GDPR: PAPER DOCUMENT STORAGE AND SHREDDING

GDPR and document retention: Best practices for paper records

Discover GDPR's impact on document retention and learn about secure shredding practices and compliance tools for businesses.

RECOMMENDED BY THE FELLOWES WORKLIFE COACH

The European General Data Protection Regulation (GDPR), enacted on May 25, 2018, has brought about significant changes in how businesses manage personal data, extending its jurisdiction from public authorities to small and medium-sized enterprises. Stringent rules for the processing of personal data, covering information such as names, addresses, email addresses, social security numbers, means that organisations of all sizes need to ensure they implement best practices when it comes to processing data. Not only is there a moral obligation, but non-compliance could result in fines of up to 4% of global turnover or €20 million, emphasising the critical need for businesses to prioritise data protection.

GDPR and Document Retention: Best Practices for Paper Records

To align with GDPR, businesses must extend their data protection policies to encompass paper documents. Whether stored electronically or as hard copies, organisations need to implement technical and organisational measures to ensure secure data processing. Key considerations for paper documents under GDPR include:

- **Secure Destruction:** Documents containing data no longer needed must be securely destroyed through methods such as shredding.
- **Organised Storage:** Documents that need retention should be stored in a manner allowing easy traceability and accessibility when required.
- **Access Control:** Sensitive documents require storage in locked cabinets, with restricted access limited to authorised personnel.
- **Inclusion of Remote Workers:** Policies should encompass temporary and remote workers, outlining procedures for protecting documents and data in their possession.

The Data Protection Principles

Every data protection strategy should respect the principles that data shall be:

1. Processed lawfully, fairly and in a transparent way
2. Collected for specific, explicit, and legitimate purposes, and not subsequently processed in a way that goes against those purposes
3. Adequate, relevant, and limited to what is necessary
4. Accurate and up to date. Inaccuracies should be processed, erased, and rectified
5. Kept for no longer than is necessary
6. Processed securely

We've seen that a core principle of GDPR is that data must not be kept any longer than is necessary and is disposed of securely. Below we'll investigate why shredding is so important to complying with GDPR.

Secure Shredding and GDPR: What You Need to Know

It's not secure until it's shredded!

Every organisation has a legal responsibility to safeguard sensitive information and dispose of confidential material securely. The organisation is also responsible for any confidential material that's taken outside its premises by any of its employees. This includes both hard copy documents and anything that can be viewed on a computer, laptop or mobile device.

Despite increased awareness of identity fraud over the last few years, crime is still growing at an alarming rate in the UK. And, because we deal with so many pieces of information on a daily basis, we're all at risk – individuals and organisations alike.

A discarded bank statement, or a snippet of payroll information or a crumpled customer proposal could be all a criminal needs to cause irreparable damage to you and your business

---

Three Tips for Better Shredding Practices

Secure shredding is key to keeping confidential paperwork out of the wrong hands and reducing organisational exposure to data breaches. Using a shredder to safely destroy confidential paperwork should be part of our daily routine, wherever we work.

- Don't assume everyone understands GDPR. Educate all employees on GDPR requirements, personal data handling and the six principles of data protection. This training should be given to all new starters, whenever legislation is updated, and as part of regular data security refresher sessions.
- Shred all sensitive paperwork before recycling or disposing of it, ideally without needing to take the risk of transporting it from home to office, or vice versa.
- Give all employees easy access to a secure shredder at home and at work to ensure GDPR compliance wherever your team might work.

It's clear that shredding is the best way to securely destroy confidential documents, protecting sensitive business information and personal identities.

Take action to protect your business today.