CS Shredding
Est 2004

GDPR Data Destruction Steps 1-4

GDPR: Data retention and data destruction

Use this guide to data retention and destruction for your organisation…

September 2019 v1

Step 0

If you don't already have a Data Retention and Destruction Policy, create one. Even the most basic policy will assist you in your GDPR compliance. You should also designate a 'responsible person' to ensure compliance.

Step 1

The responsible person should check your organisation's policy for updates to types of data that is retained and updates of retention deadlines. Any updates of any type should be communicated with all staff, as data affects all areas of business.

Step 2

The responsible person should add the deadlines for regular review to their diary; diarising these deadlines will help remind you to remind your colleagues and peers.

Step 3

Destruction. Once a deadline has been reached and it is time to destroy the data. For soft copies of data, it is a case of right-clicking and deleting. For hard copies, paper copies with data on them, it is imperative that the data is shredded for recycling (which covers you for GDPR and sustainability objectives).

Step 4

Documenting your destruction. Note down against your data/document types when and what data was destroyed. This will come in handy for your own recollection and the paperwork needed for ISO quality management certifications. The best way to document the destruction of your data is to use a data or document destruction company, such as CS Shredding, as they will provide you with a 'Certificate of Destruction' which will correspond with the documented dates of your data clear out.

For very small organisations, you can usually handle the shredding of data using an office shredder but for any organisation with 10 or more staff/100 or more customers it can be more financially viable to use a confidential shredding company.