**Data Retention Policy**

Prepared by Mark Gracey
September 2022

**Overview**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version Name** | **Date Amended** | **Summary of Changes** | **Status** | **Name** |
| Version 1 | 02/09/2022 | Creation of new policy | Final | Mark Gracey  |
|  |  |  |  |  |
|  |  |  |  |  |

# Contents

[1. Introduction 3](#_Toc119918624)

[2. Roles and responsibilities 3](#_Toc119918625)

[2.1. Senior Management Team 3](#_Toc119918626)

[2.2. Data Protection Officer 3](#_Toc119918627)

[2.3. Employee responsibilities 3](#_Toc119918628)

[3. What data retention means in practice 3](#_Toc119918629)

[4. Retention schedule 4](#_Toc119918630)

[5. After the retention period has expired 6](#_Toc119918631)

[6. General approach to retention 6](#_Toc119918632)

[7. Policy review 7](#_Toc119918633)

# Introduction

This document provides advice and guidance to ensure we meet the data protection requirements set out in the General Data Protection Regulation (“GDPR”), the UK’s implementation of aspects of the Regulation into UK law and any guidance the Information Commissioner’s Office provide.

Data protection applies to “personal data” which is any data that identifies an individual, so that includes data relating to our customers, employees, contacts, suppliers, and data supplied by our clients, etc.

Article 5 of the GDPR sets out the “Principles relating to processing of personal data” which includes Article 5(1)(e), which states that data must be “*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed* “.

It is therefore unlawful to retain data any longer than is necessary. So, if there is no lawful reason to retain the data, it must be deleted.

We take data protection seriously and place a high importance on the correct and lawful processing of all personal data as well as respecting the rights and privacy of our customers and employees. As such, this policy sets out the company procedures that are to be followed, by all employees when dealing with the retention of personal data across the business.

# Roles and responsibilities

## Senior Management Team

Ultimately the senior management team are responsible for ensuring appropriate data protection and privacy controls are in place. Should the Data Protection Officer be unavailable, your line manager should be contacted for escalation to the Senior Management Team.

## Data Protection Officer

The Data Protection Officer is responsible for ensuring this policy is upheld across the business.

Our Data Protection Officer is:

t: 01628950960

e: luke.donnebaum@radcliffe-group.com

## Employee responsibilities

All employees will familiarise themselves with this policy and any associated policies, relating to the processing of personal data and ensure their processing of personal data is within the rules set out within this and all our data protection policy documents.

# What data retention means in practice

To comply with the law, we must consider whether we are retaining data longer than we should be. This means we must:

* Understand what circumstances it is lawful for us to continue to process data, even when we do not actually need it ourselves (e.g. because a law requires us to keep data) and identify specifically how long we should be retaining it
* Put in place a process to review and act upon any data that is no longer needed and should be deleted (covered in this policy)
* Identify data that we no longer need and securely delete it
* Maintain an ongoing process for routinely deleting data that is no longer needed

Generally, it would be considered lawful to continue to process data (and therefore retain it) when:

* Consent has been given, authorising the continued retention and processing of the data
* The data is required to continue to provide the service to a client, or in the case of an employee, to continue employment
* A legal or regulatory obligation (e.g. employment or tax law) requires us to keep the data for a specific time (even when we no longer need it)

# Retention schedule

|  |  |
| --- | --- |
| **Type of Data** | **How Long We Keep It** |
| **Employee Data** |
| Employee data (in the UK) (including training records and contracts) | During employment and up to 6 years after someone has left (unless insurance policies say otherwise or if there is risk from an industrial injury claim) |
| Working time records | 2 years |
| Payroll records | 6 years from the end of the financial year |
| Maternity pay, sick pay, national minimal wage records | 3 years from the end of the financial year |
| Unsuccessful job applicants. | 6 months after rejecting the application unless consent is received to retain for future opportunities |
| CV and contact details for unsuccessful candidate that we might want to use in the future | 6 months after receiving consent from the candidate that they are happy for us to keep the data for this purpose |
| Immigration checks | 2 years from the termination of employment |
| Vetting information | 6 months |
| Disclosure & Barring service checks | Unless there is justification to keep the information, it should be deleted, and we should simply record whether the outcome of the check was successful/unsuccessful. If we can justify keeping the records, then we must not keep them any longer than 6 months after the check |
| Pension related data | Generally, 6 years although opt-out information must only be kept for 4 years |
| **Business Data** |
| Business financial records | The current year, plus 6 years |
| Contracts with suppliers, etc. | 6 years after termination of the agreement |
| Banking records | 6 years from the transaction date |
| Employer liability insurance | 40 years |
| Insurance policies, documentation and claims data | 3 years from expiry (or after a claim has been settled) |
| Health and safety records (including accident books and reports) | 3 years after the last entry or end of an investigation |
| **Client Data** |
| Data supplied to us by our customers for the purposes of delivering a service (i.e. where we act as the processor of the data) | As set out in any agreement (e.g. our Data Processing Agreement or other contract or terms of service) with the client (usually delete or return at end of service) |
| Data relating to clients | Current client data can be kept for as long as the client remains a client. Past client data will need to be kept where it relates to information relevant for tax purposes, etc. |

# After the retention period has expired

Once the retention period has expired and we no longer need to keep the data, we have two options:

**1. Anonymise the data**

If we wish to continue to keep the data, perhaps for statistical, research or other analysis then it would be lawful for us to do so, if we anonymise the data. Anonymisation means removing any aspect of the data that identifies an individual such as their name and address.

When we consider anonymising data we must be mindful that depending on the data, removal of just identifying information (e.g. name, email address, etc.) may not be enough. So, when anonymising data we must consider whether an individual can still be identified from the remaining data (e.g. because of retention of a postcode, or a particular medical condition, or other attribute that could enable us to identify the individual the data relates to, etc.). We should also be careful if the data is stored or processed along with other data which may be used in cross-referencing the apparent anonymised data.

**2. Destroy the data**

If we no longer need the data (in anonymised form or otherwise) then we must securely destroy the data. This means that for paper records we must make sure the data is shredded (cross-cut or micro-cut) or we use an approved confidential shredding service.

Electronic records should be deleted from all sources using the delete function available in the application where the data is stored. We should also make sure that our backups will, over time (because of a suitable rolling back up process) be replaced – there is no requirement for us to delete the data from backups, provided we can demonstrate we have a procedure in place to ensure that if we were to recover from a backup, the deleted data is not restored.

Where we use a third-party service for retaining records we should be mindful of that services own policy regarding the retention of data which may extend past our own retention periods (i.e. they may keep your data longer in case we need to recover your data). In such cases, we should ensure that where possible we manually purge these deleted files following the services documented procedure.

# General approach to retention

* We only collect data that we need for the purposes of running our organisation.
* We only keep that data for as long as we have a lawful business reason for doing so.
* We anonymise any data that we no longer lawfully need to retain, but wish to process for analysis purposes.
* Where we have no future need for the data (analysis or otherwise) we securely destroy the data and we have processes (automated or manual) in place to destroy or anonymise data once is it no longer needed.
* We have checked the third-party services we use to store data to ensure that when we delete that data from their service it is not retained; where it is retained we follow their instructions to purge the data from the service.

# Policy review

This document is the responsibility of, and will be reviewed annually, by the Data Protection Officer to ensure it is still relevant and up to date with any changes in the law, guidance or precedents set.