The mini guide to risk management in information security, disposal and compliance

Contents

Foreword

Robert Guice
Shred-it, Executive Vice President EMEA

One of the most important duties of any business, charity or public sector organisation is to safeguard the personal information that it collects as part of its normal operations. All organisations are required by national and European law to keep information secure to the point of destruction before disposing of it. Sound information management therefore goes beyond best practice and compliance (although these are still important drivers). Protection of reputation or brand, guarding against identity theft, fraud and improper disposal of information, are integral to sustainability.

Everything from a pay slip, sales invoice, supplier tender, strategy paper, operational documentation, budgets, sales and marketing planning, staff appraisals and medical records for example, has value to someone because it contains sensitive or confidential information about your organisation, employees or customers. At what point does this information become 'waste' and when is it safe to be seen internally or externally by a competitor, an investigative journalist or identity thief? "Never" is the safest answer but each organisation has different challenges and must tailor their solutions accordingly.

I hope you find this guide a valuable starting point in forming a secure information management solution.

What is secure information management?

Secure information management is the business process by which corporate and non-corporate organisations keep personal data on individuals safe. It begins from the moment personal information is acquired and only ends when that information is no longer stored and has been securely destroyed. The responsibility between those times belongs to the management of the organisation keeping the data.

Controlling the life cycle of information and its distribution internally and externally is what secure information management is all about. The risk points and setting protocols need to be understood and designed to minimise the opportunity to see, copy or remove information in digital and hard copy format throughout the life cycle of that information.

Despite the computerisation of many organisations' document storage methods, the paperless office is yet to materialise. While the technology used to store and exchange sensitive and confidential information may have changed, the need to take document management seriously within an organisation has not.

Secure information management is also about the way in which information is disposed of. How and when information is destroyed and where it enters the 'waste' stream is crucially important.

Why is information security important?

All UK organisations have a legal duty of care for the personal data they hold and there are a range of regulations and stipulations to be aware of.

The Information Commissioner's Office (ICO) can levy fines of up to £500,000 for a serious breach of the Data Protection Act. An example of this is business or employee information leaks (inadvertently or otherwise).

Risking a criminal prosecution is one thing, but customers do not tend to return to organisations who fail to look after sensitive information appropriately (including bank account details, phone numbers or other items that can help the ID fraudster). Reputations can take a long time to repair if a data breach becomes headline news.

There are information security risks throughout the life cycle of every piece of information – from access and distribution to printing and disposal of copies and master files. Planning and maintaining appropriate information security protocols is much more than a compliance issue – it is essential for the well-being and sustainability of an organisation, its day to day business operation and the protection of its employees.

A guide to the legislative landscape

Data protection is a large, rapidly changing issue where legislation and regulation will always be playing catch-up to the latest technological advances. Here are the main elements of the current legislative framework surrounding information management and disposal in the UK.

The **Data Protection Act 1998 (DPA)** came into force in the UK in 2000. It remains the most important piece of legislation regarding data security as it outlines the protection and policies that must be in place to protect the use and storage of information that can identify any living individual (by itself or in connection with other information held by the organisation).

At the heart of the DPA are 8 data protection principles:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The DPA also embeds the principles of the EU Data Privacy Directive into UK domestic law.

HM Revenue and Customs tax rules also require organisations to retain information for certain periods. Businesses must generally keep a record of all their receipts, expenses, sales and purchases that are relevant for VAT for a minimum of 6 years. Business taxpayers submitting self assessment returns must keep their returns and supporting documents for longer periods of time dependent on individual circumstances.

The **Companies Act 2006** compels companies to keep accounting records for up to 6 years in the case of a public company and other formal company documents for an indefinite period.

The **Freedom of Information Act (FOIA)** was introduced on the 1 January 2005 and applies to the information held by public authorities. Guidance issued under the FOIA makes clear that records should be disposed of in accordance with established policies and these policies should be enforced by authorised staff. While awaiting disposal, records should be stored correctly to meet the required standards. Records not selected for permanent storage should be destroyed once they have ceased to be of use to the authority, keeping a record of what is chosen for destruction.

The **Waste Hierarchy** came in to force in England and Wales on 28 September 2011 - **Waste Regulations 2011**, and requires all organisations (public and private) that produce, handle or control waste, to take all reasonable measures to prevent waste and apply a "waste hierarchy" designed to reduce environmental impact.

The **EU Waste Electrical and Electronic Equipment Directive (WEEE)** applies to the disposal of electronic equipment including hard drives, photocopiers etc. Much of this electrical equipment contains sensitive information which should be securely recycled or disposed of to ensure that there is no unauthorised access to personal data within or at the end of the life cycle of a digital storage system.

European Data Protection Review and the ensuing legislation

The basis of the EU Data Protection Directive 1995 sets out the framework for data protection laws across the EU and establishes an individual's right to privacy in respect of the processing of their personal data.

The European Commission is currently in the process of reviewing the general EU legal framework on the protection of personal data.

It is expected that new legislation will bring about a more unified, consistent approach to data protection regulation across member states. These could affect how companies compile, store, use and destroy business and employee information.

The impending changes to the Data Protection Directive are likely to include enhanced powers for national regulators and may bring US social network companies which handle personal data relating to EU citizens within the reach of EU law.

Enforcement

In the UK, it is the ICO which enforces data privacy legislation. The ICO has powers to take action against any public, private or not for profit organisation as they are all **legally obliged** to protect any personal data they hold.

It is the responsibility of the ICO to enforce the stipulations of the Data Protection Act, the Freedom of Information Act, the Environmental Information Regulations and the Privacy and Electronic Communications Regulations.

The ICO is also under an obligation to promote openness from public bodies alongside the protection of data for individuals.

The ICO has a **range of measures** it can take to enforce data privacy legislation which **were added to in April 2010**. They range from undertaking information audits, to **financial fines of up to £500,000** for a serious breach and finally assisting in criminal prosecution. They can be used separately or in combination, depending on the severity of the issues being investigated.

The ICO **decides the level of fine based on the seriousness of the data breach**, the likely damage, the distress caused to individuals, whether the breach was deliberate or negligent, and what reasonable steps the organisation has taken to prevent breaches.

Case study

Practice Manager,
Field House Medical Group

Field House Medical Group is an NHS practice in Grimsby serving over 15,000 patients. Their concern is patient confidentiality and inappropriate access to sensitive information, together with how environmentally friendly the practice is.

The practice is required to adhere to the Information Governance Assurance Programme (IGAP) guidelines which apply to the health and social care sector. They provide advice for the storage, destruction and recycling of information held by health organisations and requires an unbroken chain of information security to protect patient records and other sensitive information.

"Shred-it is integral to our information security solution. Secure consoles enable all staff to dispose of unwanted, old or archive information in real time with no chance of access by anyone else. The consoles are emptied at regular intervals to suit the practice by CRB-checked security staff and the information is immediately destroyed on site in a Shred-it truck behind a locked security screen before being recycled. The process is simple and convenient, secure, has freed up valuable staff time and increased the amount of material we recycle".

Where does the information security threat come from?

Potential threats to information security do not just come from outside an organisation. According to research from KPMG (Data Loss Barometer Issue 3 November 2010), one in five data loss incidents are now triggered by 'malicious insiders'.

Here is a summary of the most important internal and external data breach sources organisations should bear in mind.

Inside the organisation

- Leaving confidential documents in non-secure locations such as **recycling bins** or **waste paper** baskets means they could be accessed by anyone at anytime, including being stolen whilst awaiting collection
- If a **confidential shredding console** is allowed to overflow, then it's no longer secure. Make sure you have enough consoles and that they are secure and emptied regularly
- Have a **clear desk policy** and secure storage areas for employees to place 'work in progress' documents when they're out of the office
- It's a sensitive subject, but what do you really know about **your employees**? Make sure that everyone who has access to sensitive or confidential information has been CRB checked

- CD-ROMs, USB sticks and other **digital storage devices** are great storage facilities, but make sure you know who has access to devices which hold confidential information and limit what they copy or transfer
- Blurred **photocopies** containing confidential information should be securely disposed of. They may have no value to you but could be very helpful to a fraudster
- Confidential **electronic data** should be treated in the same way as paper based information. If you need to dispose of a hard drive, have it pulverised so that information stored on it cannot be retrieved.

Outside the organisation

- Off site shredding: If using an external provider for off site shredding or recycling, your organisation may be in danger by handing over confidential information intact to a third party without the ability to conveniently witness the destruction of your confidential information
- Multi-occupancy premises: If you share premises with other companies, make sure that no one from outside your organisation can gain access to confidential information within your office space

- Contract staff: If you CRB check your own staff, make sure you also vet anyone from outside the organisation who is working on your premises. This applies to suppliers, consultants and seasonal workers too
- Passers by: Try to minimise the amount of documents left open on desks and near ground floor windows
- External meetings and working from home: It may seem obvious, but when you are out of the office you need to still follow the same information protection processes that you would in the office – your client or suppliers' offices may not be as safe as yours so don't leave anything behind and only take the minimum amount of information you need out of your own office.

The road to compliance

The first stage of ensuring your organisation is safe from the risk of data breaches and is compliant with the law is to draw up a document retention policy.

Things you may wish to include in your policy are:

- A statement of purpose
- Categories of documents and how long they should be kept
- Definition of "document" and the format in which it is to be retained (electronic or hard copy)
- Guidance on creation of documents
- Members of staff designated to deal with the document management system
- Methods of document destruction
- How to keep an accurate record of documents destroyed.

A list of organisations that will be able to provide specialist advice on how to protect against the threat of data breaches is included at the end of this guide. On the following pages are some suggestions to get you started.

Document retention

- Make yourself aware of any legal requirements relating to the length of time official documents need to be kept
- Be clear about who has the final say over whether a document should be destroyed or kept
- Make sure no staff member will dispose of records unless authorised to do so.

Hard copy

- Be ruthless about allowing access to sensitive information – keep it to only those who really need to know
- Try to reduce the amount of paper which needs printing and therefore destroying – can you project all the information for a meeting from a laptop rather than printing a set of documents for everyone in the room?
- Have a process in place for storing written information securely
- Have a process in place for destroying information when it is no longer needed
- Ensure sensitive material is cross-shredded to prevent anyone being able to reconstuct it.

Electronic storage

- Keep access to information limited as you would for hard copies
- Ensure staff use secure passwords and do not share them with colleagues
- Encrypt personal information held electronically
- Securely remove all personal information before disposing of old computers
- Remember that information is also stored on external devices including USB sticks, laptops and even the hard drives of photocopiers and printers
- Regularly review group email lists
- Check a recipient's security arrangements before sending emails to them
- Prevent employees from keeping records in separate, individual filing systems or on their computer hard-drive.

Management and treatment of waste

- Adhere to the 'Waste Hierarchy' by considering and reducing the environmental impact of the waste you are responsible for. The five recommended steps from most to least desirable are:
    1. Prevention (use less and greener material)
    2. Prepare for re-use (check, clean, repair, refurbish)
    3. Recycle (turn waste in to new products)
    4. Other recovery (including producing energy)
    5. Disposal (landfill or incineration without energy recovery)

Disposal comparisons

Landfill

Pros:

- Relatively low cost
- No need for staff training

Cons:

- No peace of mind that information has been securely destroyed
- Liability in the event of data breach incident
- Places secure information in waste stream
- Not environmentally sustainable

In-house shredding

Pros:

- Perceived low cost
- Convenience
- Control over the process

Cons:

- Not always cross-shredded
- Machine failure can lead to backlogs of unshredded confidential material
- Not all material is always recycled
- Inefficient use of employee resource and time
- Health and safety risk

Recycling

Pros:

- Environmentally sustainable
- Low cost

Cons:

- Places secure information in waste stream
- Confidential material segregated and sorted by hand before shredding
- Supplier staff may not be CRB checked

Off site document destruction via third party supplier

Pros:

- Confidential information not placed in waste stream
- Convenience of outsourcing
- Staff are typically CRB checked

Cons:

- Waiting period before Certificate of Destruction is issued
- No categoric proof that information has been destroyed securely
- No guarantee all staff are CRB checked

On site document destruction via a third party supplier

Pros:

- Audit trail (you can prove material has been destroyed)
- Cost savings possible verses in-house (staff) shredding
- Environmentally sustainable
- Instant receipt of Certificate of Destruction (peace of mind)
- Legal responsibilities satisfied
- Low cost and easy to implement
- More paper is recycled
- Tailor-made solution
- Totally secure

Cons:

- None

Questions to ask yourself

- At what point does your confidential information become 'waste'?
- If your confidential information was 'waste', why would anyone want to steal it?
- What are your organisation's internal protocols when it comes to information security (hard and soft copy)?
- Are these documented or enforced and do all employees know about them?
- When was the last time information security protocols were reviewed and independently audited?
- How do existing information security processes prevent sensitive and confidential information from entering the waste stream?
- Can you be sure that every employee in every office is fully compliant with the correct security processes?
- What would the consequences of a data breach be for your organisation?
- Who would be ultimately responsible for a data breach internally?
- How compliant is your organisation with data protection policies, best practice and legislation?
- What is the true environmental impact of our organisation's activity and have we taken all measures available that are reasonable in the circumstances to apply the waste hierarchy?

Questions to ask your supplier(s)

- How secure is the 'waste' removal and destruction process?
- When was the last time you audited the process and how frequently do you do this?
- Do you outsource information destruction or is every employee who comes in to contact with your organisation's 'waste' directly employed and security-vetted?
- What level of security checks on employees are standard for your company?
- What happens to my organisation's 'waste' when it leaves my site and how quickly is it destroyed?
- Is there any hand sorting or handling before it is destroyed?
- Who would be accountable if a data breach were to occur (assuming the 'waste' had left my site)?
- Can I audit the process?
- What documentation is supplied to support an audit?
- When do you issue a Certificate of Destruction?
- How do you support carbon reduction efforts?
- Do current arrangements enable us to recycle all paper and electronic equipment ensuring environmental obligations under the waste hierarchy are met?
- Do you provide waste transfer notes containing confirmation of compliance with the waste hierarchy duty?

Case study

Jon Higgins
Managing Director, Aon M&A Solutions

Aon M&A Solutions provide advice and support for companies and private equity groups who are involved in the buying or selling of other businesses. It is crucial to the continued success of their business that they are able to assure their clients that their information is 100% secure. The company's Managing Director, Jon Higgins said, "Our reputation would be severely damaged if the information we hold ended up in the public domain".

Across the Aon group, staff are expected to uphold the highest standards of data security. They have a comprehensive process which covers everything from the acquisition of data, through distribution and onto its eventual destruction.

Aon M&A Solutions, has implemented a "zero tolerance approach to document management" in order to protect private information. They have a shred-all policy. All paper is deposited into locked security consoles where it is removed and destroyed on site in special security trucks before being recycled.

"We know that all of our confidential information is shredded before it leaves our site. This ensures that we are compliant with data protection regulations and no information will be compromised once it leaves our premises."

Glossary

Certificate of Destruction
Some document destruction service providers present their customers with a Certificate of Destruction once they have completed the shredding of their confidential documents. This assures the customer that their material has been completely destroyed.

Data breach
The failure of an organisation to have adequate procedures in place to protect sensitive or confidential information, resulting in it ending up in the public domain. Serious breaches involving personal data are now punishable by fines of up to £500,000.

Data controllers
Data controller is interpreted in the DPA as "a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed".

Data processor
As interpreted by the DPA a "data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Processing
As interpreted by the DPA, " processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including -

a) organisation, adaptation or alteration of the information or data,
b) retrieval, consultation or use of the information or data,
c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
d) alignment, combination, blocking, erasure or destruction of the information or data.

Document retention policy
The codification of processes designed to ensure that confidential information remains private from acquisition through storage and onto destruction. All organisations handling business and personal information should have such a system in place.

EU Data Protection Directive
The directive requires that EU member states (countries) protect the privacy of personal data that is processed in the member state, whether the processing is done by government agencies, businesses, or other organisations or individuals.

Information notice
An information notice is a written notice from the Information Commissioner to a Data Controller or a Public Authority seeking information that the Commissioner needs to carry out its functions. Failure to comply with an information notice is a criminal offence.

In-house shredding
Using individual or central shredding machines for the disposal of confidential or personal information within an organisation rather than using external suppliers.

Off site document destruction
Using a third party supplier to take away, shred and dispose of confidential information at a location other than that of the business from which the material has been generated.

On site document destruction
Using a third party supplier to shred documentation securely at the premises, generating the material and providing an immediate Certificate of Destruction.

Personal data
Personal data is described as any information that can lead to a specific person being identified, either directly or indirectly, and either in itself or in connection with other information held by the data controller, for example; reference to aspects of their identity, appearance or, in particular, by reference to an identification number. Examples of such data include address, bank statements, credit card numbers, email address etc.

Public Authority
The Freedom of Information Act (FOIA) defines a public authority widely and this definition includes: Government departments, Houses of Parliament, local government, NHS hospitals, doctor's surgeries, dentists, opticians, pharmacists, state schools, universities, police and prisons are all covered by the FOIA. The Secretary of State can add to this list where appropriate.

Secure document destruction
Secure document destruction is the process of making sure private information remains private by ensuring that no longer needed printed information is shredded or burned.

Shred-all policy
Is the gold standard in information security meaning that all paperwork regardless of content is routinely shredded and put beyond information use.

Waste
Any materials disposed of by an organisation that does not contain personal or sensitive information which therefore does not need to be securely disposed of by a professional information security company.

Waste hierarchy
Five steps for dealing with waste ranked according to environmental impact. 'Prevention', 'Enable re-use' and 'Recycling' are the top three ultimate goals.

Further information sources

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
T: 0162 554 5745
www.ico.gov.uk

General guidance on data protection, regulation and compliance

Direct Marketing Association
DMA House
70 Margaret Street
London
W1W 8SS
T: 0207 291 3300
www.dma.org.uk

'Data Council' aims to provide advice and drive policy development across the entire data space

Environment Agency
National Customer Contact Centre
PO Box 544
Rotherham
S60 1BY
T: 0370 850 6506
www.environment-agency.gov.uk

Advice on environmental-friendly document disposal and the WEEE Directive

Financial Services Authority
25 The North Colonnade
Canary Wharf
London
E14 5HS
T: 0845 606 1234
www.fsa.gov.uk

Advice on data protection for financial organisations

Local Government Association
Local Government Group
Local Government House
Smith Square
London
SW1P 3HZ
T: 0207 664 3000
www.lga.gov.uk

Advice and checklists for local government professionals and elected members

Ministry of Justice
102 Petty France
London
SW1H 9AJ
T: 0203 334 3555
www.justice.gov.uk

Government department ultimately responsible for data privacy

NHS Connecting for Health
Vantage House
40 Aire Street
Leeds
LS1 4HT
T: 0113 397 3333
www.connectingforhealth.nhs.uk

Provides information on information management throughout the NHS

PDP Training
16 Old Town
London
SW4 0JY
T: 0845 226 5723
www.pdptraining.com

Data protection training

PDP Journals
16 Old Town
London
SW4 0JY
T: 0845 226 5723
www.pdpjournals.com

Publishers of Privacy and Data Protection Freedom of Information journals

Shred-it Limited
Unit 1 Foresters Green
Trafford Park
Manchester
M17 1EJ
T: 0800 028 1164
www.shredit.co.uk

Secure information destruction services

The Law Society
The Law Society's Hall
113 Chancery Lane
London
WC2A 1PL
T: 0207 242 1222
www.lawsociety.org.uk

Guidance on records management

Workplace Law Network
110 Hills Road
Cambridge
CB2 1LQ
T: 0871 777 8881
www.workplacelaw.net

Network community for UK employers interested in employment law, H&S and premises management

If you would like further guidance on any aspect of information security, including management, destruction and recycling of paper and non-paper, please contact Shred-it on **0800 028 1164**

Assessing your current information security arrangements

Shred-it offer a complimentary data security survey which takes approximately 60 minutes at your site. This is designed to:

- Evaluate current information security and employee practices
- Identify areas for improvement
- Agree a tailor-made solution
- Calculate cost and value benefits

To book please call **0800 028 1164**

Shred-it is a world-leading document destruction company that ensures the security and integrity of customers' private information. The company operates in more than 140 branches in 16 countries worldwide, servicing over 150,000 global, national and local businesses, including the world's top intelligence and security agencies and more than 500 police forces, 1,500 hospitals, 8,500 bank branches and 1,200 universities and colleges.

In the UK, Shred-it has 16 branches, employs over 400 people and operates 125 shredding trucks, providing the most secure and trustworthy information destruction services possible for its customers. Shred-it UK has customers which span the sectors, from government agencies to financial and legal institutions, taking each customer's unique needs into account and bringing secure on site document destruction services direct to their door, thus ensuring total confidentiality in security and shredding.

Shred-it has branches in the following locations: Belfast, Dublin, Glasgow, Edinburgh, West Yorkshire, Chippenham, Essex - Waltham Abbey, Newcastle, Manchester, Birmingham, Milton Keynes, Portsmouth, Exeter, London - Stratford, London - Brentford, Nottingham and now Cardiff.

Shred-it has been assessed and certified as meeting the requirements of ISO 14001, ISO 9001 and EN15713

MG/UK102011