board
* Signed minutes of any committees
* Record of incorporation
* Articles of incorporation
* Annual corporate reports

# 4. Correspondence and internal memoranda

The vast majority of correspondence and internal memoranda must be retained to match the period of time as the document or data to which they relate. Examples may include an email relating to a contract – in which case the email in question would be expected to be retained for a period of 7 years after the expiration of the corresponding contract.

Bearing this in mind, [COMPANY NAME] recommends that all correspondence and internal memoranda as it relates to a company project be kept with said project as part of a project-wide file.

Company correspondence or internal memoranda unrelated to documents that have a defined retention period, should be securely destroyed at an earlier time depending upon which of the following two categories it corresponds:

## Category 1

Category 1 correspondence or internal memoranda includes any and all data as it relates to routine processes. Category 1 correspondence and internal memoranda generally do not carry any significant consequences and should be disposed of with 2 years.

Examples of category 1 correspondence and internal memoranda may include (but are not limited to):

* Notes of appreciation or thanks
* Plans for meetings
* Forms or letters that do not require a follow up
* General enquiries that have been settled
* Chronological correspondence data
* Complaints requesting a specific action that have already been addressed and carry no further value
* Correspondence relating to inconsequential subject matter

All copies of internal office correspondence should be read and destroyed as per this policy unless that correspondence includes data or content that must be retained as part of a wider project.

## Category 2

Category 2 correspondence or internal memoranda includes non-routine information or correspondence that is likely to have a consequential impact upon the company or its employees. Category 2 correspondence and internal memoranda should be retained on a permanent basis.

# 5. Personal data

There will be times when [COMPANY NAME] and its employees must retain and/or delete personal data in line with its legal obligations.

For the purposes of this data retention and erasure policy, ‘personal data’ can be defined as any identifying information as it relates to an individual. We never keep personal data for longer than is necessary for the purpose in which that data was collected. All personal data as defined within the following categories should be deleted based upon this retention and erasure schedule:

|  |  |
| --- | --- |
| **Record** | **Retention period** |
| Data relating to customer devices | 2 years after the account is closed |
| Data relating to use of our company website | 2 years after the account is closed |
| Any data collected when registering with our website | 2 years after the account is closed |
| Data collected and submitted as part of any profile creation processes | 2 years after the account is closed |
| Data submitted for the purpose of subscribing to email marketing activities | Indefinitely (or until customer unsubscribes) |
| Data submitted as part of online service delivery | Indefinitely |
| Data relating to any subscriptions | 2 years after the account is closed |
| Data posted in a public area on our company website | 2 years after the post |
| Data contained in communications sent through the website | 2 years after contact |
| Any other personal data | 2 years after contact |

[COMPANY NAME] reserves the right to retain any and all documents (both electronic and print) containing personal data to the extent our company is required by law to do. We will also retain documents containing personal data if we have reason to believe said documents could be relevant to legal proceedings, or to establish and/or exercise our own legal rights.

Our company will organise backups of our database and all of the electronic data held within our company server(s). Backup activities should include all data that relates to current users or customers, alongside any document or dataset relating to one of the aforementioned reasons as outlined within this data retention and erasure policy. [COMPANY NAME] does this to ensure that lost information can be retrieved within one year, as and where needed.

# 6. Electronic data

## Emails

Most emails do not need to be kept. Emails that are inconsequential or unrelated to contracts or projects should subsequently be treated in line with the following policies:

* All emails should be deleted after 12 months. This includes both internal and external emails
* [COMPANY NAME] will archive emails for six months after employees have deleted them. After this six-month period, archived emails will be destroyed
* Employees should never send emails containing confidential or proprietary data to external sources unless it has been approved by a relevant manager

## Electronic documents

Electronic documents include, among other formats, both PDF document and files originating from Microsoft Office Suite or similar software.

Retention and erasure will depend upon the purpose of the electronic document, yet as a general rule of thumb employees can apply the following rules:

For PDF documents, the maximum period of retention should be 6 years. PDF documents that employees deem vital to their performance or role should be printed and/or stored in the relevant employee’s workspace.

For text documents or other formatted files, the maximum period of retention should be 5 years. Text documents or other formatted files that employees deem vital to their performance or role should be printed and/or stored in the relevant employee’s workspace.

[COMPANY NAME] does not and will not automatically delete electronic documents or corresponding data beyond the time periods defined within this policy. It is the responsibility of our employees to ensure they are adhering to our policy guidelines.

# 7. Insurance data

|  |  |
| --- | --- |
| **Record** | **Retention period** |
| Certificates | Permanent |
| Claims files | Permanent |
| Current insurance policies | Permanent |
| Expired insurance policies | Permanent |

# 8. Legal data

|  |  |
| --- | --- |
| **Record** | **Retention period** |
| Legal memoranda and legal opinions | 7 years after resolution |
| Litigation data | 1 year after expiration of appeals or time for filing appeals |
| Court orders | Permanent |
| Requests for a departure from [COMPANY NAME] retention and erasure schedule | 10 years |
| Register of members | Permanent |
| Director’s meetings minutes | 10 years |

# 9. Miscellaneous data

|  |  |
| --- | --- |
| **Record** | **Retention period** |
| Reports from consultants | 2 years |
| Documents containing content of historical value | Permanent |
| Original policy and procedures manuals | Current version with revision history |
| Copies of policy and procedures manuals | Retain current version only |
| Annual company reports | Permanent |
| Records of personal identification | 5 years |
| Any work-related reportable accident, injury or death | 3 years from incident |
| Immigration checks | 2 years from termination of job |

# 10. Personnel data

|  |  |
| --- | --- |
| **Record Type** | **Retention Period** |
| Job applications and/or related interview data concerning unsuccessful candidates | 6 months |
| Employee personnel records | 6 years after end of contract |
| Employment contracts | 7 years after end of contract |
| Employment records correspondence with employment agencies | 3 years from date of hiring |
| Job descriptions | 3 years after superseded |
| Working time opt-out documentation | 2 years |
| Financial details of employees | As long as necessary |

# 11. Tax data

[COMPANY NAME] keeps accounts and/or records to demonstrate and establish amounts of gross income, deductions, credits and other information. These records are crucial to maintaining our company’s compliance of tax laws.

Associated records and documentation will include (but are not limited to) the following records and associated schedules:

|  |  |
| --- | --- |
| **Record** | **Retention period** |
| Tax-exemption documentation | Permanent |
| Tax bills | 7 years |
| Tax returns | Permanent |
| Tax receipts | Permanent |
| Tax statements | Permanent |
| Sales and/or use of tax records | 7 years |
| Annual returns | Permanent |
| Payroll/wage records for unincorporated businesses | 5 years after 31 Jan following the year of assessment |
| PAYE records | 3 years from the end of the tax year to which they relate |
| Maternity records | 3 years after the end of the tax year in which the maternity pay period ends |