# 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.

1

### GDPR awareness & data protection policy

Everyone in your organisation should be made aware of the new regulations. Your data protection policy should be updated for the GDPR and the importance of adhering to the policy reinforced. The risks of not complying should be highlighted to decision makers in your organisation.

2

### Data processing audit

Consider what data you hold, where it came from, how and when it's updated and how long you hold it. Are you recording data consent from individuals and what permissions you have for that data, can you remove data at someone's request.

Both electronic and paper documents need to be considered.

Some example areas to look at:

- **Quote processing**
- **Order processing**
- **Newsletter/mailshot lists**.

3

### Data access audit

Consider what you do with the data. Who do you pass data to (other people & organisations), how do you transfer data, where do you hold the data and is it secure.

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

Example areas include:

- **3rd party suppliers/shipping/ sub-contractors**
- **Data storage**
- **Archiving**
- **Data deletion/destruction**.

4

### Data destruction policy

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

- **Placing confidential documentation and data into the required locked, secure, receptacle**
- **There should be separate receptacles for paper and electronic media.**

For large organisations you may also wish to highlight where receptacles can be found.

5


### Outsourcing data destruction

Providing an audit trail for each step of your data can prove compliance with the GDPR. For data destruction you can set up a regular schedule with a GDPR compliant, secure, data destruction provider to ensure receptacles are emptied and shredded in a timely and secure manner. Secure receptacles will often be supplied free of charge with a regular service.

A certificate of destruction is received to complete your data audit trail.

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

- **UKAS accredited ISO 9001 incorporating EN15713**
- **PCI DSS - for credit card data.**

A reputable, trusted shredding company goes beyond required accreditations and will also be a member of relevant trade organisations and associations. For example:

- **BSIA**
- **UKSSA**
- **SafeContractor**
- **Fleet Operator Recognition Scheme (FORS)**
- **Gangmasters and Labour Abuse Authority (GLAA).**

**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/guide-to-the-general-data-protection-regulation-gdpr