Getting Started with
Data Retention & Destruction

Knowing what data to keep and what data to destroy can be daunting for any business. But it doesn't have to be. This guide covers the basics of data retention and destruction and we hope it will give you the confidence to make informed decisions about retaining and destroying your data.

Why is a well-managed data retention schedule so important?

Handling data responsibly is a legal requirement for all data processors, so getting this right is vital. But, with many legal requirements to meet, it can be stressful for employees. Reassure your workers that correct data retention and destruction is something positive for your business, not something to be afraid of.

Getting your employees up to speed with data retention will:

- Help to keep your customers' and employees' personal information safe
- Minimise the risk of data breaches and fines
- Help to keep your business GDPR compliant
- Enable you to create helpful policies and give your business proof of compliance.

Getting started with a data retention policy.

To get started with a data retention policy, we must understand what is meant by personal data. The Data Protection Act (2018) defines personal data as "any information relating to an identified or identifiable living individual".

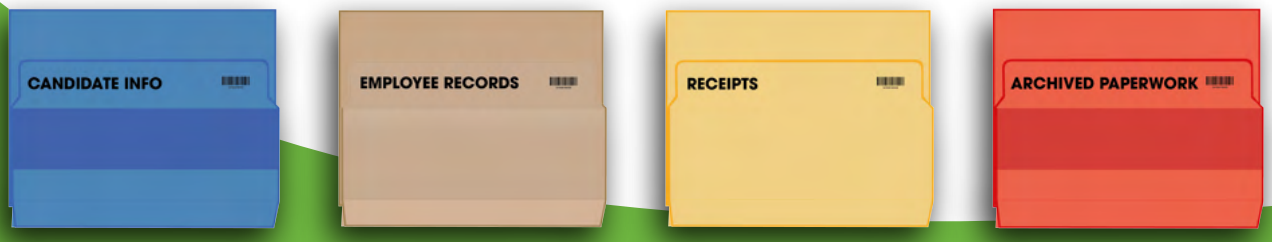
But what does this mean?

In short, it means any living person who can be identified, either directly or indirectly, through:

- Identifiers such as names, ID numbers, location data and online identifiers
- Factors such as their physical, physiological, genetic, economic, cultural or social identity.

Some examples of personal data that most organisations keep include:

- Employee addresses and emergency contact details
- Letters and general correspondence where the recipient's full name is printed
- Equal opportunities monitoring data, e.g. a person's race, religion, medical information or sexual orientation.



Getting Started with Data Retention & Destruction

Getting started with a data retention policy.

Now you're familiar with different kinds of personal data, you must identify what types of personal data your organisation collects and uses. From there, you must determine how long you reasonably need to keep this information.

General Data Protection Regulations (GDPR).

General Data Protection Regulations do not dictate specific lengths of time that businesses should keep personal data. Instead, it's up to organisations to justify how long data is retained, based on the purposes of processing that data. GDPR does, however, state that data should not be held for any longer than necessary. You should not hold onto data indefinitely without review, or hold it longer than is reasonable "just in case" you need it.

Retention needs will vary from business to businesses, but organisations should always consider how long to store data that includes personally identifiable information. If individuals do not need to be identified, data should be anonymised to prevent identification and reduce the risk of personal data being breached. If data is no longer needed, it should be securely destroyed.

Data Retention To Do List:

1) Identify what data your business processes

2) Decide how long you need to keep data before deletion and destruction

3) Create a data retention policy and a data destruction schedule.

Getting Started with
Your Data Retention Policy

The GDPR storage limitation principle is quite flexible and recognises that data retention needs vary from business to business. Your organisation's data retention needs will likely not mirror another organisation's exactly. Because of this, it's a good idea to implement a data retention policy specific to your business.

To get started, you need to identify what data your business processes. You must then decide how long you can reasonably, and legally, keep this data before it needs to be destroyed.

Below, we've set out two examples of data to get your started with your data retention policy. Please note, your business needs may differ from the examples below.

Examples of personal data to get you started.

Example One - Collecting names and contact details of people booking to eat at your restaurant.

Your restaurant may collect names and contact details of people booking a table. Unless you've gained proven consent to use this data for other purposes, this information should not be held longer than necessary or processed for any purposes other than confirming the booking.

There are few reasons you should hold on to personal booking data after the date has passed. However, you may need to keep general booking data for things like footfall and cover analysis. In this case, data should be anonymised. Most secure restaurant booking software applications will have a function to do this automatically. If you prefer the old-school method of writing bookings in a diary, diaries should be destroyed once no longer needed and should be kept secure away from unauthorised access. Personal details should also be redacted where possible.

Example Two - A customer had a negative experience with a product they purchased from your store. They submit a letter of complaint to your head office.

Customer feedback is highly valuable for improving products and services. However, once any complaints are resolved, there may not be a need for you to retain their personal data in your record of the complaint.

If you wish to look back on this feedback later on to improve services, you should anonymise the complaint to remove all personal and identifiable information.

We recommend seeking expert advice for information on statutory retention periods. This is the information you legally must keep for a certain amount of time, such as HMRC data. You can find some useful resources for advice on statutory retention periods and recommended retention periods on the final page of this document.

Getting Started with
Your Data Retention Policy

As well as personal data, there are many other forms of data that businesses should securely destroy, for example, financial paperwork that is no longer needed, old incident reports, visitor logs, expired cheque books and more.

Retention periods for other documents.

Retention periods for other documents vary according to government legislature.

For example, the default standard retention period for HMRC records is 6 years + 1 or 6 years plus the current accounting year. HMRC records should only be retained beyond this default retention period if justifiable for statutory, legal, regulatory or other security purposes, or for their historic value.

With HR information, there are also legal retention periods. For example, payroll data and salary records should be kept for 6 years from the end of the tax year to which they relate.

The same goes for health and safety information. As an example, accident report books should be kept for three years from the data of the last entry, or, if the incident involves a young person, until that person reaches 21 years of age.

There are some useful resources outlining these statutory retention periods on the following page.

Communicating your data retention policy

All personnel in your organisation should be aware of their own responsibilities when it comes to protecting personal information and following their department's data retention and destruction timescales. Once you have written your data retention and destruction policy and sought legal advice, you should communicate this policy to all members of your organisation, making sure a copy is readily available to anyone who needs it.

Useful Resources & Information
Data Retention & Destruction

Please see our list of useful resources where you can find information regarding the most up-to-date regulations for retaining, storing and destroying materials containing personal information.

Useful Resources.

HM Revenue & Custom's policy paper on Records Management and Retention and Disposal Policy:
https://bit.ly/ShredStation-HMRC1

The UK Government's Statutory Instrument: The Data Retention and Acquisition Regulations 2018:
https://bit.ly/ShredStation-UK1

The Information Commissioner's Office's templates for document data processing activities:
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/documentation/how-do-we-document-our-processing-activities/

The Information Commissioner's Office's Guide to the General Data Protection Regulations:
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

The CIPD's summary of UK legislation regarding statutory retention periods for HR records: https://bit.ly/ShredStation-CIPD1

The Health and Safety Executives guidance on record keeping, health surveillance and more:
https://bit.ly/ShredStation-HSE

PLEASE NOTE: Policy and Data Retention Regulations are subject to constant change and may differ between industries. The contents of this guide are correct at the time of publication and Shred Station cannot take any responsibility for information that is hereafter incorrect. This contents of this guide should be used as guidance only. For any legal advice on general data protection law, we advise all companies to consult a solicitor.