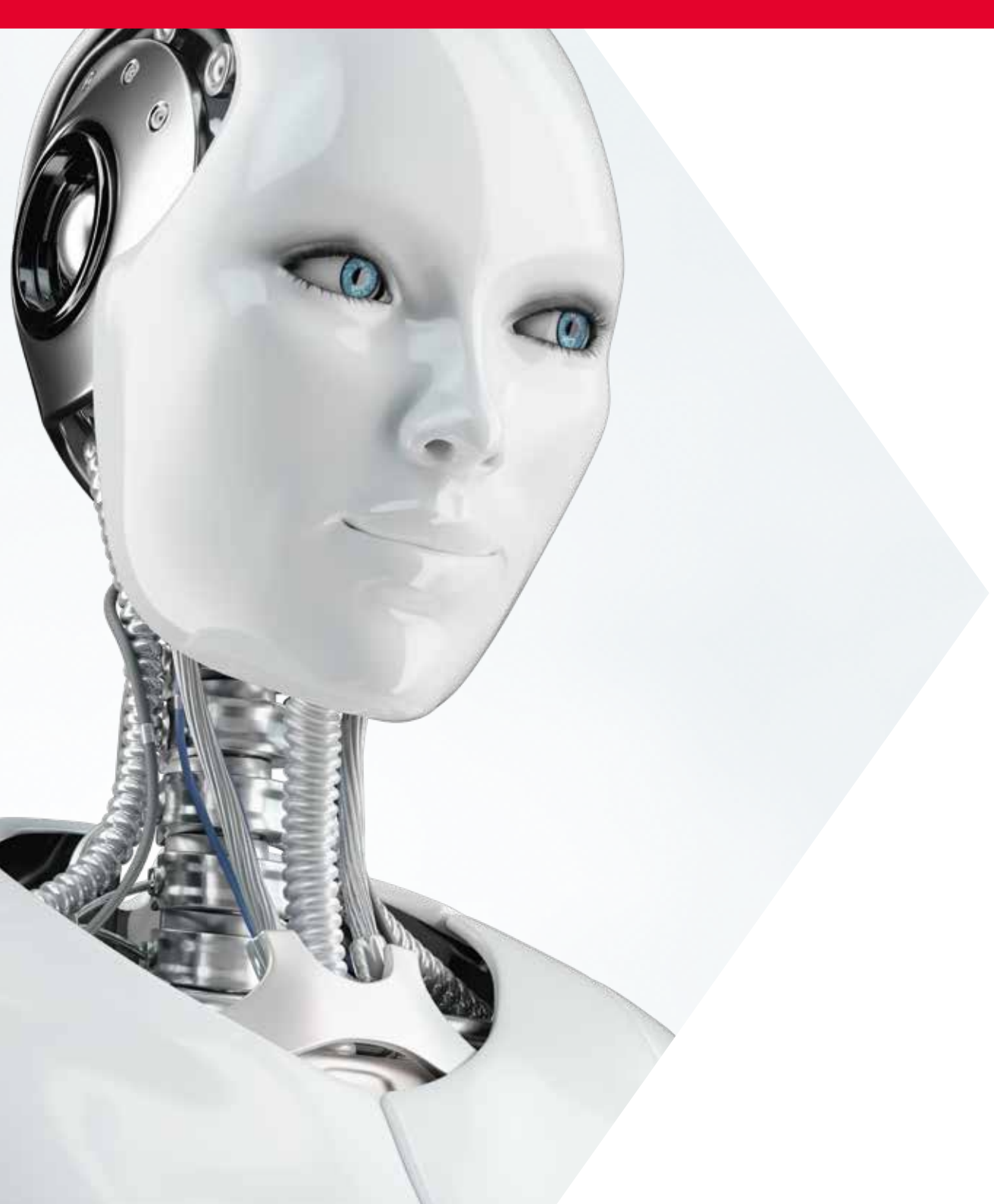


Intelligent shredding

For A GDPR Compliant Generation

Why a paper security policy is an integral part of your GDPR compliance.

Disclaimer

Nothing contained herein should be construed as legal advice. Organisations should consult legal counsel with regard to compliance with the General Data Protection Regulation or any other applicable laws or regulations.

GET GDPR COMPLIANT*

*shredding supports GDPR compliance

With compliments of Viking

› About this document

This white paper gives you **an overview of what the GDPR aims to achieve**, the problems it presents to organisations, and offers a framework solution for businesses to use to support compliance with this new regulation.

The purpose of this paper is to give you an introduction to the EU's General Data Protection Regulation (GDPR) and how it impacts different businesses, so you can create a framework for a paper security policy for your own business, now these regulations have come into effect.

So what is the GDPR? It requires organisations to apply sound security practices to electronic and paper-based data and, in the case of a data breach, notify affected or potentially affected individuals.

The GDPR's reach extends globally to all organisations that control or process personally identifiable data about people in the EU, regardless of the geographic footprint of those organisations. GDPR requirements apply to both electronic and paper-based personal data and means that all organisations should address GDPR requirements if they handle EU-originated personally identifiable data.

While electronic data security is rightly top of mind for many organisations, many fail to adequately address security of paper-based data. In fact, two thirds of offices admit to not shredding confidential information.[1] This puts organisations at risk for non-compliance with GDPR, and data subjects at risk for fraud and identity theft. With this in mind, Rexel, a leading shredding machine brand, encourages organisations to review their security policies and practices relating to both paper-based and electronic data.

THE GENERAL DATA PROTECTION REGULATION

An overview

The GDPR seeks to protect privacy rights of individuals in Europe, whether they are EU citizens or not. These privacy rights include, but are not limited to:

Transparency
The right to be provided clear information about how organisations process personal information.

Consent
The right to control how organisations use personal information.

Security
The right to have information about how organisations adequately protect personal information.

Collection and purpose limitation
The right to expect that organisations minimise their information collection and uses.

Breach notification
The right to be informed in the case of a data breach.

The GDPR is part of the European Commission's plan to modernise and harmonise data protection rules.

While the GDPR's main objective is to strengthen online privacy rights, it still addresses paper-based data privacy.

It focuses on tackling the ever-increasing challenges towards data protection and privacy, exposure to security breaches, hacking and other unlawful processing.

THE GENERAL DATA PROTECTION REGULATION

What's changed?

The following points **identify the specific areas within the GDPR that are new** rights for individuals or existing rights under the Data Protection Act (DPA) that have been strengthened as part of the GDPR:

Data portability and the right to be forgotten

- Individuals now have the right to transport their personal data from one organisation to the next
- Personal data must be provided in a structured and machine-readable format
- A person can request the deletion or removal of personal data

Data breach notification

- Any breaches should be reported to the supervisory authority
- Individuals affected by the breach should also be informed

Inventory

- Local authorities no longer have to be informed that personal data is being processed
- Organisations must maintain a record of processing activities under its responsibility

Data Protection Impact Assessments and security

- DPIAs are a means to identify high risks to the privacy rights of individuals
- Security requirements and recommendations should be based on a risk assessment

Data governance and accountability

- Organisations must also be able to demonstrate compliance with the GDPR

Non-compliance with the GDPR may result in **fines of up to 20 million Euro, or 4% of the Global Company Revenue**, whichever is greatest. Furthermore, a data subject has the right to sue an organisation within a court of law.

THE GENERAL DATA PROTECTION REGULATION

Why does it apply to?

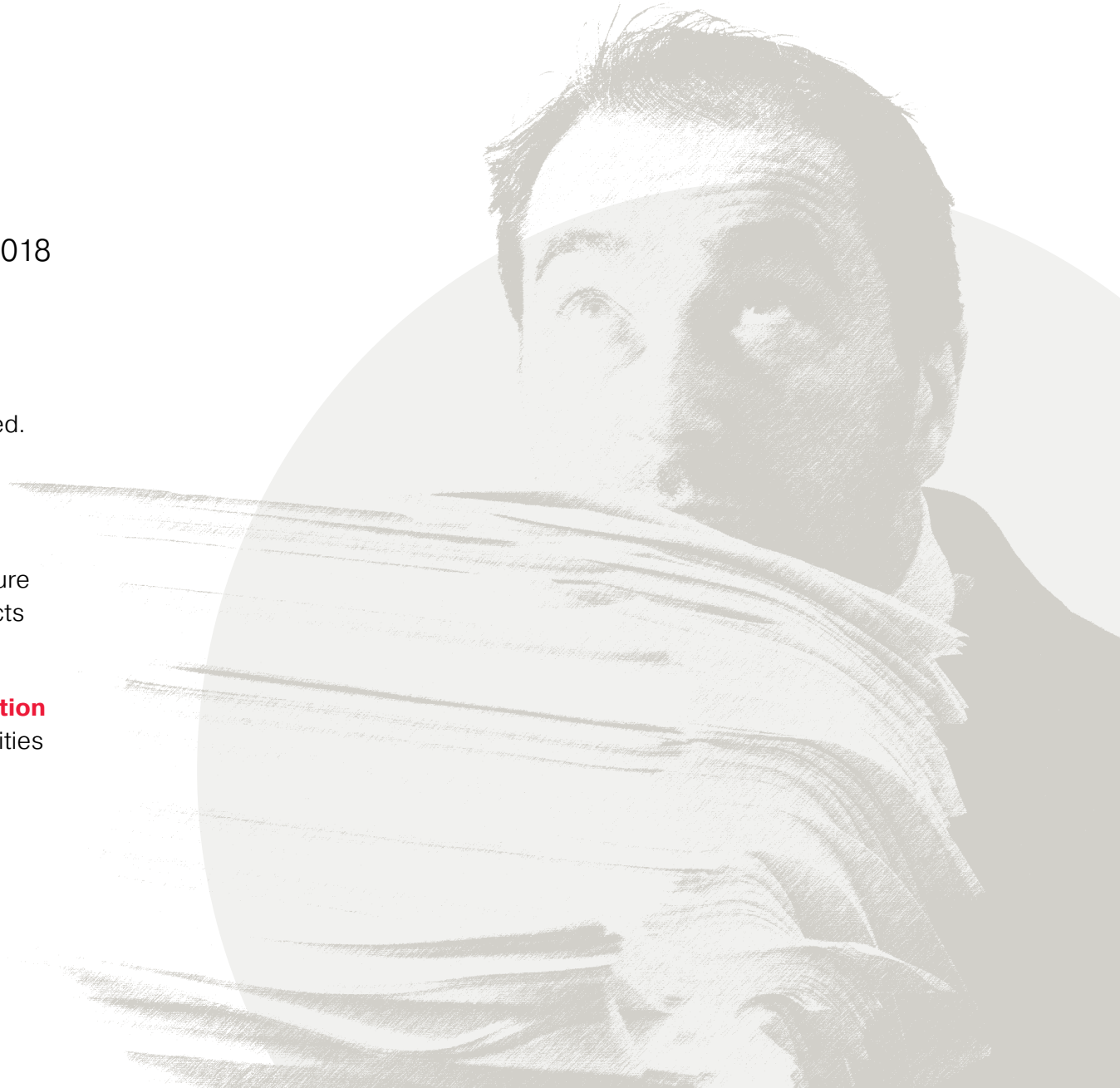
The introduction of the GDPR in May 2018 impacts the following roles:

Data Controllers
They say how and why personal data is processed.

Data Processors
People acting on the controller's behalf.

It is the responsibility of these two figures to ensure that their clients are fully compliant with all aspects of the GDPR, to avoid incurring any fines.

A Data Processor **must appoint a Data Protection Officer** and keep records of all processing activities they perform on behalf of clients.



GDPR covers personal data and sensitive personal data in electronic and physical formats

It's important to consider what kinds of data the GDPR will apply to, when constructing a compliance policy for your organisation.

Data within scope of the GDPR includes any information about an identifiable person. Some examples of GDPR-covered **personal data** include full name, e-mail address and phone number.

The GDPR also applies additional protections to a **sub-category of personal data, called sensitive personal data.**

The GDPR is concerned with personal data handled by organisations in both **electronic and physical formats**, such as paper documents.

A business framework to GDPR compliance

Organisations have three main areas that must be reviewed in order to achieve GDPR compliance. By addressing these three components, businesses can construct clear frameworks of a data security policy for each aspect, which will enable full compliance in all areas of the GDPR.

These components are:

People

Staff ownership and responsibility of any data processed by them within the organisation is critical. An organisation must set out clear rules to each and every employee for the proper management of all electronic or paper-based data held within the business. These regulations put into action the requirements of the GDPR regarding the handling all data. For example, it may be that you wish to introduce clear rules about the use of paper documents containing sensitive information and the process for the correct shredding the document once used, based on the sensitivity level of the data contained within.

Processes

This relates to the processes within the organisation. For example to manage the use of data such as processing or storing data on customers. It is crucial that businesses review all of their current processes relating to data. Once gaps and weaknesses within their existing procedures are identified, a framework plan must be developed by the business that will see these areas strengthened or replaced, where necessary, in order to comply with the GDPR.

Technology

Current IT capabilities and requirements should also be reviewed and adjusted accordingly. It is up to the individual business to ensure that any existing systems that do not fully support the regulations are either improved or replaced, to avoid incurring any potential fines.

Why does paper security matter?

Having discussed what the GDPR requires businesses to do, it is now pertinent to address the issue of paper security within organisations and why it is a key concern for businesses in order to meet the GDPR's requirements.

In fact, a 2014 PwC report, in conjunction with records management company Iron Mountain[2] – which surveyed European mid-market companies about how they perceive and manage their information risk – found that two-thirds of respondents said that managing the risks associated with paper records was a top concern.

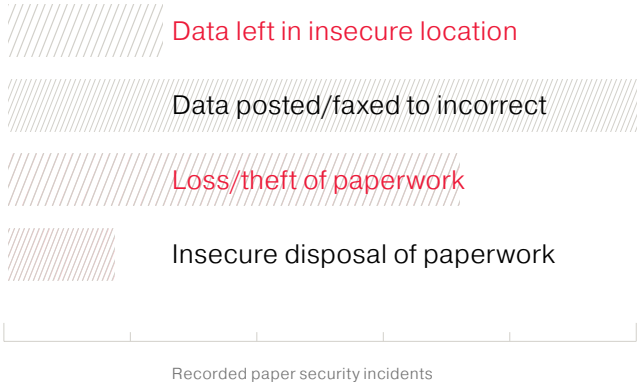
While digital threats are high on an organisation's agenda, it would be a mistake to assume **that paper-based security risks** have gone away.

Paperwork still accounts for many common security breaches

Of 598 data security incidents recorded between July and September 2016 by the UK's data protection regulator, the Information Commissioner's Office (ICO):

14% were due to the loss or theft of paperwork. **A further 19%** were posted or faxed to the incorrect recipient. **Another 3%** were due to the insecure disposal of paper. So despite an exponential rise in digital technologies, **40% of incidents** were attributable to paper[3].

40% of UK data security incidents were attributed to paper



User cooperation is critical to GDPR compliance

If we can conclude that paper security remains vital to information security, then the question is:

what can organisations do about it?

Rexel specialises in providing paper shredders to organisations, with the ability to partner directly with organisations such as Kensington, the world's leader in physical security for IT hardware when sharing customer insights, has allowed us to gain valuable insights into the needs, wants and challenges facing organisations seeking to protect themselves and comply with the GDPR.

These insights have lead us to believe that there are two main barriers to effective document shredding in organisations:

Lack of awareness

Businesses are disregarding the importance of paper in an increasingly digital workplace and are therefore not taking the time to address the security issues associated with paper documents. Even when there is a policy in place, if regulation is not communicated effectively to all levels of the business, it will often lead to a lack of awareness.

Ease of use

The availability of suitable shredding machines is crucial to the success of an effective document shredding policy. Too often organisations or offices are relying on ineffective manual shredders that are not fit to meet their capabilities, leaving employees unable to shred documents effectively and productively.

Once the barriers to implementing an effective shredding policy have been pinpointed within the organisation, the next step is to determine a suitable solution to tackle these barriers.

Solution one to GDPR compliance

Lack of Awareness

Employees generally perform activities which are clearly highlighted as a priority by their managers.

With this in mind, a clear and firm document shredding policy can solve many inefficiencies.

The 2014 PwC/Iron Mountain survey[2] of European midmarket companies notes that just 40% have clear employee guidance on internal disposal and storage of physical documents, and only 27% have company policies for the safe security, storage and disposal of confidential information.

Solution two to GDPR compliance

Ease of Use

A second common cause of employee non-compliance with document shredding is the difficulty and time consumption of the task.

While workers may have access to shredders, not all workers may shred necessary documents if the activity takes significant time or is difficult to manage.

Unsurprisingly, no organisation wishes to invest in shredders that their employees are likely to neglect to use due to poor productivity or ease-of-use barriers so these issues should be solved to ensure maximum use.

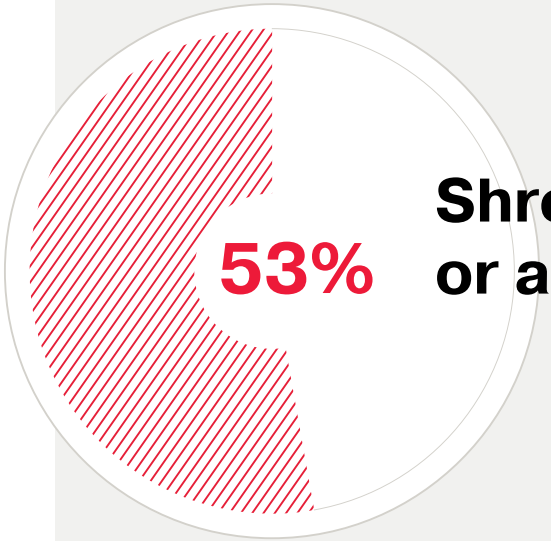
Increase employee productivity with Auto Feed technology

Conclusion

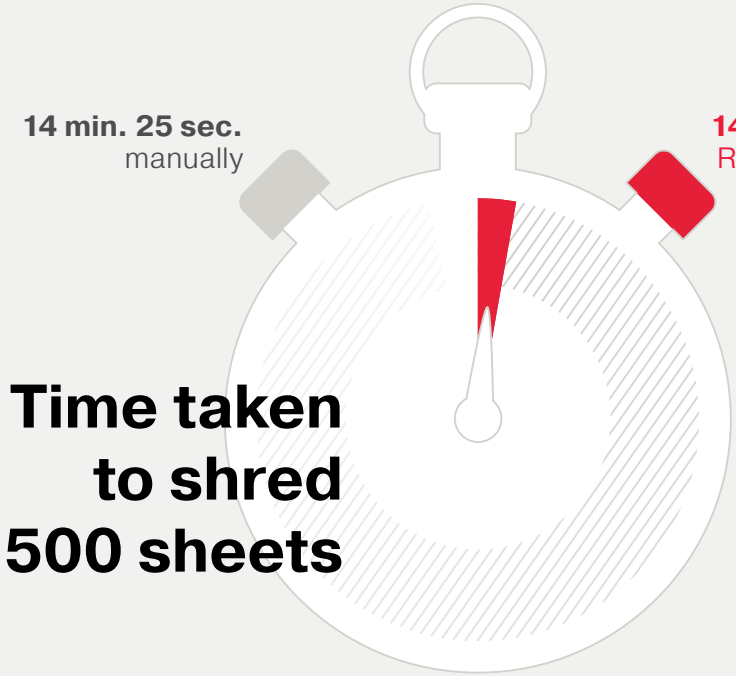
Make your paper security policy work with Auto+ SmarTech shredders.

Our Auto+ SmarTech shredders, auto feeds paper which enables monitoring and maintenance in multiple locations and are a direct response to encourage employee compliance with paper security. Research[4] shows that 53% of employees adopt batch shredding behaviour, whereby the employee builds a stack of multiple documents before they feel a trip to the shredder is merited.

By allowing employees to shred stacks of paper, an independent research found that their employees could spend 98% less time shredding [5] and be more inclined to shred more frequently.



Shred in batches or all at once



14 min. 25 sec. manually

14 sec. with Rexel Auto+ Shredders

Time taken to shred 500 sheets

6-point GDPR action plan for your business

1. Appoint a Data Protection Officer

This officer must be fully commensurate with the organisation's responsibilities regarding GDPR and have a thorough understanding of what data within your organisation counts as 'personal', where it's kept, who has access to it, how to spot breaches when they occur and who to report this to. The Data Protection Officer doesn't have to be an employee – you can outsource this function.

2. Assess your systems

Review all contracts, technology support, procedures and tools that relate to the processing, handling, storing and deleting of data to enable you to identify any weaknesses or gaps that require changes to be made.

3. Develop a strategy

Construct a new strategy that will ensure full compliance with the GDPR. This strategy may encompass new investment in technology, revise staff procedures and responsibility for data processing, create new roles within the organisation.

4. Implement new organisation policy

The next step towards GDPR compliance is to put your plan into action throughout all levels of the organisation. Invest and introduce new technologies and systems required in the workplace and publish an informative data handling and processing guide.

5. Employee engagement

Launch your new data compliance policy to all staff; provide training, information and guides to employees so they are educated and aware of the changes taking place and their responsibility in ensuring that the company meets the requirements of the GDPR.

6. Review and improve

After launching your GDPR compliance plan, it should be continually reviewed and improved, even after the regulations have come into effect.
By continually identifying any necessary improvements it will successfully and efficiently ensure your organisation is completely compliant.

Sources

1 envirowaste.co.uk/blog/articles/third-companies-shred-private-documents

2 Beyond good intentions: The need to move from intention to action to manage information risk in the mid-market, PwC report in conjunction with Iron Mountain, June 2014

3 ico.org.uk/action-weve-taken/data-security-incident-trends

4 Evaluating Auto Feed Shredders. Prepared for ACCO Brands by Deep Blue Insight

5 Independent test from Intertek Testing & Certification Ltd June 2012

- Max saving when using an Auto+ 500X with SmarTech compared to a traditional feed shredder in a similar price level
- Research shows it takes an average of 14 minutes and 25 seconds to manually insert 500 sheets of paper into a traditional, manual-feed-shredder – but only 14 seconds to load the same number of sheets into an Auto+ 500X with SmarTech

www.rexeleurope.com

For more information please contact:

ACCO UK Ltd.
Oxford House
Oxford Road
Aylesbury
Buckinghamshire
HP21 8SZ