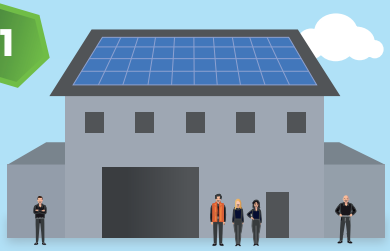
Simple Guide to GDPR
Compliance & Data Destruction

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 aware of GDPR. If an employee's role involves handling confidential information, they should receive formal training. Your data protection policy should be updated to cover the GDPR and the importance of adhering to the policy should be reinforced. The risks of not complying with GDPR should be highlighted to all employees.

2

Data processing audit

Consider what data you hold, where it came from, how and 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?

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.

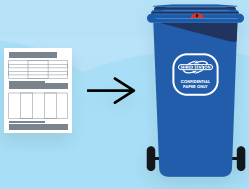
Do you pass data to other people or other organisations? How do you transfer data? Where do you hold the data and is it adequately protected?

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

Example areas include:

- Any third party suppliers, shipping or sub-contractors that you use
- 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:

- Placing confidential documents and data into the required locked, secure receptacle
- Paper and electronic or magnetic media should be kept separate

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 compliance and fully accredited data destruction supplier to ensure receptacles are emptied and materials shredded in a timely and secure manner.

Secure receptacles will often be supplied free of charge with a regular service.

A Waste Transfer Note and Certificate of Destruction will be issued to you to complete your data audit trail.

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 9001:2015 incorporating EN 15713
- PCI DSS Level 1 Service Provider for credit card data

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

- BSIA
- UKSSA
- SafeContractor and SafePQQ
- Gangmasters
- FORS

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/