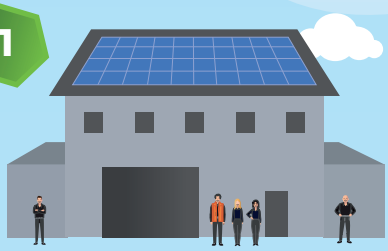
Simple Guide to GDPR
Compliance & Data Destruction

With the implementation of General Data Protection Regulations back in May 2018, we have compiled a simple guide to staying compliant, with particular regard to meeting data destruction requirements. Fundamentally, you should only collect the data you need, only use it for its intended purpose, and only keep it for as long as necessary.

1



GDPR awareness & data protection policy

As well as paying an annual data protection fee to the ICO, everyone in your organisation should be aware of GDPR. If an employee's role involves handling confidential or personal information, they should receive formal training, either via online courses or delivered in person. Your data protection policy should also be updated to cover the GDPR, reinforcing the importance of protecting data. You should also highlight the risks of not complying.

2

Data processing audit

Consider what data you hold, where it came from, how/when it is updated and how long you retain it.

Are you recording data consent from individuals? What permissions do you have for that data? Can you remove data at an individual's request? Are you only keeping it as long necessary for the original processing purpose? Is it special category data?

Both electronic and paper data needs to be considered.

Some example areas to look at:

- Quote processing
- Email and mailshot lists
- Personnel files

3

Data access audit

Consider what you do with the data.

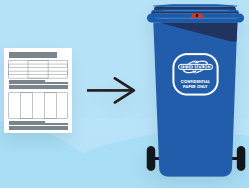
Do you pass data to other people or organisations? How do you transfer data? Where is the data held and is it adequately protected?

Again, both electronic and paper documents need to be considered.

Example areas include:

- Any suppliers/sub-contractors used
- Data storage
- Archiving
- Data deletion and destruction

4



Data destruction policy

Create a data destruction policy and communicate it to everyone in your organisation. Keep it simple and easy to follow. Your policy should include at least the following steps:

- When data should be destroyed or deleted, considering mandatory retention periods
- Placing confidential materials that need to be destroyed into secure containers or lockable bins
- Keeping materials separated to ensure destruction and recycling is possible - e.g. separate bins for paper and hard drives

For large firms, you could also highlight where to find lockable containers, how often they are collected, and what to do if they are full.

5

Outsourcing data destruction

When you outsource information destruction, you'll receive a Waste Transfer Note and Certificate of Destruction with every service. These documents complete your audit trail for confidential materials, further demonstrating GDPR compliance.

With regularly scheduled destruction, you also help to ensure that your organisation stays on top of its data destruction obligations throughout the year, as well as cementing proper information destruction as a regular part of your employees' day-to-day responsibilities.

An established and fully accredited shredding service supplier will also be able to supply receptacles as part of the service, keeping your confidential materials safe between collections.

It's important to outsource to an accredited data destruction supplier. Ensure the provider you outsource to can prove relevant accreditations, such as:

- UKAS accredited ISO 9001
- UKAS accredited ISO 14001

A reputable, trusted shredding service provider will also be a member of:

- The BSIA
The UK's trade association for the private security industry

- UKSSA
To become a United Kingdom Security Shredding Association member, businesses must demonstrate EN 15713 compliance - the European standard for shredding services.

Please note: This document is not intended to be a definitive guide to GDPR compliance. The GDPR has many aspects to consider for full compliance. The ICO provide detailed guidance to help meet all requirements of the GDPR:

https://ico.org.uk/for-organisations/